Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Российский экономический университет имени Г. В. Плеханова»
(ФГБОУ ВО «РЭУ им. Г. В. Плеханова»)

А. В. Бабаш

ТЕОРИЯ АВТОМАТОВ. СИНТЕЗ ШИФРУЮЩИХ АВТОМАТОВ

Утверждено издательским советом университета
в качестве учебного пособия

Москва
ФГБОУ ВО «РЭУ им. Г. В. Плеханова»
2020

УДК 004.056.55(075.8)
ББК 32.81я73
Б121

Рецензенты: доц. Е. К. Б а р а н о в а (Высшая школа экономики);
канд. экон. наук М. С. Г а с п а р и а н (РЭУ им. Г. В. Плеханова)

Бабаш, А. В.

Б121 Теория автоматов. Синтез шифрующих автоматов : учебное пособие / А. В. Бабаш. – Москва : ФГБОУ ВО «РЭУ им. Г. В. Плеханова», 2020. – 348 с.

ISBN 978-5-7307-1644-5

В учебном пособии рассмотрен теоретико-автоматный подход к синтезу криптографической защиты информации. Цель пособия состоит в описании методов синтеза шифрующих автоматов. Предлагаются удобные для применения в криптографической практике методы оценки числа неэквивалентных ключей шифров, построенных по классической схеме – управляющий блок и шифрующий блок. Приведен более эффективный, чем известные ранее, алгоритм нахождения областей импримитивности групп подстановок, заданных системой образующих элементов. Представлена также методика оценки периодов и приближенных периодов выходных последовательностей шифрующих автоматов различных классов при заданных начальных состояниях и входных периодических последовательностях.

Для студентов, обучающихся по направлениям «Прикладная информатика» и «Информационная безопасность».

УДК 004.056.55(075.8)
ББК 32.81я73

ISBN 978-5-7307-1644-5 © ФГБОУ ВО «РЭУ им. Г. В. Плеханова», 2020

Оглавление

Предисловие 9
Определения, обозначения и сокращения 12
Глава 1. КЛАССЫ АВТОМАТОВ И ОПЕРАЦИИ НАД АВТОМАТАМИ 17
1.1. Автономный линейный регистр сдвига 17
1.2. Неавтономный линейный регистр сдвига 18
1.3. Неавтономный регистр сдвига 18
1.4. Проходная линия задержки 18
1.5. Шифрующий автомат 19
1.6. Операции над автоматами 20
Глава 2. НЕОТЛИЧИМОСТЬ СОСТОЯНИЙ АВТОМАТОВ 22
2.1. Основные понятия 22
2.2. Неотличимость состояний перестановочных автоматов 24
2.3. Гомоморфизмы автоматов 32
Глава 3. НЕОТЛИЧИМОСТЬ ВХОДНЫХ СЛОВ АВТОМАТОВ 36
3.1. Автономность автоматов 36
3.2. Степени перестановочных автоматов 36
3.3. Псевдоавтономность перестановочных автоматов 40
3.4. Слабая автономность автоматов 48
3.5. Слабый гомоморфизм автоматов 54
Глава 4. ДЕКОМПОЗИЦИЯ АВТОМАТОВ 59
4.1. Разбиения и покрытия множества. Примеры 59
4.2. Фактор-автомат. Покрытие автомата 61
4.3. Параллельное соединение автоматов 64
4.4. Последовательное соединение автоматов 67
Глава 5. ПЕРИОДИЧНОСТЬ ФУНКЦИОНИРОВАНИЯ КОНЕЧНЫХ АВТОМАТОВ 76
5.1. Вспомогательное почти тривиальное утверждение 77
5.2. Основные теоретико-автоматные обозначения 78
5.3. Оценка периодов последовательностей состояний автомата при заданной периодической входной последовательности 79
Глава 6. ГОМОМОРФИЗМЫ НЕАВТОНОМНЫХ ДВОИЧНЫХ РЕГИСТРОВ СДВИГА 81
6.1. Основные понятия 81
6.2. Теорема А. Я. Прососова 82
6.3. Теорема В. А. Башева 85

6.4. Обзор по работе В. И. Солодовникова «Гомоморфизмы двоичных регистров сдвига» 86
Глава 7. ВЕРХНЯЯ ОЦЕНКА СТЕПЕНИ РАЗЛИЧИМОСТИ СВЯЗНЫХ ПЕРЕСТАНОВОЧНЫХ АВТОМАТОВ С ЗАДАННЫМ ДИАМЕТРОМ 98
7.1. Формулировка основных результатов 98
7.2. Доказательство основной оценки 98
7.3. О роли диаметра перестановочного связного приведенного автомата в его оценки степени различимости 101
7.4. Доказательство достижимости полученной оценки степени различимости 109
Глава 8. НЕОТЛИЧИМОСТЬ СОСТОЯНИЙ ПЕРЕСТАНОВОЧНЫХ, АФФИННЫХ И АВТОНОМНЫХ НЕЛИНЕЙНЫХ ВЕКТОРНЫХ АВТОМАТОВ 120
8.1. Основные понятия 120
8.2. Неотличимость состояний перестановочных автоматов 122
8.3. Оценки вероятности k-неотличимости двух случайно и равновероятно выбранных состояния автомата 129
8.4. Неотличимость состояний n-й степени перестановочного автомата 132
8.5. Неотличимость состояний аффинных автоматов 133
8.6. Неотличимость аффинных автоматов 138
8.7. Неотличимость состояний автономных векторных нелинейных автоматов 140
Глава 9. НЕОТЛИЧИМОСТЬ СОСТОЯНИЙ АВТОНОМНОГО ПОСЛЕДОВАТЕЛЬНОГО СОЕДИНЕНИЯ ПЕРЕСТАНОВОЧНЫХ АВТОМАТОВ 143
9.1. Оценки числа классов неотличимых состояний автономных последовательных соединений перестановочных автоматов 143
9.2. Оценки мощностей классов неотличимых состояний автономных последовательных соединений перестановочных автоматов 153
Глава 10. АЛГОРИТМЫ НАХОЖДЕНИЯ МИНИМАЛЬНЫХ СИСТЕМ ОБЛАСТЕЙ ИМПРИМИТИВНОСТИ ГРУППЫ ПОДСТАНОВОК 158
10.1. Алгоритм нахождения минимальных систем импримитивности групп подстановок (M. D. Atkinson) 158
10.2. Новый алгоритм получения минимальных систем областей импримитивности группы подстановок 161

Глава 11. ОДНОСТОРОННЯЯ НЕОТЛИЧИМОСТЬ СОСТОЯНИЙ КОНЕЧНЫХ АВТОМАТОВ 166
11.1. Понятие (Ψ, η)-неотличимости состояний автомата 166
11.2. Определение начального состояния автомата по его входному и выходному слову 167
11.3. Свойства (Ψ, η)-неотличимых состояний автомата 168
11.4. (η, d)-периодические выходные последовательности автономного автомата 172
11.5. G-приведенность автономного последовательного соединения автоматов 175
Глава 12. СИЛЬНО ПРИВЕДЕННЫЕ АВТОМАТЫ 178
Глава 13. ОБ ОДНОМ ПОДХОДЕ К ЛИНЕАРИЗАЦИИ УРАВНЕНИЙ ПОЛУЧЕНИЯ ВЫХОДНОЙ ПОСЛЕДОВАТЕЛЬНОСТИ ВЕКТОРНОГО АВТОМАТА 182
13.1. ℑ-размерность векторного автомата, ℑ-линейная размерность 182
13.2. Определение начального состояния векторного автомата A по его входной и выходной последовательностям 183
Глава 14. ЗАПРЕТЫ АВТОМАТОВ И ДВОИЧНЫХ ФУНКЦИЙ 185
14.1. Криптографические приложения 185
14.2. Запреты автоматов 186
14.3. Запреты двоичных функций 191
14.4. Критерии наличия запрета двоичной функции 192
14.5. Оценки длины запрета двоичной функции 193
Глава 15. ВНЕШНЕ ПЕРИОДИЧЕСКИЕ АВТОМАТЫ 197
15.1. Введение 197
15.2. Автоматы с L-потерей информации о выходе 197
15.3. Критерий внешней периодичности автомата 199
Глава 16. ПЕРИОДИЧЕСКИ ВНЕШНЕ НАСЛЕДСТВЕННЫЕ ПЕРЕСТАНОВОЧНЫЕ АВТОМАТЫ 203
16.1. Автоматы с L-потерей информации 203
16.2. Периодически внешне наследственные автоматы 205
16.3. Критерий внешней наследственности автомата 213
Глава 17. ПЕРИОДЫ ВЫХОДНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ АВТОМАТА ПРИ ЗАДАННОЙ ПЕРИОДИЧЕСКОЙ ВХОДНОЙ ПОСЛЕДОВАТЕЛЬНОСТИ 216
17.1. Краткий обзор результатов по данной теме. Обозначения, основные понятия, вспомогательные результаты 216

17.2. Периоды выходных последовательностей автомата без внешне автономных состояний при входной периодической последовательности заданной полноты 219
17.3. Периоды выходных последовательностей линейного векторного автомата при заданной входной периодической последовательности..... 226
17.4. Период внешнего функционирования автономного последовательного соединения автоматов 231
17.5. Периоды выходных последовательностей перестановочного автомата без потери информации при заданных периодических входных последовательностях 233
17.6. Периоды выходных последовательностей последовательного соединения автономного автомата с перестановочным автоматом без потери информации..... 239
Глава 18. КЛАССЫ АВТОМАТОВ С ГАРАНТИРОВАННЫМИ ПЕРИОДАМИ ВЫХОДНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ..... 243
18.1. Необходимость построения автоматов с гарантированными периодами выходных последовательностей 243
18.2. Кодирующее устройство с конечной памятью..... 244
18.3. Полноцикловый автомат..... 247
18.4. Обратимый автомат..... 253
18.5. Обобщенный узел выборки 254
Глава 19. КЛАССЫ АВТОМАТОВ С ГАРАНТИРОВАННЫМИ ПАРАМЕТРАМИ ПОДПЕРИОДА ВЫХОДНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ 258
19.1. Основные обозначения и понятие подпериода последовательности..... 258
19.2. Автомат Медведева 260
19.3. Кодирующее устройство с конечной памятью (проходная линия задержки с функцией усложнения)..... 263
19.4. Обратимые автоматы 266
Глава 20. О ПЕРИОДИЧНОСТИ ПОСЛЕДОВАТЕЛЬНОСТИ СОСТОЯНИЙ АВТОМАТА, ОТВЕЧАЮЩЕЙ ЕГО НАЧАЛЬНОМУ СОСТОЯНИЮ И ВХОДНОЙ ПЕРИОДИЧЕСКОЙ ПОСЛЕДОВАТЕЛЬНОСТИ. ПРИБЛИЖЕННЫЕ ПЕРИОДЫ ПОСЛЕДОВАТЕЛЬНОСТИ СОСТОЯНИЙ АВТОМАТА 268
20.1. Введение, вспомогательные обозначения, понятия и результаты 268
20.2. Нижние оценки мер приближенных периодов последовательностей состояний автомата, отвечающих

его начальным состояниям и входным смешанно-периодическим последовательностям 274
20.3. Нижние оценки мер приближенных периодов выходных последовательностей регистров сдвига, отвечающих его начальным состояниям и входным смешанно-периодическим последовательностям 278
Глава 21. ПРИБЛИЖЕННЫЕ ПЕРИОДЫ ВЫХОДНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ ПОЛНОЦИКЛОВОГО АВТОМАТА, ПРЕДСТАВИМОГО ПОСЛЕДОВАТЕЛЬНЫМ СОЕДИНЕНИЕМ АВТОНОМНОГО АВТОМАТА С НЕАВТОНОМНЫМ ПЕРЕСТАНОВОЧНЫМ АВТОМАТОМ 281
21.1. Полноцикловое последовательное соединение автоматов 282
21.2. Полноцикловое последовательное соединение автономного автомата с перестановочным коммутируемым автоматом 284
21.3. Класс функций выхода полноциклового последовательного соединения автономного автомата с перестановочным коммутируемым автоматом 285
21.4. Автономное последовательное соединение автоматов со свойством принудительного восстановления состояния второго автомата 290
Глава 22. G-ИЗОПЕРИОД ВЫХОДНОЙ ПОСЛЕДОВАТЕЛЬНОСТИ АВТОНОМНОГО ПОСЛЕДОВАТЕЛЬНОГО СОЕДИНЕНИЯ АВТОМАТОВ 293
22.1. Основные понятия и предварительные результаты 293
22.2. Изопериод последовательности внешнего функционирования перестановочного автомата при заданной входной периодической последовательности 298
22.3. Изопериоды полноциклового автомата, представимого последовательным соединением двух автоматов 299
22.4. Изопериоды последовательного соединения автоматов с выходным алфавитом-группой 303
Глава 23. ОЦЕНКИ ПАРАМЕТРОВ ОБОБЩЕННОЙ ПЕРИОДИЧНОСТИ ВЫХОДНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ НЕКОТОРЫХ ПОЛНОЦИКЛОВЫХ АВТОМАТОВ С ВЫХОДНЫМ АЛФАВИТОМ, ЯВЛЯЮЩИМСЯ ГРУППОЙ 306
23.1. Основные понятия, постановка задачи 306
23.2. σ-периоды последовательности $A^H(P^1)$ для стабильных слева (справа) бинарных отношений на G 309
23.3. Оценки мер приближенных σ-периодов последовательности $A^H(P^1)$ для стабильных слева (справа) бинарных отношений на группе G 312

23.4. Примеры стабильных слева (справа) бинарных отношений на группе G 319
23.5. φ-периоды последовательности $A^H(P^1)$ для автоморфизмов φ-группы G 321
23.6 Оценки мер приближенных φ-периодов последовательности $A^H(P^1)$ для автоморфизмов группы 324
Глава 24. КЛАССЫ ВЕКТОРНЫХ АВТОМАТОВ С ГАРАНТИРОВАННЫМИ ПЕРИОДАМИ ВЫХОДНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ ПРИ ЗАДАННОЙ ВХОДНОЙ ПЕРИОДИЧЕСКОЙ ПОСЛЕДОВАТЕЛЬНОСТИ 328
24.1. Основные понятия. Вспомогательные результаты 328
24.2. Способ построения векторного автомата с гарантированным выходным периодом на основе оценки его слабой автономности 331
24.3. Способ построения векторного автомата с гарантированным выходным периодом на основе нахождения его сильно различимых входных слов 334
24.4. Пример синтеза векторного нелинейного автомата с гарантированным выходным периодом 339
Список литературы 344

Предисловие

Данное учебное пособие посвящено теоретико-автоматному подходу к синтезу криптографической защиты информации. Обобщение и универсальность изложения методов синтеза шифр-аппаратуры достигается выбором теоретико-автоматного языка. Одновременно постановка задач криптографической защиты в терминах теории автоматов и их решения существенно расширили классическое содержание теории автоматов.

Шифры могут описываться моделями автоматов. Так, входной последовательностью (входным словом) автомата является открытый текст, подлежащий шифрованию. Выходной последовательностью является шифрованный (зашифрованный) текст. Ключами являются компоненты начальных состояний и/или функции переходов и выходов автомата. В блочных шифрах открытый текст трактуется как начальное состояние автомата, шифрованный текст – как заключительное состояние автомата, в которое он приходит под воздействием последовательности раундовых ключей. Управляющие блоки шифров предварительного шифрования моделируются автономными автоматами. Для обеспечения реверсивности устройств шифрования требуется взаимная однозначность частичных функций переходов автомата, моделирующего данное устройство, то есть изучение так называемых перестановочных автоматов.

Учитывая криптографическую направленность приводимых теоретико-автоматных утверждений и их приложения, мы называем автоматы с изучаемыми свойствами *шифрующими автоматами*.

В пособии представлена методика оценки периодов и приближенных периодов выходных последовательностей автоматов при заданных начальных состояниях и входных периодических последовательностях.

В ней решаются задачи, связанные:

– с неотличимостью состояний перестановочных автоматов и их слабой автономностью;

– запретами автоматов и двоичных функций;

– оценкой периодов выходных последовательностей конечных автоматов;

– оценкой приближенных периодов выходных последовательностей автоматов;

– оценками мер приближенных периодов выходных последовательностей автоматов, моделирующих поточные шифры.

Представлены следующие классы автоматов:

– автоматы без потери информации;
– перестановочные автоматы;
– автоматы без внешне автономных состояний;
– автономные последовательные соединения автоматов;
– линейные векторные автоматы;
– автоматы Медведева;
– кодирующие устройства с конечной памятью;
– обратимые автоматы;
– полноцикловые автоматы.

Цель пособия состоит в описании разработанных методов синтеза шифрующих автоматов, которые связаны:

– с описанием новых методов оценки количества эквивалентных ключей шифров, основанных на представлении шифр-системы или ее отдельного блока конечным автоматом;

– оценками мощностей классов неотличимых состояний автономных последовательных соединений перестановочных автоматов, моделирующих шифры предварительного шифрования;

– описанием новых методов оценки периодов выходных последовательностей конечных автоматов, моделирующих шифры предварительного шифрования.

Другими словами, она состоит в *нахождении новых классов дискретных устройств с гарантированными периодами выходных псевдослучайных последовательностей* и получении методики оценки мер приближенных периодов выходных последовательностей конечных автоматов, моделирующих шифры предварительного шифрования.

Для класса перестановочных автоматов указаны новые алгоритмы доказательства их приведенности. Разработаны новые способы проверки наличия у автоматов автономных и слабоавтономных состояний. Приведены доказательства верхних оценок сложности таких алгоритмов.

Указаны новые методы доказательства приведенности автоматов из следующих классов: перестановочных, аффинных и автономных нелинейных векторных автоматов, автономного последовательного соединения перестановочных автоматов. При этом даны удобные для применения в криптографической практике методы оценки числа неэквивалентных ключей шифров, построенных по классической схеме – управляющий блок и шифрующий блок (чис-

ло классов неотличимых состояний автономных последовательных соединений перестановочных автоматов и оценки их мощностей).

Приведенный в работе алгоритм нахождения областей импримитивности групп подстановок, заданных системой образующих элементов, более эффективен, чем известные ранее. Он позволяет для ряда шифр-систем применять новый способ доказательства отсутствие в них эквивалентных ключей. Дело в том, что нетривиальная система классов эквивалентных ключей в этих шифр-системах является и некоторой системой областей импримитивности группы подстановок. Полученная оценка длины запрета произвольной двоичной функции говорит о намного меньшей трудоемкости известного метода распознавания закона функционирования проходной линии задержки с неизвестной функцией выхода, основанного на наличии запретов у данного криптографического узла. Описаны методы построения новых классов автоматов с гарантированными периодами их выходных последовательностей. Так, в частности, найдены условия кратности периодов выходных последовательностей автоматов из построенных классов периоду входной последовательности. Эти классы таковы: автоматы без потери информации, перестановочные автоматы, автоматы без внешне автономных состояний, автономные последовательные соединения автоматов, линейные векторные автоматы, автоматы Медведева, кодирующие устройства с конечной памятью, обратимые автоматы.

Введены понятия:

– меры приближенного периода периодической последовательности элементов, отражающее Хэммингову близость последовательности к периодической последовательности заданного периода;

– изопериода периодической последовательности элементов;

– σ-периода периодической последовательности элементов.

Приведены:

– оценки приближенных периодов выходных последовательностей полноциклового автомата, представимого последовательным соединением автономного автомата с неавтономным перестановочным автоматом;

– оценки изопериода и σ-периода последовательностей специальных автоматов, моделирующих получение суммарных шифров поточных шифров.

Приведенные алгоритмы и методы являются новыми и более эффективными, чем ранее известные.

Полученные результаты являются фундаментом для построения шифрующих автоматов с гарантированными периодами их управляющих и результирующих гамм. Они могут быть использованы в криптографической практике. Одновременно эти результаты являются основой для построения приближенных моделей автоматов и построения на их основе новых методов криптографического анализа и синтеза.

Определения, обозначения и сокращения

Для множества Z, состоящего из элементов 1, 2, …, k используется обозначение $Z = \{1, 2, \ldots, k\}$.

Далее:

(a, b) – наибольший общий делитель двух чисел a, b, или ОНД(a, b);

НОК(a, b) – наибольшее общее кратное чисел a, b, в ряде случае для удобства используется и обозначение [a, b];

a|b – a делит b;

$X \times Y$ – декартовым произведением множеств X и Y;

X^k – множество слов в алфавите X длины k;

|M| – мощность множества M;

h(M') – образ подмножества $M' \subseteq M$ для отображения $h: M \to V$. Часто мы будем опускать скобки и писать hM', а для элемента $m \in M$ будем писать h(m) или hm.

Под словом «автомат» подразумевается конечный автомат A = (X, S, Y, h, f), где:

X – конечное непустое множество, названное множеством входных символов (входной алфавит);

X* – множество всех слов конечной длины в алфавите X;

S – конечное непустое множество, названное множеством состояний (внутренний алфавит);

Y – конечное непустое множество, названное множеством выходных символов (выходной алфавит);

$h: S \times X \to S$ – функция переходов;

$f: S \times X \to Y$ – функция выхода.

Если в момент времени t = 1, 2, … автомат A находится в состоянии $s(t) \in S$ и на его вход поступил символ $x(t) \in X$, то в этот же момент времени на выходе автомата A образуется символ f(s(t), x(t)) и автомат A переходит в новое состояние s(t + 1) = h(s(t), i(t)).

При условии, что $f(s, x) = \lambda(s)$ для любых $x \in X$, $s \in S$, где $\lambda: S \to Y$, автомат Мили A может рассматриваться как автомат Мура и будет обозначатся через:

$$A = (X, S, Y, h, \lambda).$$

Если X состоит из одного элемента $|X| = 1$, то такой автомат называется автономным, и обозначается через $A = (S, Y, h, \lambda)$.

Автомат часто задают его графом переходов: вершинами графа являются состояния автомата. Из каждого состояния s и каждого $x \in X$ проводится ориентированная дуга (стрелка) в состояние $s` = h(x, s)$. Она помечается двумя символами (x, y), где $y = f(x, s)$. Таким образом, из каждого состояния выходят $|X|$ дуг. Говорят, что состояние s` *достижимо из s* в автомате A, если в его графе переходов существует ориентированный путь из s в s`. Для таких пар состояний (s, s`) можно ввести минимальное расстояние m(s, s`) от s до s` как минимальное число дуг, по которым можно перейти из s в s`.

Диаметром автомата A называют величину $\max\limits_{(s,s`)} m(s,s`)$, где максимум берется по всем парам состояний (s, s`), для которых существует m(s, s`).

Граф переходов автомата (или просто «автомат») называют связным, если для любых его двух состояний s, s` в графе существует *неориентированный* путь из s в s`, что равносильно существованию неориентированного пути из s` в s. Неориентированный путь – это путь по состояниям графа переходов, использующий обычные дуги $\rightarrow$ и обратные к ним $\leftarrow$. Если автомат не связный, то его граф переходов состоит из нескольких связных компонент – связных подавтоматов автомата.

Автономный автомат $A = (S, Y, h, \lambda)$ называют полноцикловым, если его граф состоит из цикла, содержащего все его состояния.

Граф переходов автомата (автомат) называют *сильно связным*, если для любой пары упорядоченных его состояний (s, s`) существует ориентированный путь из s в s`. В любом связном автомате можно выделить сильно связный подавтомат.

Зачастую нам удобно использовать несколько другое обозначение автомата: A = (X, S, Y, h, f).

Определим так называемые *частичные функции переходов* $(h_x)_{x \in X}$ и *выходов* $(f_x)_{x \in X}$ через h и f следующим образом:

$$h_x: S \to S,\ h_x(s) = h(x, s);\ f_x: S \to Y,\ f_x(s) = f(x, s).$$

Новое обозначение автомата A имеет вид:

$$A = (X, S, Y, (h_x)_{x \in X}, (f_x)_{x \in X}).$$

Итак:

h_x: S→S – частичная функция переходов автомата A, соответствующая входному символу x∈X, задаваемая соотношением $h_x(s) = h(s, x)$, s∈S (для удобства ниже в этой записи мы опускаем скобки при h_x: $h_x s = h(s, x)$;

$h_x(Z)$ – образ множества Z, Z⊆S при отображении h_x;

f_x: S→Y – частичная функция выхода соответствующая входному символу x∈X, задаваемая соотношением $f_x(s) = f(s, x)$, s∈S (для удобства ниже в этой записи мы опускаем скобки при f_x: $f_x s = f(s, x)$).

Читателю необходимо помнить, что *слово в каком-либо алфавите мы пишем, отделяя буквы запятыми.*

Используются дополнительные обозначения:

P = x(1), x(2), …, x(k), x(j)∈X, j∈{1, 2, …, k} – входное слово длины k автомата A;

в ряде случаев (например, чтобы отличить обозначение вероятности P), мы используем и другие обозначения, в частности обозначение ℑ = x(1) ,x(2), …, x(k), или J = x(1), x(2), …, x(k);

|P| – длина входного слова P автомата A;

$h_P = h_{x(k-1)}\, h_{x(k-2)} \ldots h_{x(1)}$ – отображение S→S, осуществляемое автоматом A в результате приложения к нему входного слова P = x(1), x(2), …, x(k);

каждое состояние вида $h_x(s)$ называется 1-приемником состояния s;

состояние вида $h_{x(k)}\, h_{x(k-1)} \ldots h_{x(1)}\,(s)$ называется k-м преемником состояния s;

$f_P = f_{x(k)}\, h_{x(k-1)}\, h_{x(k-1)} \ldots h_{x(1)}$ – отображение S→Y, осуществляемое автоматом A в результате приложения к нему входного слова P = x(1), x(2), …., x(k);

f_{PS} или P(s) – заключительное состояние автомата, полученное с начального состояния s при водном слове (последовательности) P;

A(s, P) = $y_1, y_2, ..., y_k$, y_i∈Y, j∈[1, k] – выходное слово автомата A, полученное в результате приложения входного слова P = x(1), x(2), …., x(k) к автомату A с начальным состоянием s∈S;

$A_M(s, P) = s_1, s_2, \ldots, s_j, \ldots$ – последовательность состояний автомата A = (X, S, Y, h, f), отвечающая его входной последовательности P и начальному состоянию s = s_1 из S;

полугруппа $G = \langle (h_x)_{x \in X} \rangle$ автомата A – это полугруппа отображений множества S в себя, порожденная частичными функциями перехода $(h_x)_{x \in X}$ автомата A и тождественным отображением S в себя;

Автомат A называют *перестановочным*, если его частичные функции переходов $(h_x)_{x \in X}$ осуществляют взаимно однозначные отображения S в S; говорят также: биекции S в S, (подстановки на S).

Имея дело с несколькими автоматами, будем отмечать пятерки X, S, Y, h, f различными символами (верхними и нижними), например, $A = (X_A, S_A, Y_A, h_A, f_A)$. Если же автомат обозначается символом A с каким-нибудь индексом, например A', то иногда для простоты мы будем помечать элементы его пятерки тем же индексом, например, (X', S', Y', h', f'). Аналогичным образом мы будем поступать и для различения введенных параметров автоматов, например, полугруппа автоматов A и B удобно соответственно обозначать через G_A и G_B.

Напомним следующие основные понятия.

Определение 1. Состояние s и s' автомата A называется k-неотличимыми, если A(s, P) = A(s', P) для любого входного слова P = x(1), x(2),…, x(k) длины k автомата A. В противном случае они называются k-различимыми.

Определение 2. Состояния s и s' автомата A называются неотличимыми, если они k-неотличимы для любого k. В противном случае они называются различными (отличными).

Хорошо известна следующая теорема [14; 21].

Теорема 1. Для неотличимости двух состояний автомата A = (X, S, Y, h, f) достаточна их $(|S| - 1)$-неотличимость.

Поскольку бинарное отношение k-неотличимости состояний автомата является отношением эквивалентности, все множество состояний S автомата A разбивается на непересекающиеся классы k-неотличимых состояний.

Будем обозначать это разбиение через:

$$N^k = (N_1^k, N_2^k, \ldots, N_{l_k}^k),$$

где N_j^k, $j \in [1, l_k]$ – классы k-неотличимых состояний автомата A, а l_k – число классов k-неотличимых состояний автомата A.

Классы неотличимых состояний автомата A будем обозначать через N_j, $j \in [1, l]$, а само разбиение множества S эти классы через

$$N = (N_1, N_2, \ldots, N_l),$$

где l – число классов неотличимых состояний автомата A.

Определение 3. Число R называется степенью различимости автомата A, если

$$N^R = N \text{ и } N^k \neq N \text{ при } k < R.$$

Определение 4. Автомат A называется приведенным (или находится в приведенной форме), если $|N_j| = 1$ для любого $j \in [1, l]$.

Очевидно, если A приведенный автомат, то $l = |S|$.

Любая тайна, порожденная человеческим сознанием,
им же может быть и раскрыта.
Артур Конан Дойл

…Едва ли разуму человека дано загадать такую загадку,
которую разум другого его собрата,
направленный должным образом, не смог бы раскрыть.
Эдгар По

Нет недешифруемых шифров.
Л. П. Берия

Шифр случайного гаммирования дешифруем.
А. В. Бабаш

Глава 1. КЛАССЫ АВТОМАТОВ И ОПЕРАЦИИ НАД АВТОМАТАМИ

Ниже приводятся некоторые классы автоматов, используемые при синтезе симметричных шифр-систем [16].

1.1. Автономный линейный регистр сдвига

Обозначим через F_2 из двух элементов, F_2^n – координатное векторное пространство размерности n над полем F_2 (вектора – двоичные наборов длины n). Выберем некоторую линейную двоичную функцию на F_2^n, которую запишем в виде

$(a, x) = a_1x_1 \oplus a_2x_2 \oplus \ldots \oplus a_nx_n$,

$(a_1, a_2, \ldots, a_n) \in F_2^n$, $x = (x_1, \ldots, x_n)$ – двоичные переменные, $\oplus$ – сложение по модулю 2.

Автономным линейным регистром сдвига называется автономный автомат

$$A = (S, Y, h, \lambda),$$

где $S = F_2^n \setminus (o)$;

F_2^n с исключенным нулевым вектором;

$Y = F_2$, $h: S \to Y$, для $v = (v_1, v_2, \ldots, v_n) \in F_2^n \setminus (o)$;

$h(v_1, v_2, \ldots, v_n) = (v_2, \ldots, v_n\ (a, v))$;

λ – произвольная, отличная от нуля линейная функция на F_2^n (ее ограничение на $F_2^n \setminus (o)$ мы обозначили той же буквой).

1.2. Неавтономный линейный регистр сдвига

Используем введенные обозначения. *Неавтономным линейным регистром сдвига* называется автомат

$$A = (X, S, Y, (h_x)_{x \in X}, \lambda),$$

где $X = F_2$, $S = F_2^n \setminus (0)$;

$h_0(v_1, v_2, \ldots, v_n) = (v_2, \ldots, v_n, (a, v))$;

$h_1(v_1, v_2, \ldots, v_n) = (v_2, \ldots, v_n, 1 \oplus, (a, v))$;

λ – произвольная отличная от нуля линейная функция на F_2^n.

1.3. Неавтономный регистр сдвига

Используем введенные обозначения и дополнительно через $\theta(x_1, \ldots, x_n)$ обозначим произвольную двоичную функцию на F_2^n. Неавтономным регистром сдвига называется автомат

$$A = (X, S, Y, (h_x)_{x \in X}, \lambda),$$

где $X = F_2$, $S = F_2^n$;

$h_0(v_1, v_2, \ldots, v_n) = (v_2, \ldots, v_n, \theta(v_1, v_2, \ldots, v_n))$;

$h_1(v_1, v_2, \ldots, v_n) = (v_2, \ldots, v_n, 1 \oplus \theta(v_1, v_2, \ldots, v_n))$;

$(v_1, v_2, \ldots, v_n) \in F_2^n$, λ – произвольная двоичная функция на F_2^n.

Автономный регистр сдвига $A = (S, Y, h, \lambda)$ отличается от неавтономного наличием одной частичной функции перехода:

$$h(v_1, v_2, \ldots, v_n) = (v_2, \ldots, v_n, \theta(x_1, \ldots, x_n)).$$

1.4. Проходная линия задержки

Проходная линия задержки – это неавтономный автомат $A = (X, S, Y, (h_x)_{x \in X}, \lambda)$ вида $X = F_2$, $S = F_2^n$, $Y = F_2$, $h_0(v_1, v_2, \ldots, v_n) = (v_2, \ldots, v_{n-1}, 0)$, $h_1(v_1, v_2, \ldots, v_n) = (v_2, \ldots, v_{n-1}, 1)$, λ – произвольная двоичная функция.

В качестве упражнения:

– определите аналогичные автоматы для произвольного конечного поля F_q;

– докажите, что неавтономный регистр сдвига будет перестановочным автоматом тогда и только тогда, когда двоичная функция θ имеет вид

$$\theta(x_1, \ldots, x_n) = x_1 \oplus \theta`(x_2, \ldots, x_n),$$

где $\theta`(x_2,\ldots,x_n)$ – произвольная функция от двоичных переменных $x_2,\ldots,x_n$.

1.5. Шифрующий автомат

Понятие шифрующего автомата трактуется неоднозначно [6].

Первое определение состоит в том, что *шифрующий автомат есть* множество автоматов A(r), $r\in R$ с начальными состояниями $s(r)\in S(r)$. Такое определение равносильно тому, что под шифрующим автоматом понимают некоторое *множество автоматных отображений* множества открытых текстов в шифрованные.

Второе определение шифрующего автомата состоит в том, что автомат $A = (X, S, Y, (h_x)_{x\in X}, (f_x)_{x\in X})$ является *шифрующим автоматом, если его автоматные отображения* $\varphi_{A,s}$ $X^*\to Y^*$, $s\in S$ *являются инъективными отображениями*. Такое определение согласуется с определением шифра (X, К, У, f) в том смысле, что в качестве отображений f_χ берутся автоматные инъективные отображения.

Для большей общности иногда второе определение обобщают. Именно рассматривают автоматы, у которых $X = \Gamma\times@$, где Γ – алфавит внешней части ключа, часть ключа: $\gamma = \gamma1, \gamma2, \ldots, \gamma L, \gamma j\in\Gamma$; @ – алфавит открытого текста. При фиксированных частях ключа $\gamma\in\Gamma^L$ и $s\in S$ требуют инъективность отображения $@^L$ в Y^L, то есть при входных различных последовательностях вида P = (a1, γ1), (a2, γ2), …, (aL, γL) и P` = (a`1, γ1), (a`2, γ2), …, (a`L, γL) требуют, чтобы $A(s, P) \neq A(s, P`)$ при любом натуральном L.

Выясним условия, при которых автомат A = (X, S, Y, h, f) является шифрующим автоматом, то есть автоматные отображения $\varphi_{A,s}$ $X^*\to Y^*$, $s\in S$ являются инъективными отображениями. Для отображения f: $X\times S\to Y$ обозначим через f_s отображение X в Y: $f_s(x) = f(x, s)$. Через S_s обозначим множество состояний автомата A, содержащее s и все состояния $s`\in S$, достижимые из s в графе переходов автомата A, то есть для которых есть пути из s в s`. На множестве S_s определен подавтомат $A_s = (X, S_s, Y, h, f)$ автомата A (здесь ограничения отображений h, f обозначены теми же буквами). С использованием введенных определений несложно доказывается.

Утверждение. Автоматное отображение $\varphi_{A,s}$ $X^*\to Y^*$, $s\in S$ является инъективным тогда и только тогда, если при каждом состоянии s` из $S_s$ отображение $f_{s`}$ инъективно.

В *третьем определении* под шифрующим автоматом понимают автомат, моделирующий устройство шифрования либо некоторого его блока. В таком понимании устройство шифрования моделируют автоматом $A = (X, S, Y, (h_x)_{x\in X}, (f_x)_{x\in X})$, у которого отображения $(h_x)_{x\in X}$ S в S являются биекциями S в S. *Такие автоматы обычно называют перестановочными* [6]. Часто гаммообразующее устройство шифратора называют шифрующим автоматом.

В последнее время появилось еще одно понимание шифрующего автомата. *Четвертое определение* состоит в следующем. Пусть K – произвольное конечное множество, названное множеством ключей. Определим автомат A = (X, S, Y, h, f) следующим образом:

$$S = S` \times K,$$

где S` – некоторое конечное непустое множество, названное новым множеством состояний.

Тогда по определению автомата

$$h: S`\times K\times X\to S`\times K,\ f: S`\times K\times X\to Y.$$

Теперь представляют действие h в виде

$$h(s`, k, x) = (h_1(s`, k, x), h_2(s`, k, x)),$$

где h_1, h_2 – координатные функции h;

$h_1: S`\times K\times X\to S`$, $h_2: S`\times K\times X\to K$.

В [34] эти функции названы:

– *функцией переходов* (h_1);
– *функцией обновления ключа* (h_2).

Вводится еще одна функция z: K→S`, которая названа *функцией инициализации*.

1.6. Операции над автоматами

Последовательным соединением автоматов $A = (X, S_A, Y, h^A, f^A)$, $B = (X_B = Y, S_B, Z, h^B, f^B)$ называют автомат $A\to B = (X, S_A\times S_B, Z, h, f)$, где для любых $x\in X$, $(s_A, s_B)\in S_A\times S_B$

$$h((s_A, s_B), x) = (h^A(s_A, x), h^B(s_B, f^A(s_A, x)), f((s_A, s_B), x) = f^B(s_B, f^A(s_A, x)).$$

Последовательное соединение A→B изображается в виде схемы (рис. 1).

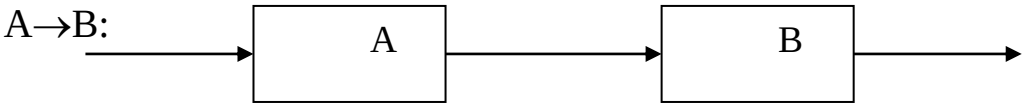

Рис. 1

Под обобщенным последовательным соединением с выходной функцией Ф автоматов $A = (X, S_A, Y, h^A, f^A)$, $B_M = (X_B = Y, S_B, Z, h^B)$ называют автомат

$$A \xrightarrow{\Phi} B = (X, S_A \times S_B, Z, h, \Phi),$$

где для любых $x \in X$, $(s_A, s_B) \in S_A \times S_B$

$$h((s_A, s_B), x) = (h^A(s_A, x), h^B(s_B, f^A(s_A, x)), \Phi: S_A \times S_B \to Z.$$

Параллельным соединением автоматов $A = (X, S_A, Y, h^A, f^A)$, $B = (X, S_B, Z, h^B, f^B)$ называют автомат $C = (X, S_A \times S_B, Z, (h^A, h^B), (f^A, f^B))$, где $(h^A, h^B)((s_A, s_B), x) = (h^A(s_A, x), h^B(s_B, x))$,

$(f^A, f^B)((s_A, s_B), x) = (f^A(s_A, x), f^B(s_B, x))$.

Параллельное соединение автоматов A и B представляется в виде схемы (рис. 2).

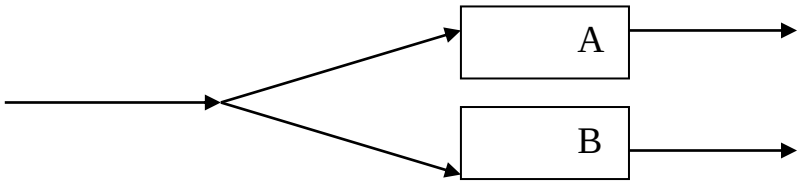

Рис. 2

В ряде случаев параллельное соединение автоматов $A = (X_A, S_A, Y, h^A, f^A)$, $B = (X_B, S_B, Z, h^B, f^B)$ представляют в виде, показанном на рис. 3.

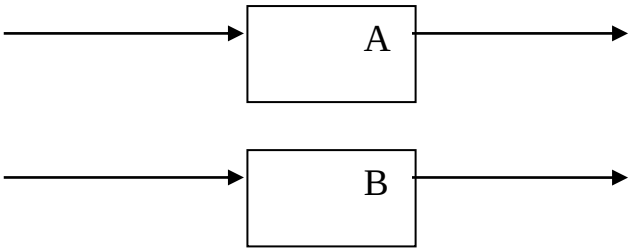

Рис. 3

В качестве упражнения выпишите законы функционирования такого соединения автоматов. Объединением автоматов $A = (X, S_A, Y, h^A, f^A)$, $B = (X, S_B, Z, h^B, f^B)$ называют автомат C, состоящий из подавтоматов A и B. При этом требуют, чтобы $S_A \cap S_B = \varnothing$. Так,

$$C = (X, S_A \cup S_B, Y^C, h^C, f^C),$$

где $h^C(s, x) = h^A(s, x)$, если $s \in S_A$, $h^C(s, x) = h^B(s, x)$,), если $s \in S_B$,

$f^C(s, x) = f^A(s, x)$, если $s \in S_A$, $f^C(s, x) = f^B(s, x)$,), если $s \in S_B$.

Глава 2. НЕОТЛИЧИМОСТЬ СОСТОЯНИЙ АВТОМАТОВ

2.1. Основные понятия

Напомним следующие основные понятия [16; 27; 17].

Определение 1. Состояние s и s’ автомата A называется k-неотличимыми, если A(s, P) = A(s’, P) для любого входного слова P = x(1), x(2), …, x(k) длины k автомата A. В противном случае они называются k-различимыми.

Определение 2. Состояния s и s’ автомата A называются неотличимыми, если они k-неотличимы для любого k. В противном случае они называются различными (отличными).

Рассмотрим хорошо известную теорему.

Теорема 1. Для неотличимости двух состояний автомата A = (X, S, Y, h, f) достаточна их ($|S|-1$)-неотличимость.

Поскольку бинарное отношение k-неотличимости состояний автомата является отношением эквивалентности, все множество состояний S автомата A разбивается на непересекающиеся классы k-неотличимых состояний. Будем обозначать это разбиение:

$$N^k = (N_1^k, N_2^k, \ldots, N_{l_k}^k),$$

где N_j^k, $j \in [1, l_k]$ – классы k-неотличимых состояний автомата A, l_k – число классов k-неотличимых состояний автомата A. Здесь *k играет роль индекса* (не надо путать N^k с декартовой степенью множества).

Классы неотличимых состояний автомата A будем обозначать через N_j, $j \in [1, l]$, а само разбиение множества S эти классы через

$$N = (N_1, N_2, \ldots, N_l),$$

где l – число классов неотличимых состояний автомата A.

Определение 3. Число R = R(A) называется степенью различимости автомата A, если

$$N^R = N \text{ и } N^k \neq N \text{ при } k<R.$$

Определение 4. Автомат A называется приведенным (или находится в приведенной форме), если $|N_j| = 1$ для любого $j \in [1, l]$.

Очевидно, что если A – приведенный автомат, то $l = |S|$.

Теорема 2. Для степени различимости R(A) любого автомата A = (X, S, Y, h, f) с числом состояний $|S| \geq 2$ справедлива достижимая верхняя оценка $R(A) \leq (|S| - 1)$.

Доказательство. Используем введенное ранее обозначение

$$N^k = (N_1^k, N_2^k, \ldots, N_{l_k}^k).$$

Возможны два случая.

а) Функции выходов постоянны на S, что равносильно $N^1 = (N_1^1)$, то есть $N_1^1 = S$, $l_1 = 1$. Тогда очевидно, что $N^k = N^1$. Следовательно, R(A) = 1 и R(A) ≤ |S| – 1.

б) Функции выходов не постоянны на S. Тогда $l_1 \geq 2$. Из этого и того, что k-неотличимые состояния являются и (k-1)-неотличимыми, и определения величины R(A) получаем

$$l_2 \geq 3,\ l_3 \geq 4, \ldots,\ l_k \geq k+1$$

для всех k≤R(A). В частности, $l_{R(A)} \geq R(A)+1$, но $|S| \geq l_{R(A)}$. Следовательно, $|S| \geq R(A)+1$, или R(A) ≤ |S| – 1.

Для доказательства достижимости данной оценки достаточно привести пример автомата с R(A) = |S| – 1. Рассмотрим автономный автомат A = (S, Y, h, λ), где S = {1, …, n}, n>1, Y={0, 1}, $h(s_j) = s_{j+1}$ для j∈{1, …, n–1}, h(n) = 1, λ(1) = 1, а λ(j) = 0, j∈{1, …, n–1}. Читателю предлагается доказать, что для данного автомата A

$$R(A) = n - 1.$$

Доказательство теоремы 1. В связи с теоремой 2 для доказательства теоремы 1 достаточно доказать, что если для автомата A разбиения N^k и N^{k+1} совпадают, то $N^k = N^{k+j}$ для любого j∈{1, 2, …}. Для этого в свою очередь достаточно доказать, что $N^{k+1} = N^{k+2}$, то есть воспользоваться индукцией. Пусть $N^k = N^{k+1}$, и s, s∈N^k, то есть

$$A(s, x(1), \ldots, x(k)) = A(s`, x(1), \ldots, x(k)).$$

При любом слове x(1), …, x(k)∈X^k. По условию

$$A(s, x(1), \ldots, x(k+1)) = A(s`, x(1), \ldots, x(k+1)) \qquad (1)$$

при любом слове x(1), …, x(k), x(k+1)∈X^{k+1}. В частности, A(s, x(1)) = A(s, x(1)). Фиксируем произвольное слово x(1), x(2), …, x(k), x(k+1), x(k+2) длины k+2. Покажем, что

$$A(s, x(1), \ldots, x(k), x(k+1), x(k+2)) = A(s`, x(1), \ldots, x(k), x(k+1), x(k+2)) \qquad (2)$$

Из (1) следует

$$A(h_{x(1)}s, x(2), \ldots, x(k+1)) = A(h_{x(1)}s`, x(2), \ldots, x(k+1))$$

при любом слове x(2), …, x(k+1)∈X^k, то есть $h_{x(1)}s$, $h_{x(1)}s`$ k-неотличимы. Тогда они должны быть (k+1)-неотличимыми. Следовательно, для слова x(2), …, x(k), x(k+1), x(k+2) имеем

$$A(h_{x(1)}s, x(2), \ldots, x(k+1), x(k+2)) = A(h_{x(1)}s`, x(2), \ldots, x(k+1, x(k+2)).$$

Совместно с A(s, x(1)) = A(s, x(1)) это равенство показывает, что выполняется требуемое равенство. Теорема 1 полностью доказана.

Определение 5. Два или большее число автоматов называется *сравнимыми,* если они имеют одинаковые входные и выходные алфавиты.

Если A и B – сравнимые автоматы, s_A и s_B – состояния автоматов A и B, соответственно, то k-неотличимость и неотличимость этих состояний может быть определены аналогично определениям 1, 2.

Определение 6. Говорят, что сравнимые автоматы A и B k-неотличимы, если каждому состоянию автомата A соответствует по крайней мере одно k-неотличимое от него состояние в автомате B и если каждому состоянию автомата B соответствует по крайней мере одно k-неотличимое от него состояние в автомате A. Если автоматы не являются неотличимыми, то они называются различными.

Очевидно, если автоматы k-неотличимы при любом k, то они неотличимы. Напомним еще раз одно важное понятие в теории конечных автоматов [17; 6].

Определение 7. Автомат A = (X, S, Y, h, f) называется перестановочным автоматом, если его частичные функции переходов $(h_x)_{x\in X}$ осуществляют взаимно однозначные отображения множества S в себя.

В случае перестановочного автомата A полугруппа G_A автомата A есть группа. Граф переходов перестановочного автомата A распадается на связанные компоненты, которые в силу перестановочности автомата A является сильно связанными [27].

Компонентами автомата A будут называться подавтоматы автомата A, отвечающие соответствующим компонентам его графа переходов. Очевидно, что компоненты перестановочного автомата являются перестановочными автоматами.

2.2. Неотличимость состояний перестановочных автоматов

Исследование неотличимости состояний конечных автоматов проводились в целом ряде работ, например, [16, 27, 17]. Полученные в них результаты основаны на табличном задании автомата, которые эффективны лишь при сравнительно малом числе состояний.

В настоящем пункте рассматривается задача описания классов неотличимых состояний конечных перестановочных автоматов [17]. Полученные результаты могут быть использованы при исследовании эквивалентности ключей [1; 6] в ряде шифрующих устройств,

которые могут трактоваться как конечные перестановочные автоматы с большим числом состояний.

Обозначим через B_i, $i \in [1,W]$ связанные компоненты перестановочного автомата A. Известно, что отношение неотличимости автоматов является отношением эквивалентности, поэтому множество всех связных компонент B_i, $i \in [1, W]$ автомата A разбивается на некоторое число непересекающихся классов неотличимых связных компонент автомата A. Пусть t – число классов неотличимых связных компонент автомата A. Если A_i, $i \in [1, t]$ подавтомата A, состоящего из некоторого класса неотличимых связных компонент автомата A, то перестановочный автомат A можно представить как автомат, состоящий из перестановочных подавтоматов A_i, $i \in [1, t]$ автомата A, все связанные компоненты которых неотличимы. Для перестановочных автоматов приводимое ниже утверждение дает возможность свести задачу определения классов неотличимых состояний к двум задачам:

1) задача определения классов неотличимых состояний перестановочного автомата, связанные компоненты которого являются неотличимыми перестановочными автоматами;

2) задача определения неотличимости или различимости связных перестановочных автоматов.

Теорема 3. Каждый класс неотличимых состояний перестановочного автомата A является классом неотличимых состояний некоторого подавтомата A_i, $i \in [1, t]$, состоящего из одного из классов неотличимых связных компонент автомата A, где t – число классов неотличимых связных компонент автомата A.

Доказательство. Для доказательства теоремы 3 очевидно достаточно показать, что если два состояния автомата A, принадлежащие различным связным компонентам автомата A, неотличимы, то эти компоненты неотличимы (то есть соответствующие им подавтоматы неотличимы). А это утверждение немедленно следует из того факта, что приемники неотличимых состояний неотличимы. Предоставляем читателю доказать, что если автоматы B и B’ сильно связаны и различимы, то любое состояние автомата B различимо с каждым состоянием автомата B’. Докажите также, что сильная связанность каждой связной компоненты автомата A следует из его перестановочности.

Из теоремы 3 непосредственно вытекает следствие 1.

Следствие 1. Перестановочный автомат A является приведенным тогда и только тогда, если каждая связная компонента автомата

A приведена и нет ни одной пары неотличимых связных компонент автомата A.

Замечание 1. Как следует из доказательства теоремы 2, ее утверждение и утверждение следствия 1 справедливы для более широкого класса автомата, а именно для автоматов, состоящих из изолированных сильно связных компонент.

Перейдем теперь к решению первой из поставленных выше двух задач. Рассмотрим сначала связный перестановочный автомат, то есть перестановочный автомат, состоящий из одной связной компоненты.

Теорема 4. Мощности классов неотличимых состояний связного перестановочного автомата A одинаковы и равны числу О. Н. Д.:

$$(\,|N_1^1|, |N_2^1|, \ldots, |N_{l_1}^1|, |N_1^2|, \ldots, |N_{l_2}^2|, \ldots, |N_1^{|S|-1}|, \ldots, |N_{l_{|S|-1}}^{|S|-1}|\,)$$

Доказательство. Рассмотрим классы неотличимых состояний $N_1, N_2, \ldots, N_l$ автомата $A = (X, S, Y, h, f)$ и предположим, что при некоторых $i, j \in [1, l]$, $|N_j| > |N_i|$

$$s_j \in N_j \text{ и } s_i \in N_i .$$

Так как автомат A сильно связан, то существует входное слово $\Im$ (конечной длины), для которого $h_\Im(s_j) = s_i$.

Вследствие того что каждое состояние из множества $h_\Im(N_j)$ неотличимо от состояний s_i и $h_\Im$, есть подстановка множества S, заключаем, что

$$|N_i| \geq |N_j| .$$

Это противоречит предположению $|N_j| > |N_i|$. Таким образом, первое утверждение теоремы 4 доказано. Воспользуемся теперь тем обстоятельством, что каждый класс k-неотличимых состояний есть объединение некоторых классов (k+1)-неотличимых состояний. Если $d = |N_n^{|S|-1}|$, $n \in [1, l_{|S|-1}]$, то получаем, что мощность каждого класса k-неотличимых состояний при $k < |S|$ есть число кратное d, откуда и следует второе утверждение теоремы 4.

Следствие 2 (из теоремы 3). Если $|S|$ – простое число, то связанный перестановочный автомат $A = (X, S, Y, h, f)$, у которого не все частичные функции выхода постоянны на множестве S, является приведенным автоматом.

Доказательство. Действительно,

$$|S| = \sum_{i=1}^{l} |N_i| = l \cdot d, \; d = |N_i|, \; i \in [1, l].$$

Следовательно, либо $l = 1$, либо $d = 1$. Первый случай противоречит условию следствия 2 – и значит $d = 1$, то есть A – приведенный автомат.

Непосредственно из теоремы 3 получаем еще одно следствие.

Следствие 3. Если $(\left| N_i^1 \right|, \left| N_j^1 \right|) = 1$ для некоторых $i, j \in [1, l_1]$, то связанный перестановочный автомат A является приведенным автоматом.

Напомним, что разбиением $\Pi = \{\Pi_k, k \in \{1, \ldots, L(\Pi)\}$ множества S называются множество его подмножеств Π_k, таких что

$$\Pi_k \cap \Pi_j = \varnothing,\ k \neq j, \quad \bigcup_k \Pi_k = S.$$

Среди всех разбиений множества S выделяют так называемые *тривиальные разбиения.* Это разбиение на одноэлементные множества: $|\Pi_k| = 1$, $k \in \{1, \ldots, |S|\}$, $L(\Pi) = |S|$ и разбиение, состоящее из одного подмножества: $L(\Pi) = 1$, $\Pi_1 = S$. Под *тривиальным разбиением на классы неотличимых состояний* автомата A понимают лишь одно разбиение Π, при котором $|\Pi_k| = 1$, $k \in \{1, \ldots, |S|\}$. В этом случае автомат A является приведенным.

Напомним понятие *импримитивной группы автомата.*

Пусть $G_A = \langle (h_x)_{x \in X} \rangle$ – группа, порожденная множеством частичных функций переходов перестановочного автомата $A = (X, S, Y, (h_x)_{x \in X}, (f_x)_{x \in X})$. Будем предполагать, что группа G_A транзитивна, то есть для любых $s, s` \in S$ найдется подстановка $g \in G$, для которой $g(s) = s`$. Будем рассматривать только нетривиальные разбиение $\Pi = \{\Pi_k, k \in \{1, \ldots, L(\Pi)\}$ множества S со свойством C:

для любых $g \in G_A$ и k существует j, при котором $g(\Pi_k) \subseteq \Pi_j$.

Каждое такое разбиение, если оно существует, называется *системой блоков областей импримитивности* группы G, а группа называется импримитивной. В противном случае, когда не существует система блоков импримитивности группы, группа называется *импримитивной.* Пусть Π^* – множество всех систем блоков импримитивности транзитивной группы G автомата A. Будем говорить, что $\Pi = \{\Pi_k, k \in \{1, \ldots, L(\Pi)\}$ из Π^* не меньше $\Pi' = \{\Pi'_j, j \in \{1, \ldots, L(\Pi')\}$ из Π^*, если для любого j найдется k такое, что $\Pi'_j \subseteq \Pi_k$. Множество Π^* частично упорядочено и более того, несложно показывается , что оно является структурой. Обозначим через $\Pi^\beta = \{\Pi^\beta_k, k \in \{1, \ldots, L(\Pi^\beta)\}$ такое разбиение $\Pi^\beta \in \Pi^*$, при котором частичные функции выхода $(f_x)_{x \in X}$ автомата A постоянны на каждом множестве $\Pi^\beta_k \in \Pi^\beta$.

Покажите, что разбиение множества состояний S связного перестановочного автомата A на классы неотличимых состояний является максимальным элементом в совокупности вида Π^{β}. Если A неприведенный связный, перестановочный автомат, у которого не все частные функции выхода постоянны на множестве состояний S, то очевидно, что разбиение множества S на классы неотличимых состояний автомата A представляет собой максимальный элемент в совокупности разбиений, определяемых всеми системами областей импримитивности группы G_A, на которых частичные функции выхода постоянны. В частности, имеют место следующие утверждения.

Следствие 4. Связный перестановочный автомат A = (X, S, Y, h, f), у которого не все частичные функции выхода постоянны на множестве состояний S, не является приведенным автоматом тогда и только тогда, если его частичные функции выхода постоянны на блоках некоторой системы областей импримитивности группы G автомата A.

Следствие 5. Связный перестановочный автомат с примитивной группой, не все частичные функции выхода которого постоянны на множестве его состояний, является приведенным автоматом.

Пример 1. Пусть X = {0}, Y = {0, 1}, S = {1, 2, 3, 4, 5, 6}, $h_0 = \begin{pmatrix} 1\,2\,3\,4\,6 \\ 2\,3\,4\,5\,1 \end{pmatrix}$ – подстановка на S, λ – отображение S в Y, определенное равенствами:

$$\lambda(1) = \lambda(2) = \lambda(3) = 0;\ \lambda(4) = \lambda(5) = \lambda(6) = 1.$$

Данный автомат A = (X, S, Y, h_0, λ) является автономным связным перестановочным автоматом Мура. На основании следствий 2, 3 сказать что-либо о существовании различных неотличимых состояний данного автомата нельзя, так как $|S| = 6$ – не простое число и разбиение на классы 1-неотличимых состояний имеет вид:

$$N^1 = (N_1^1, N_2^1) = (\{1, 2, 3\}, \{4, 5, 6\}),$$

и следовательно $(|N_1^1|, |N_2^1|) = 3$.

Поэтому воспользуемся разбиением

$$N^2 = (N_1^2, N_2^2, N_3^2, N_4^2) = (\{1, 2\}, \{3\}, \{4, 5\}, \{6\})$$

Так как $(|N_1^2|, |N_2^2|) = (2, 1) = 1$, то на основании теоремы 4 заключаем, что данный автомат не имеет неотличимых различных состояний.

Пример 2. Пусть X = {0}, $S=V_n\backslash 0$ – векторное пространство размерности n над полем из двух элементов F_2 с исключенным нулевым вектором 0, Y = F_2, h_0 – полноцикловая подстановка множества

S, λ – равновероятная двоичная функция, определена на V_n. Тогда в силу утверждения следствия 3 автомат A = (X, S, Y, h_0, λ) является приведенным автоматом.

Пусть теперь A – произвольный перестановочный автомат, связные компоненты которого неотличимы. Будем считать, что A состоит из T>1 неотличимых связных компонент B_i, i∈[1, T]. Согласно теореме 3 классы неотличимых состояний каждого автомата B_i, i∈[1, T] имеют одинаковую мощность d_i. Описание мощностей классов неотличимых состояний рассматриваемого автомата дается приводимым ниже утверждением.

Теорема 5. Мощности классов неотличимых состояний перестановочного автомата A, состоящего из неотличимых связных компонент B_i, i∈[1, T], одинаковы и равны

$$d = \sum_{i=11}^{p} d_i,$$

где d_i – мощность классов неотличимых состояний связной компоненты B_i, i∈[1, T] автомата A.

Доказательство. Пусть s некоторое состояние автомата A. Построим класс состояний автомата A, неотличимых от s. Без ограничения общности доказательства предположим, что s принадлежит некоторому классу неотличимых состояний компоненты B(1), $s = s(1) \in {}^{B(1)}N_{s(1)}$. Компонента B(1) неотличима от компоненты B(i), i∈[2, T]. Следовательно, существует состояние $s(i) \in {}^{B(i)}N_{s(i)}$ компоненты B(i), i∈[2, T], неотличимое от s(1). В силу транзитивности отношения неотличимости состояний множество состояний $\bigcup_{i\in[1,T]} {}^{B(i)}N_{s(i)}$ является множеством состояний автомата A, неотличимых от s(1), мощности $\sum_{i=1}^{T} d_i$, так как множества ${}^{B(i)}N_{s(i)}$ принадлежат различным компонентам, и поэтому попарно не пересекаются. Остается теперь заметить, что любое состояние s автомата A, неотличимое от s_1 должно принадлежать одному из классов ${}^{B(i)}N_{s(i)}$, i∈[1, T]. Таким образом, утверждение теоремы 5 полностью доказано.

Прежде чем перейти к решению задачи о неотличимости связных перестановочных автоматов, сделаем одно полезное замечание и докажем ряд вспомогательных утверждений.

Замечание 2. Если классы k-неотличимых состояний автомата A(1) имеют вид ${}^{A(1)}N^k_i$, i∈[1, $l^{A(1)}{}_k$], классы k-неотличимых состояний автомата A(2) есть ${}^{A(2)}N^k_i$, i∈[1, $l^{A(2)}{}_k$], а s^1_i – представитель класса ${}^{A(1)}N^k_i$, s^2_j – представитель класса ${}^{A(2)}N^k_j$, то очевидно, что

k-неотличимость автоматов A(1), A(2) индуцирует взаимно однозначное соответствие μ_k между классами разбиений ${}^{A(1)}N^k$ и ${}^{A(2)}N^k$, а именно класс ${}^{A(1)}N^k_i$, $i\in[1, l^{A(1)}_k]$ автомата A(1) соответствует классу ${}^{A(2)}N^k_j$, $j\in[1, l^{A(2)}_k]$ при соответствии μ_k тогда и только тогда, если состояние s^1_i автомата A(1) k-неотличимо от состояния s^2_j автомата A(2). В этом случае, конечно, любое состояние из ${}^{A(1)}N^k_i$ автомата A(1) k-неотличимо от любого состояния из ${}^{A(2)}N^k_j$ автомата A(2). В силу изложенных соображений имеем

$$l^{A(1)}_k = l^{A(2)}_k,$$

если автоматы A(1) и A(2) k-неотличимы.

Теорема 6. Для неотличимости двух автоматов $A(1) = (X, S, Y, h^1, f^1)$, $A(2) = (X, S, Y, h^2, f^2)$ достаточна их $(\min(R_1, R_2)+1)$-неотличимость, где R_1, R_2 – степени различимости автоматов A(1), A(2) соответственно.

Доказательство. Пусть автоматы A(1) и A(2) m-неотличимы, $m = \min(R_1, R_2)+1$. Рассмотрим автомат A, состоящий из подавтоматов A(1) и A(2) (см. замечание 2). Согласно замечанию 2 классы m-неотличимых состояний автомата A имеют вид:

$${}^{A}N^m_t = {}^{A(1)}N^m_i \cup {}^{A(2)}N^m_j,\ i, j\in[1, l_m],\ l_m = l^{A(1)}_m = l^{A(2)}_m,\ t\in[1, l^{A}_m],$$

где j определяется биекцией μ_m: ${}^{A(1)}N^m_i \to {}^{A(2)}N^m_j$.

Теперь осталось показать, что $R_A \le m$, что в свою очередь следует из того, что на самом деле $R_A \le m-1$, так как очевидно, что

$${}^{A(1)}N^m_i = {}^{A(1)}N^{m-1}_i,\quad {}^{A(2)}N^m_j = {}^{A(2)}N^{m-1}_i,\ i, j\in[1, l_m].$$

Отметим, что примеры автономных регистров сдвига, а также и другие примеры показывают невозможность понижения оценки $\min(R_1, R_2) + 1$, данной в теореме 6.

Теорема 7. Степени различимости неотличимых автоматов равны.

Доказательство. Предположим, что для неотличимых автоматов A(1) и A(2) $R_1 > R_2$. Тогда вследствие замечания 2 имеем:

$$l^{A(1)}_{R_2} = l^{A(2)}_{R_2} = l^{A(2)}_{R_2+i} = l^{A(2)},\ i\in\{0, 1, \ldots\}.$$

Поэтому $l^{A(1)}_{R_2+i} = l^{A(2)}$, $i\in\{0, 1, \ldots\}$. Следовательно, $R_1\ge R_2$, что противоречит предположению. Из приведенных двух теорем вытекает следующее следствие.

Следствие 6. Степень различимости автомата A, состоящего из неотличимых подавтоматов A(1) и A(2), равны степеням различимости автоматов A(1) и A(2).

Сейчас мы имеем все необходимое для решения вопроса неотличимости связных перестановочных автоматов.

Теорема 8. Связные перестановочные автоматы B(1) и B(2) с множествами состояний S_1 и S_2 неотличимы тогда и только тогда, когда общий наибольший делитель мощностей всех классов k-неотличимых состояний автомата A $k \in [1, \max(|S_1|, |S_2|)]$, состоящего из подавтоматов B(2) и B(2), равен $d_1 + d_2$, где d_i – мощность класса неотличимых состояний автомата B(i) , $i \in \{1, 2\}$.

Доказательство. Пусть автоматы B(1) и B(2) неотличимы, тогда согласно теореме 5 мощность каждого класса неотличимых состояний автомата A, состоящего из неотличимых связных компонент B(1), B(2), равна $d_1 + d_2$. Из следствия 6 вытекает:

$$|{}^{A}N_i^R| = d_1 + d_2,\ i \in \{1, \ldots, l_R^A\},\ R = R_A = R_{B(1)} = R_{B(2)}.$$

И так как (см. теорему 1) $R_{B(1)} < |S_1|$, $R_{B(2)} < |S_2|$, то $R \le \min(|S_1| - 1, |S_2| - 1)$.

Теперь остается заметить, что каждый класс k-неотличимых состояний автомата A есть объединение некоторых непересекающихся классов (k+1)-неотличимых состояний, откуда и следует необходимость утверждения теоремы 8. Достаточность условий этой теоремы доказывается аналогично, при этом используется утверждение теоремы 6.

Замечание 3. Утверждение теоремы 8 позволяет судить о неотличимости или различимости двух перестановочных автоматов. Действительно, как нетрудно видеть, такие автоматы неотличимы тогда и только тогда, если для любой связной компоненты первого автомата существует неотличимая от нее связная компонента второго автомата и наоборот. Таким образом, считая этот перебор компонент автоматов выполнимым, утверждение теоремы 8 решает и эту более общую задачу.

Замечание 4. Методы и их применения при доказательствах сформулированных теорем позволяют решить еще одну задачу, стоящую в стороне от рассматриваемой здесь темы перестановочных автоматов, а именно проверить справедливость следующего утверждения.

Два приведенных автомата A_1 и A_2 с множествами состояний S_1, S_2 неотличимы тогда и только тогда, если общий наибольший

делитель мощностей классов k-неотличимых состояний $k \in \{1, \ldots, \max(|S_1|, |S_2|)\}$ автомата A, состоящего из подавтоматов A_1 и A_2, равен двум.

2.3. Гомоморфизмы автоматов

Определение 8. Гомоморфизмом по состояниям автомата A = = (X, S, Y, h, f) *в* автомат A’ = (X, S’, Y, h’, f’) называется отображение $\varphi: S \to S'$, для которого

$$\varphi h_x s = h'_x \varphi s, \; f_x s = f'_x \varphi s, \qquad (3)$$

для всех $x \in X$, $s \in S$.

Такое отображение φ называют так же внутренним гомоморфизмом (иногда – вложением A в A’). На образе φ(S) множества S определен подавтомат автомата A’. Этот подавтомат обозначают через φ(A) и называют образом автомата A. Если отображение φ в данном определении сюръективно, то говорят, что φ – гомоморфизм A *на* A’, в этом случае говорят так же, что φ – сюръективный внутренний гомоморфизм, а A’ называют образом A. Если φ – биекция, то φ называют (внутренним) изоморфизмом автоматов A, A’.

Условия (3) трактуют как коммутативность следующих диаграмм (рис. 4).

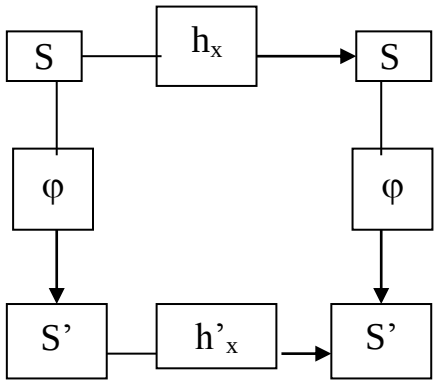

Рис. 4

Из равенств (3) легко получить равенства

$$\varphi h_P s = h'_P \varphi s, \; f_P s = f'_P \varphi s.$$

для всех $P \in X^*$, $s \in S$. Напомним, что $h_P = h_{x(k-1)} h_{x(k-1)} \ldots h_{x(1)}$ – отображение S→S, осуществляемое автоматом A в результате при-

ложения к нему входного слова P = x(1), x(2), ..., x(k); $f_P = f_{x(k)}\ h_{x(k-1)}\ h_{x(k-1)}\ \ldots h_{x(1)}$ – отображение S→Y, осуществляемое автоматом A в результате приложения к нему входного слова P = x(1), x(2), ..., x(k).

Важным следствием (внутреннего) гомоморфизма φ автомата A в A’ является выполнение следующей импликации: из равенства

$$A(s, P) = y_1, y_2, \ldots, y_k,\ \ s \in S,\ P \in X^*$$

следует

$$A'(\varphi s, P) = y_1, y_2, \ldots, y_k.$$

Дадим общее определение гомоморфизма.

Определение 9. *Гомоморфизмом автомата* A = (X, S, Y, h, f) *в* автомат A’ = (X’, S’, Y’, h’, f’) называется тройка отображений (ψ, φ, η). Отображения:

ψ: X→X’, φ: S→S’, η: Y→Y’ такие, что для любых x∈X, s∈S выполняются равенства

$$\varphi h_x s = h'_{\psi x}\varphi s,\ \ \eta f_x s = f'_{\psi x}\varphi s. \qquad (4)$$

Аналогично уточняющим определениям внутреннего гомоморфизма вводятся понятия гомоморфизма A *на* A’, то есть сюръективного гомоморфизма и изоморфизма (случай биективности отображения (ψ, φ, η)).

Условия (4) трактуют как коммутативность следующих диаграмм (рис. 5).

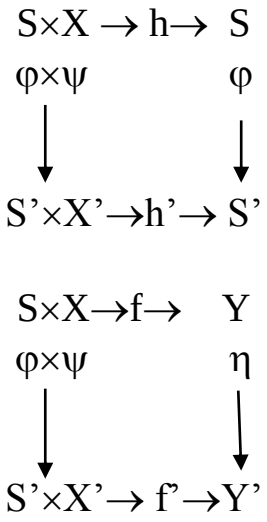

Рис. 5

Если ψ, η – тождественные отображения (X = X’, Y = Y’), то гомоморфизм превращается во *внутренний гомоморфизм*.

Изоморфные автоматы могут отличаться лишь в обозначениях элементов их алфавитов. Однако их практические реализации могут существенно различаться. Образом $A^{\psi,\varphi,\eta}$ автомата A при гомоморфизме (ψ,φ,η): $A \to A'$ называется подавтомат автомата A' с алфавитами $\psi(X)$, $\varphi(S)$, $\eta(Y)$. Вопросы практического использования гомоморфизмов автоматов отражены в [6].

Задача нахождения гомоморфных образов A' автомата A при гомоморфизме (ψ,φ,η) сводится к задаче определения образа внутреннего гомоморфизма φ: $A\eta \to \psi A'$.

Для вспомогательных автоматов:

$A\eta = (X, S, Y, h, \eta f)$, где $\eta fs = \eta(f(s))$;

$\psi A' = (X, S', Y', {}^{\psi}h', {}^{\psi}f')$, где ${}^{\psi}h'(s', x) = h'(s', \psi x)$, ${}^{\psi}f'(s', x) = f'(s', \psi x)$, $x \in X$, $s' \in S'$.

Задача же определения всех возможных гомоморфизмов (ψ, φ, η) автомата A может быть разбита на задачи:

1) определения неотличимых состояний некоторых вспомогательных автоматов;

2) нахождения автономных подавтоматов некоторых вспомогательных автоматов или, другими словами, неотличимости их входных слов.

Определение 10. Конгруэнцией автомата A называется тройка бинарных отношений эквивалентности $(\varepsilon, \delta, \chi)$ соответственно на множествах X, S, Y, для которых выполняется условие:

из $x \varepsilon x'$, $s \delta s'$ следует $(h_x s)\ \delta\ (h_{x'} s')$, $(f_x s)\ \chi\ (f_{x'} s')$.

При этом под внутренней конгруэнцией понимают конгруэнцию (E, δ, E), где E – бинарное отношение эквивалентности вида xEx для $x \in X$ и yEy для $y \in Y$, то есть бинарное отношение равенства. Из контекста всегда будет ясно, идет ли речь о внутреннем гомоморфизме, внутренней конгруэнции либо об общем случае гомоморфизма и конгруэнции. Каждой конгруэнции $(\varepsilon, \delta, \chi)$ естественным образом соответствуют разбиения R_X, R_S, R_Y множеств X, S, Y. Класс разбиения R_X содержащий $x \in X$ обозначим через [x], аналогично – [s] и [y] для R_S, и R_Y.

Определение 11. Фактор-автоматом $A/(\varepsilon,\delta,\chi)$ автомата A по конгруэнции $(\varepsilon, \delta, \chi)$ называется автомат

$$A/(\varepsilon,\delta,\chi) = (X/\varepsilon, S/\delta, Y/\chi, h', f'),$$

где $h'([x], [s]) = [h(x, s)]$, $x \in X$, $s \in S$.

Определение 12. Естественным гомоморфизмом γ автомата A на A / (ε, δ, χ) называется тройка отображений (ψ_ε, φ_δ, η_χ):

$$\psi_\varepsilon: x \Rightarrow [x],\ \varphi_\delta: s \Rightarrow [s],\ \eta_\chi: y \Rightarrow [y].$$

Легко проверяется, что (ψ_ε, φ_δ, η_χ) – гомоморфизм автомата A на A / (ε, δ, χ).

Гомоморфизму (ψ, φ, η) A на A’ соответствует конгруэнция (ε_ψ, δ_φ, χ_η) (иногда называемая ядром гомоморфизма (ψ, φ, η)):

$x \varepsilon_\psi x`$ тогда и только тогда, когда $\psi(x) = \psi(x`)$;

$s \delta_\varphi s`$ тогда и только тогда, когда $\varphi(s) = \varphi(s`)$;

$y \chi_\eta y`$ тогда и только тогда, когда $\eta(y) = \eta(y`)$.

Из приведенных фактов легко получить следующую важную теорему.

Теорема 9. Если (ψ, φ, η) – гомоморфизм автомата A на A’, то фактор-автомат A / (ε_ψ, δ_φ, χ_η) изоморфен A’ при изоморфизме $u = (u_X, u_S, u_Y)$:

$$u_X: [x] \Rightarrow \psi(x),\ u_S: [s] \Rightarrow \varphi(s),\ u_Y: [y] \Rightarrow \eta(y),$$

и гомоморфизм (ψ, φ, η) представляется суперпозицией отображений:

$$\psi = u_X \psi_\varepsilon,\ \varphi = u_S \varphi_\delta,\ \eta = u_Y \eta_\chi.$$

Иными словами, коммутативна диаграмма гомоморфизмов (рис. 6).

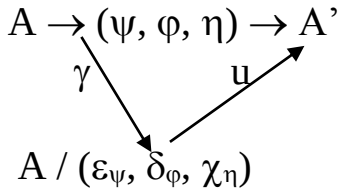

Рис. 6

Если (ψ, φ, η) – гомоморфизм автомата A в A’, то $u = (u_X, u_S, u_Y)$ – гомоморфизм A / (ε_ψ, δ_φ, χ_η) в A’ и сохраняется коммутативность приведенной диаграммы.

Из приведенной теоремы вытекает, что поиск всех гомоморфных образов автомата A можно проводить с помощью описаний всех его конгруэнций.

Определение 13. Автоморфизмом автомата A называют изоморфизм A на A.

Глава 3. НЕОТЛИЧИМОСТЬ ВХОДНЫХ СЛОВ АВТОМАТОВ

В этой главе исследуются вопросы автономности автоматов. Для перестановочных автоматов эти вопросы, во-первых, тесным образом связаны с исследованием степеней перестановочных автоматов, а во-вторых, как будет позднее показано, они играют немаловажную роль в неотличимости состояний и периодичности выходных последовательностей последовательных соединений перестановочных автоматов.

Для автомата мы используем обозначение $A = (X, S, Y, (h_x)_{x\in X}, (f_x)_{x\in X})$ или $A = (X, S, Y, h, f)$, где $h(x, s) = h_x(s)$ и $f(x, s) = f_x(s)$ для $x\in X$, $s\in S$. Ассоциированный с автоматом A автомат Медведева – это автомат $A_M = (X, S, Y = S, (h_x)_{x\in X}, (f_x = E_x)_{x\in X})$, где $E_x(s) = s$, $s\in S$. Ниже используются основные понятия автоматов: граф переходов автомата, неотличимость состояний, приведенная форма автомата, перестановочный автомат и т. д.

3.1. Автономность автоматов

Определение 1. Состояние s автомата A называется k-автономным (более точно – внешне k-автономным), если для любых входных k-грамм P и P' автомата A выполняется

$$A(s, P) = A(s, P').$$

Если состояние s автомата A k-автономно при любом k, то оно автономно (более точно внешне автономно).

Определение 2. Автомат A называется k-автономным (внешне k-автономным), если каждое его состояние k-автономно. Если автомат A k-автономен при любом k, то автомат автономен.

3.2. Степени перестановочных автоматов

N-й степенью автомата $A = (X, S, Y, (h_x)_{x\in X}, (f_x)_{x\in X})$ называется автомат $A^N = (X^N, S, Y, (h^N_{\bar{x}})_{\bar{x}\in X^N}, (f^N_{\bar{x}})_{\bar{x}\in X^N})$ с входным алфавитом X^N, множеством состояний S, выходным алфавитом Y, частичными функциями переходов $(h^N_{\bar{x}})_{\bar{x}\in X^N}$ и частичными функциями выхода $(f^N_{\bar{x}})_{\bar{x}\in X^N}$, определенными соотношениями:

$$h^N_{\bar{x}}(s) = h_{x_N} h_{x_{N-1}} \dots h_{x_1}(s);$$
$$f^N_{\bar{x}}(s) = f_{x_N} h_{x_{N-1}} \dots h_{x_1}(s),$$

где $s \in S$, $\bar{x} = x_1, x_2, \ldots, x_N \in X^N$.

В данном пункте изучаются вопросы связности степеней перестановочных автоматов. Изучение этих вопросов стимулируется использованием в ряде криптографических устройств узлов регулярной выборки, и зачастую их анализ сводится к анализу степеней некоторых автоматов. В частности, для определения мощностей классов неотличимых состояний перестановочного автомата A^N необходимо знать его области связности. В связи с этим определение связных компонент степеней данного автомата приобретает первостепенное значение.

Определение 3. Элементарным контуром графа переходов автомата A называется любой его контур, не содержащий одинаковых состояний.

Очевидно, что множество различных элементарных контуров графа переходов автомата A конечно. Обозначим через d_A наибольший общий делитель длин всех элементарных контуров. Формулируемые ниже утверждения, которые нам для единообразия удобно изложить на теоретико-автоматном языке, известны из теории конечных цепей Маркова.

Утверждение 1. Автомат A^N, представляющий собой N-ую степень сильно связного автомата A, является сильно связным автоматом тогда и только тогда, если $(d_A, N) = 1$.

(Докажите самостоятельно.)

Следствие утверждения 1. Все степени сильно связного автомата A сильно связны тогда и только тогда, если $d_A = 1$.

Предположим теперь, что $(d_A, N) = d \neq 1$. Сколько же областей связности имеет автомат A^N и каковы их мощности?

Ответ на этот вопрос для связных перестановочных автоматов дает следующее утверждение.

Утверждение 2. Пусть $A = (X, S, Y, (h_x)_{x \in X}, (f_x)_{x \in X})$ – связный перестановочный автомат и $(d_A, N) = d$. Тогда автомат A^N имеет d областей связности по $\frac{|S|}{d}$ состояний в каждой из них.

(Докажите самостоятельно.)

Теорема 1. Перестановочный связный автомат A внешне автономен тогда и только тогда, если его частичные функции выходов $(f_x)_{x \in X}$ равны и постоянны на областях связности его d_A-й степени.

Доказательству теоремы 1 предпошлем известное из теории цепей Маркова вспомогательное утверждение.

Лемма 1. Пусть s_1, s_2, s – произвольные состояния сильно связного автомата A. В графе переходов автомата A тогда и только тогда имеются пути из s в s_1 и из s в s_2 одинаковой длины, когда существует путь из s_1 в s_2 длины, кратной числу d_A.

Доказательство теоремы 1. Утверждение леммы 1 в применении к связному перестановочному автомату $A = (X, S, Y, (h_x)_{x\in X}, (f_x)_{x\in X})$ состоит в том, что данная пара состояний $s_1, s_2 \in S$ находится в одной области связности автомата A^{d_A} тогда и только тогда, если при любом состоянии $s\in S$ в графе переходов автомата A существуют пути из s в s_1 и из s в s_2 *одинаковой длины*. Следовательно, автономность автомата A равносильна тому, что частичные функции выхода равны и постоянны на областях связности автомата A^{d_A}.

Следствие 1. Мощности классов k-неотличимых состояний связного перестановочного внешне автономного автомата A=(X,S,Y,h,f) кратны числу $\frac{|S|}{d_A}$.

(Докажите самостоятельно.)

Следствие 2. Если для связного перестановочного внешне автономного автомата A = (X, S, Y, h, f)

$$d_A = 1,$$

то его частичные функции равны и постоянны на множестве состояний S.

Говорят, что автомат A = (X, S, Y, h, f) является *внутренне автономным (внутренне k-автономным)*, если ассоциированный с ним автомат Медведева $A_M = (X, S, h)$ внешне автономен (внешне k-автономен).

Пусть как обычно R_A – степень различимости автомата A. Приводимое ниже утверждение устанавливает критерий внешней автономности автомата A.

Теорема 2. Автомат A = (X, S, Y, h, f), являющийся внешне k-автономным автоматом при $k > R_A$, внешне автономен.

Доказательство. Пусть s – произвольное состояние автомата A, $x(1), x(2), \ldots, x(R+t+1)$; $x'(1), x'(2), \ldots, x'(R+t+1)$ – произвольная пара его входных слов, $R = R_A$, $t \geq 1$. Предположим, что A – внешне (R+t)-автономен. В этом случае очевидно, что состояния $h_{x(1)}s$, $h_{x'(1)}s$ будут (R+t–1)-неотличимыми, и следовательно, неотличимыми.

Используя R+t автономность автомата A и неотличимость указанных состояний, получаем:

$$f_{x(R+t+1)}h_{x(R+t)}...h_{x(2)}(h_{x(1)}(s)) = f_{x(R+t+1)}h_{x(R+t)}...h_{x(2)}(h_{x'(1)}(s)) = f_{x'(R+t+1)}h_{x'(R+t)}...h_{x'(2)}(h_{x'(1)}(s)).$$

Таким образом, показано, что из (R+t)-автономности автомата следует его (R+t+1)-автономность, $t \geq 1$, откуда и вытекает утверждение теоремы 2.

Замечание 1. Оценку R_A+1, данную в теореме 2, улучшить нельзя. Примерами R_A-автономных автоматов, не являющихся автономными, могут служить проходные линии задержки и регистры сдвига.

Теорема 3. Автомат Мура A = (X, S, Y, h, λ) внешне автономен тогда и только тогда, если его приведенная форма внутренне автономна.

Доказательство. Очевидно, автомат A внешне автономен тогда и только тогда, если внешне автономна его приведенная форма. В то же время ясно, что из внутренней автономности автомата Мура A следует его внешняя автономность (обратное же, вообще говоря, неверно). Поэтому для доказательства теоремы 3 достаточно показать, что из приведенности и внешней автономности автомата A = (X, S, Y, h, λ) вытекает его внутренняя автономность. При доказательстве теоремы 2, в частности, было показано, что состояния $h_x(s)$, $h_{x'}(s)$ при x, x'∈X и s∈S являются неотличимыми состояниями внешне автономного (внешне (R+t)-автономного) автомата A. Если теперь дополнительно предположить, что автомат A приведен, то получим $h_x(s) = h_{x'}(s)$, при любых x, x'∈X и s∈S, что равносильно внутренней автономности автомата A.

Обозначим через A(п) приведенную форму автомата A. Определим диаметр D_A автомата A как минимальное число k такое, что для любых двух вершин s, s' графа переходов автомата A, если s' достижимо из s, оно достижимо некоторым входным словом, длина которого не больше k.

Теорема 4. Если состояние s автомата A внешне k-автономно для k > D_A+$R_{A(п)}$, то оно внешне автономно.

Доказательство. Пусть имеется неотличимое от s состояние $\bar{s}$ автомата A(п). Рассмотрим граф переходов автомата $\tilde{A}$, определенного множеством достижимых из $\bar{s}$ состояний автомата A(п). При выполнении условий теоремы 4 автомат $\tilde{A}$ будет внешне (k–D_A)-автономным. Заметим, что $D_{\tilde{A}} \leq D_{A(n)}$ и $R_{\tilde{A}} \leq R_{A(n)}$, в связи с чем $k - D_{\tilde{A}} > R_{\tilde{A}}$. Согласно теореме 2 автомат $\tilde{A}$ – внешне автономен, или, то же самое, внешне автономно состояние s автомата A.

Определение 4. Степенью внешней автономности $P_A(s)$ состояния s автомата A = (X, S, Y, h, f) называется максимальное число k, если оно существует, при котором состояние s внешне k-автономно. В противном случае $P_A(s) = \infty$. Степенью внешней автономности P_A автомата A называется минимальное значение $P_A(s)$ по всем $s \in S$, если оно существует. В противном случае $P_A = \infty$.

Известно, что для любого автомата A = (X, S, Y, h, f) $D_{A(n)} \le D_A \le |S|-1$ и $R_{A(n)} = R_A \le |S|-1$. Поэтому из теорем 2, 4 непосредственно вытекают следующие утверждения.

Следствие 3. Для любого внешне неавтономного состояния s автомата A = (X, S, Y, h, f)

$$P_A(s) \le 2|S|-2.$$

Следствие 4. Для любого внешне неавтономного автомата A = (X, S, Y, h, f)

$$P_A \le |S|-1.$$

Приводимый ниже пример показывает, что данные оценки параметров $P_A(s)$, P_A достижимы.

Пример 1. Пусть X = {1, 2, ..., m}, m ≥ 2, S = $\{s^{(1)}, s^{(2)}, ..., s^{(|S|)}\}$, Y = {0,1}

$$h_x(s^{(j)}) = s^{(j+1)},\ x \in X,\ j \ne |S|,$$

$$h_1(s^{(|S|)}) = s^{(1)},\ h_x(s^{(|S|)}) = s^{(2)},\ x \in [2, m],$$

$$\lambda(s^{(|S|)}) = 1,\ \lambda(s^{(j)}) = 0,\ j \ne |S|.$$

Непосредственная проверка показывает, что состояние $s^{(1)}$ автомата A = (X, S, Y, h, λ) является внешне (2|S|–2)-автономным, но не внешне автономным. К тому же сам автомат A внешне (|S|–1)-автономен.

3.3. Псевдоавтономность перестановочных автоматов

Как в настоящем пункте, так и в следующем изучаются автоматы, в некотором смысле близкие к автономным автоматам, что обусловлено рядом факторов. Во-первых, как это будет показано далее, некоторые вопросы неотличимости состояний и периодичности последовательных соединений перестановочных автоматов сводятся к проверке той или иной «близости» данного автомата к внешне автономному автомату. Во-вторых, развитие этих вопросов дает конструктивные рекомендации к синтезу автоматов, абсолютно стойких

относительно частных классов методов определения их входных слов.

Обозначим через $P\left(y_1, y_2, \ldots, y_k / x(1), x(2), \ldots, x(k)\right)$ вероятность того, что при случайном и равновероятном выборе начального состояния $s \in S$ автомата A = (X, S, Y, h, f) и подаче на него входного слова x(1), x(2), …, x(k) автомат A выдает заданное выходное слово $y_1, y_2, \ldots, y_k$. Легко видеть, что

$$P\left(y_1, y_2, \ldots, y_k / x(1), x(2), \ldots, x(k)\right) = \frac{N_{y_1, \ldots, y_k}^{x(1), x(2), \ldots, x(k)}}{|S|},$$

где $N_{y_1, \ldots, y_k}^{x(1), \ldots, x(k)}$ – множество решений системы уравнений:

$$h_{x(1)}(s) = y_1,$$
$$f_{x(2)} h_{x(1)}(s) = y_2,$$
$$f_{x(k)} h_{x(k-1)} \ldots h_{x(1)}(s) = y_k.$$

Будем называть входные мультиграммы J, J' автомата A сравнимыми, если они имеют одинаковую длину.

Определение 5. Сравнимые входные мультиграммы J, J' автомата A = (X, S, Y, h, f) называют вероятностно неотличимыми, если $P\left(Q / J\right) = P\left(Q / J'\right)$ для любой сравнимой с J , J' выходной мультиграмме Q автомата A .

Определение 6. Сравнимые входные мультиграммы J, J' автомата A = (X, S, Y, h, f) называются A-неотличимыми (неотличимыми), если:

1) для любого $s \in S$ найдется $s' \in S$, при котором $A(s, J) = A(s', J')$;

2) для любого $s' \in S$ существует $s \in S$, при котором $A(s', J') = A(s, J)$.

Отметим, что отношение вероятностной неотличимости на множестве сравнимых входных мультиграмм автомата A представляет собой отношение эквивалентности. Тоже можно сказать и об отношении A-неотличимости сравнимых входных мультиграмм автомата A. Кроме того, легко проверить, что вероятностно неотличимые мультиграммы автомата A являются и A-неотличимыми мультиграммами.

Таким образом, изучая в дальнейшем лишь свойства A-неотличимых мультиграмм, мы тем самым получаем, в частности, информацию и о свойствах вероятностно неотличимых мультиграмм автомата A.

В дальнейшем нам потребуется некоторое обобщение понятия алгебраической независимости функций, определенных на некоторой алгебраической структуре.

Пусть $|Y|>1$, и $(\phi_i)_{i\in[1,k]}$, $\phi_i: S\to Y$ – некоторое семейство функций, определенных на S со значениями Y. Назовем функции $(\phi_i)_{i\in[1,k]}$ *зависимыми*, если существует такая отличная от константы функция $\psi(x_1,...,x_k)$, $\psi: Y^k\to Y$, и $y_0\in Y$, что $\psi(\phi_1(s),...,\phi_k(s))\equiv y_0$ при каждом $s\in S$. В противном случае эти функции назовем *независимыми*. Указанную выше функцию ψ будем называть соотношением в системе функций $(\phi_i)_{i\in[1,k]}$. Пусть $(\phi_i)_{i\in[1,k]}$ и $(\phi'_i)_{i\in[1,k]}$ – два набора функций, определенных на S со значениями в Y. Для каждого набора $y_1,...,y_k\in Y^k$ рассмотрим системы уравнений L и L' относительно неизвестных s, s' ∈ S:

$$L:\ \phi_i(s)=y_i,\ i\in[1,k]$$
$$L':\ \phi'_i(s)=y_i,\ i\in[1,k].$$

Лемма 2. Пусть при каждом наборе $y_1,...,y_k\in O^k$, при котором совместна система L, совместна и система L'. Тогда любое соотношение в системе функций $(\phi'_i)_{i\in[1,k]}$ имеется и в системе функций $(h_i)_{i\in[1,k]}$. Справедливо и обратное утверждение.

Доказательство. Докажем сначала прямое утверждение леммы. Обозначим через M_y^L $\left(M_y^{L'}\right)$ множество наборов $y_1,...,y_k\in Y^k$, при которых совместна система L (L'). Пусть $\Phi(x_1,...,x_k)$ – соотношение в системе функций $(h'_i)_{i\in[1,k]}$, то есть $\Phi(\phi'_1(s),...,\phi'_k(s))=y_0$, $y_0\in Y$ при любом $s\in S$. Последнее равносильно тому, что

$$\Phi(y_1,...,y_k)=y_0$$

для любого набора $y_1,...,y_k\in M_y^{L'}$. По условию $M_y^L\subseteq M_y^{L'}$, следовательно, $\Phi(\phi_1(s),...,\phi_k(s))=y_0$ при любом $s\in S$.

Докажем обратное утверждение леммы. Предположим, что имеется набор $y_1,...,y_k$, при котором система L совместна, а система L' – несовместна. Рассмотрим функцию $\Phi(x_1,...,x_k)$, Φ: $X^k\to Y$, значение которой равно $y'_0\in Y$ при $x_i=y_i$, $i\in[1,k]$, а на остальных наборах из Y^k она принимает значение $y_0\neq y'_0$. Такая функция существует, так как $|Y|>1$.

Очевидно, что $\Phi(\phi'_1(s),...,\phi'_k(s))=y_0$, $s\in S$ и $\Phi(y_1,...,y_k)=y'_0\neq y_0$ при указанном выше наборе $y_1,...,y_k$. То есть, Φ является соотношением в

системе $(\phi'_i)_{i\in[1,k]}$ и не является соотношением в системе $(\phi_i)_{i\in[1,k]}$. Полученное противоречие доказывает справедливость обратного утверждения леммы.

Для автомата $A=(X,S,Y,(h_x)_{x\in X},(f_x)_{x\in X})$ через A(J), A(J`), $J=i(1),...,i(k)$, $J'=i'(1),...,i'(k)$ соответственно обозначим системы функций:

$$f_{i(1)},\ f_{i(2)}h_{i(1)},\ \ldots,\ f_{i(k)}h_{i(k-1)},\ \ldots\ h_{i(1)},$$
$$f_{i`(1)},\ f_{i`(2)}h_{i`(1)},\ \ldots,\ f_{i`(k)}h_{i`(k-1)},\ \ldots h_{i`(1)}.$$

Через F(A(J)) и F(A(J`) обозначим множества соотношений в системах A(J) и A(J`) соответственно. Из леммы 2 и определения 6 непосредственно вытекает следствие.

Следствие 5. Сравнимые мультиграммы J, J' автомата $A=(X,S,Y,(h_x)_{x\in X},\ (f_x)_{x\in X})$ A-неотличимы тогда и только тогда, если

$$F(A(J)) = F(A(J`)).$$

Замечание 1. Предположим, что автомат $A=(X,S,Y,(h_x)_{x\in X},(f_x)_{x\in X})$ задается векторным автоматом вида: $S=V_n$ – векторное пространство над полем F_q из q элементов, $Y = F_q$. В этом случае множество F(A(J)) представляет собой множество всех алгебраических соотношений, имеющих место в системе функций A(J). Множество отображений $V_n \to F_q$ можно рассматривать как алгебру над F_q размерности q^n. Поэтому корректно говорить о множестве линейных $\tilde{F}(A(J))$-соотношений системы функций A(J).

Если системы A(J) и A(J`) состоят из линейных функций, то справедливо следующее уточнение следствия 5: условие

$$\tilde{F}(A(J)) = \tilde{F}(A(J`)).$$

равносильно A-неотличимости мультиграмм J, J' автомата A. Действительно, можно показать, что приведенное равенство равносильно равенству F(A(J)) = F(A(J`)).

Определение 7. Автомат A называется вероятностно k-автономным (псевдо k-автономным), если его любая пара входных k-грамм вероятностно неотличима (A-неотличима).

Определение 8. Автомат A называется вероятностно автономным (псевдоавтономным), если он вероятностно k-автономен (псевдо k-автономен) при любом k.

Очевидно, что вероятностно автономный (вероятностно k-автономный) автомат является и псевдоавтономным (псевдо k-автономным) при любом k.

Пусть $(\phi_i)_{i\in[1,k]}$ – некоторое семейство отображений S в Y. Будем говорить, что *функция* ψ: S→Y *определена* семейством $(\phi_i)_{i\in[1,k]}$, если для любого набора $y_1, y_2, \ldots, y_k, y_{k+1}\in Y^{k+1}$, при котором система уравнений

$$\varphi_i(s) = y_i,\ i\in\{1, \ldots, k\},$$
$$\psi(s) = y_{k+1}$$

совместна, множество решений ее совпадает с множеством решений ее подсистемы $\varphi_i(s) = y_i,\ i\in\{1, \ldots, k\}$.

Очевидно, что если ψ: S→Y определена семейством $(\phi_i)_{i\in[1,k]}$, то функции $\psi, \varphi_1, \varphi_2, \ldots, \varphi_k$ зависимы (обратное, вообще говоря, неверно). Для произвольного отображения Φ: $Y^k\to Y$ и семейства функций $(\phi_i)_{i\in[1,k]}$ φ_i: S→Y рассмотрим отображение $\Phi(\phi_1,\ldots,\phi_k): S\to Y$, положив $\Phi(\phi_1,\ldots,\phi_k): s\mapsto\Phi(\phi_1(s),\ldots,\phi_k(s))$.

Это отображение будет называть отображением, *индуцированным функциями* Φ и $(\phi_i)_{i\in[1,k]}$.

Лемма 3. Функция ψ определена системой функций $(\phi_i)_{i\in[1,k]}$ тогда и только тогда, если она совпадает с отображением индуцированным некоторой функцией Φ: $Y^k\to Y$ и системой функций $(\phi_i)_{i\in[1,k]}$.

Доказательство. Достаточность условий леммы очевидна. Докажем их необходимость. Пусть ψ определена системой $(\phi_i)_{i\in[1,k]}$. Обозначим через M_y множество наборов, $y_1, y_2, \ldots, y_k, y_{k+1}\in Y^{k+1}$, для которых совместна система уравнений:

$$\varphi_i(s) = y_i,\ i\in\{1, \ldots, k\},$$
$$\psi(s) = y_{k+1}.$$

Определим отображение Φ: $Y^k\to Y$, положив $\Phi(y_1, y_2, \ldots, y_k) = y_{k+1}$ для всех $y_1, y_2, \ldots, y_k, y_{k+1}\in M_y$. Это можно сделать, так как функция ψ определена системой функций $(\phi_i)_{i\in[1,k]}$. На других наборах (на наборах, не входящих в M_y) определим функцию Φ произвольным образом. Отображение $\Phi(\phi_1,\ldots,\phi_k)$, индуцированное функциями Φ, $(\phi_i)_{i\in[1,k]}$, совпадает с отображением ψ, так как по построению

$$\Phi(\phi_1(s),\ldots,\phi_k(s)) = \psi(s)$$

при любом $s\in S$.

Для автомата $A=(X,S,Y,(h_x)_{x\in X},(f_x)_{x\in X})$ обозначим через H = H(A) минимальное k, при котором найдется такое его входное слово x(1), x(2), …, x(k), что функция $f_{x(k)}h_{x(k-1)}...h_{x(1)}$ определена системой функций $f_{x(1)}$, $f_{x(2)}h_{x(1)}$, …, $f_{x(k-1)}h_{x(k-2)}\ldots h_{x(1)}$, то есть нашлась функция Φ, при которой

$$f_{x(k)}h_{x(k-1)}...h_{x(1)} = \Phi(f_{x(1)}, f_{x(2)}h_{x(1)}, \ldots, f_{x(k-1)}h_{x(k-2)}\ldots h_{x(1)}).$$

Лемма 4. Перестановочный псевдо k-автономный автомат $A=(X,S,Y,(h_x)_{x\in X}, (f_x)_{x\in X})$ при k ≥ H(A) k-автономен.

Доказательство. Можно считать, что |Y|>1, так как в противном случае автомат A автономен (внешне автономен).

По условию, существует входная мультиграмма x`(1), …, x`(H) H = H(A) автомата A, при которой

$$f_{x`(k)}h_{x`(k-1)}...h_{x`(1)} = \Phi`(f_{x`(1)}, f_{x`(2)}h_{x`(1)}, \ldots, f_{x`(k-1)}h_{x`(k-2)}\ldots h_{x`(1)}).$$

Легко показывается, что при k>H для любых слов x”(1), x”(2), …, x”(k–H) длины k–H выполняется равенство:

$$f_{x`(k)}h_{x`(k-1)}...h_{x`(1)}h_{x"(k-H)...}h_{x"(1)} =$$

$$= \Phi`(f_{x`(1)}h_{x"(k-H)}, h_{x"(k-H-1)}, \ldots, h_{x"(1)}, \ldots, f_{x`(k-1)}h_{x`(k-2)}\ldots h_{x`(1)}h_{x"(k-H)}, h_{x"(k-H-1)}, \ldots, h_{x"(1)}).$$

То есть существует мультиграмма x(1), …, x(k) и функция Φ, для которых $f_{x(k)}h_{x(k-1)}, \ldots, h_{x(1)} = \Phi(f_{x(1)}, f_{x(2)}h_{x(1)}, \ldots, f_{x(k-1)}h_{x(k-2)}\ldots h_{x(1)})$

Это выражение можно считать соотношением в системе функций $A(x(1), \ldots, x(k)) = (f_{x(1)}, f_{x(2)}h_{x(1)}, \ldots, f_{x(k)}h_{x(k-1)}\ldots h_{x(1)})$.

Так как автомат A псевдо k-автономен, то же соотношение справедливо для системы функций:

$$(f_{x(1)}, f_{x(2)}h_{x(1)}, \ldots, f_{x`(k)}h_{x(k-1)}\ldots h_{x(1)})$$

$$f_{x`(k)}h_{x(k-1)}, \ldots, h_{x(1)} = \Phi(f_{x(1)}, f_{x(2)}h_{x(1)}, \ldots, f_{x(k-1)}h_{x(k-2)}\ldots h_{x(1)})$$

при любом x`(k)∈X. Отсюда с использованием леммы 3 легко получить равенство отображений $f_{\mathbf{x`(k)}}h_{x(k-1)}, \ldots, h_{x(1)} = f_{\mathbf{x(k)}}h_{x(k-1)}, \ldots, h_{x(1)}$ при любом x`(k)∈X. Учитывая перестановочность автомата A, получаем

$$f_x = f_{x`} = \lambda$$

для любых x`, x∈X. Теперь мы имеем право переписать рассматриваемое первое соотношение в виде:

$$\lambda h_{x(k-1)}, \ldots, h_{x(1)} = \Phi(\lambda, \lambda h_{x(1)}, \ldots, \lambda h_{x(k-2)}\ldots h_{x(1)}).$$

Это соотношение вследствие псевдо k-автономности автомата A имеет место и в системе функций $(\lambda, \lambda h_{x(1)}, \ldots, \lambda h_{\mathbf{x`(k-1)}}h_{x(k-2)}\ldots h_{x(1)})$, то есть

$$\lambda h_{x`(k-1)}h_{x(k-2)}\ldots h_{x(1)} = \Phi(\lambda, \lambda h_{x(1)}, \ldots, \lambda h_{x(k-2)}\ldots h_{x(1)}).$$

при любом $x`(k-1)\in X$. Следовательно, $\lambda h_{x`(k-1)}h_{x(k-2)}\ldots h_{x(1)} = \lambda h_{x(k-1)}h_{x(k-2)}\ldots h_{x(1)}$ при любом $x`(k-1)\in X$. В частности, в силу перестановочности автомата A, имеем $\lambda h_{x`} = \lambda h_x$, для любого $x`\in X$. Продолжив аналогичным образом рассуждения, получим:

$$f_{x(1)} = f_{x`(1)};$$
$$f_{x(2)}h_{x(1)} = f_{x`(2)}h_{x`(1)};$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$
$$f_{x(k)}h_{x(k-1)}\ldots h_{x(1)} = f_{x`(k)}h_{x`(k-1)}\ldots h_{x`(1)}$$

при любых входных k-граммах x(1)x(2), …, x(k), x`(1)x`(2), …, x`(k) автомата A. Лемма полностью доказана.

Лемма 5. При $k\geq H(A)$ k-автономный автомат A автономен.

Доказательство. Легко видеть, что степень различимости k-автономного автомата A при $k\geq H(A)$ равна $H(A)-1$. Поэтому утверждение леммы 5 непосредственно вытекает из теоремы 2.

Объединим утверждение лемм 4 и 5 в общую теорему.

Теорема 5. Перестановочный псевдо k-автономный автомат при $k\geq H(A)$ автономен.

Определение 8. Степенью псевдоавтономности $Q_A^{ПС}$ (степенью вероятностной автономности Q_A^{BEP}) автомата A называется максимальное число k, если оно существует, при котором автомат A псевдо k-автономен (вероятностно k-автономен). В противном случае, $Q_A^{ПС} = \infty$ ($Q_A^{BEP} = \infty$).

Очевидно, что $Q_A^{BEP} \leq Q_A^{ПС}$. Из теоремы 5 вытекает, что для неавтономного перестановочного автомата A

$$Q_A^{BEP} \leq Q_A^{ПС} < H(A).$$

Пусть $(\phi_i)_{i\in\{1,\ldots,k\}}$ – семейство отображений множества S в множество Y и $L(y_1, \ldots, y_m)$ – множество решений системы уравнений:

$$\begin{aligned}\phi_1(s) &= y_1\\ \phi_2(s) &= y_2\\ &\ldots\ldots\ldots\ldots,\\ \phi_m(s) &= y_m\end{aligned}$$

где $m\in\{1, \ldots, k\}$, $y_j\in Y$, $j\in\{1, ..., m\}$.

Ограничимся рассмотрением лишь наборов $y_1,\ldots,y_m$, при которых данная система совместна. Обозначим через Z_m множество всех $L(y_1, \ldots, y_m)$. Очевидно, что функция ϕ_m определена семейством

функций $(\phi_i)_{i\in\{1,\dots,m-1\}}$ тогда и только тогда, если множество Z_{m-1} совпадает с Z_m. Поэтому для любого автомата $A=(X,S,Y,(h_x)_{x\in X},(f_x)_{x\in X})$

H(A)≤|S|+1, если A – автомат Мили;

H(A)≤|S|, если A – автомат Мура.

Этот факт совместно с теоремой 5 дает следующее утверждение.

Теорема 6. Для любого перестановочного неавтономного автомата $A=(X,S,Y,\ (h_x)_{x\in X},(f_x)_{x\in X})$

$Q_A^{BEP} \le Q_A^{ПС} \le |S|$, если A – автомата Мили;

$Q_A^{BEP} \le Q_A^{ПС} \le |S|-1$, если A – автомат Мура.

Автомат $A=(X,S,Y,(h_x)_{x\in X},(f_x)_{x\in X})$ называется векторным, если $S = V_n$ – векторное пространство размерности n над полем F_q из q элементов, а $Y= F_q$. Векторный автомат называется линейным, если $(h_x)_{x\in X},(f_x)_{x\in X}$ – линейные отображения.

Следствие 6. Для любого векторного перестановочного неавтономного автомата $A=(X,S,Y,(h_x)_{x\in X},(f_x)_{x\in X})$ = $(X, V_n, F_q, (h_x)_{x\in X}, (f_x)_{x\in X})$

$$Q_A^{BEP} \le Q_A^{ПС} \le q^n.$$

Доказательство. Это утверждение непосредственно вытекает из теоремы 6, тем не менее мы докажем его иным способом. Для произвольной входной последовательности J = x(1), …, x(k), k = $= q^n+1$ семейство отображений A(J) линейно зависимо в множестве всех отображений $V_n \to F_q$, так как размерность этого векторного пространства равна q^n. Поэтому $H(A) \le q^n +1$ и по теореме 5 автомата A будет автономным.

Аналогичным образом доказывается следующее следствие.

Следствие 7. Для любого линейного перестановочного неавтономного автомата $A=(X,S,Y,(h_x)_{x\in X},(f_x)_{x\in X})$ = $(X, V_n, F_q, (h_x)_{x\in X}, (f_x)_{x\in X})$

$$Q_A^{BEP} \le Q_A^{ПС} \le n.$$

Следующий пример доказывает достижение данных в теореме 6 степени псевдоавтономности и степени вероятностной автономности перестановочного неавтономного автомата Мура.

Пример 2. Положим для автомата A:

$$X=Y=\{0,1\},\ S=\{s^{(1)},s^{(2)},\dots,s^{(|S|)}\};$$
$$h_x(s^{(j)})=s^{(j+1)},\ j\ne|S|,\ j\ne 1,\ x\in X;$$
$$h_0(s^{(1)})=s^{(1)},\ h_0(s^{(|S|)})=s^{(2)},\ h_1(s^{(1)})=s^{(2)},\ h_1(s^{(|S|)})=s^{(1)};$$
$$\lambda(s^{(|S|)})=1,\ \lambda(s^{(j)})=0,\ j\in\{1,\dots,|S|-1\}.$$

Легко доказываются следующие свойства автомата A:

– A – перестановочный автомат;

– A – неавтономный автомат;

– множество всех различных выходных (|S|–1)-грамм автомата A состоит из наборов: набор сплошь из нулей и наборы с одной единицей на L-м месте, где $L+1 \in \{1, \ldots, |S|-1\}$;

– $A(s^{(1)}, J) = 0, \ldots, 0$, $A(s(|S|-L),J)=0, \ldots, 0, 1, 0, \ldots, 0$, где 1 стоит на L+1 месте, $L \in \{0, \ldots, |S|-2\}$ при любой входной (|S|–1)-грамме J автомата A.

Таким образом, автомат A является вероятностно (|S|–1)-автономным.

3.4. Слабая автономность автоматов

При изучении периодов выходных последовательностей автомата при заданной периодической входной последовательности большое значение имеет следующие обобщения понятия автономности автомата.

Определение 10. Сравнимые входные слова $P_1, P_2, \ldots, P_к$ автомата $A = (X, S, У, h, f)$ называются слабо неотличимыми относительно A (или кратко – слабо неотличимыми), если найдутся состояния $s_1, s_2, \ldots, s_к$ из S, при которых

$$A(s_1, P_1) = A(s_2, P_2) = \ldots = A(s_к, P_к).$$

В противном случае слова $P_1, P_2, \ldots, P_к$ называются сильно различимыми относительно A (сильно различимыми).

Определение 11. Автомат A называется слабо k-автономным, если все его входные слова длины k слабо неотличимы (относительно A).

Определение 12. Степенью слабой автономности $\sigma(A)$ автомата A называется максимальное число k, если оно существует, при котором он слабо k-автономен. В противном случае полагаем $\sigma(A) = \infty$.

Целью настоящего раздела является выяснение связей понятий слабой к-автономности автомата и его к-автономности, то есть независимости выходной последовательности автомата от его входных последовательностей длины к. Отметим, что слабая к-автономность автомата A равносильна слабой автономности его приведенной формы, в связи с чем исследование слабо к-автономных автоматов можно проводить, ограничиваясь рассмотрением приведенных автоматов.

Для автомата A = (X, S, У, h, f) через h(s, x(1), …, x(к)) обозначим заключительное состояние автомата A с начальным состоянием s при входном слове x(1), …, x(к), то есть h(s, x(1), …, x(к)) = $= h_{x(к)}h_{x(к-1)}\ldots h_{x(1)}s$. Напомним, что входная последовательность P = x(1), …, x(к) автомата A = (X, S, У, h ,f) называется *установочной* (для A), если из условия A(s, P) = A(s`, P), s, s`∈S вытекает

$$h(s, P) = h(s`, P).$$

Отметим, что для приведенных автоматов всегда существуют установочные последовательности. Обозначим через $L(A)_{уст}$ длину минимальной установочной последовательности для приведенной формы A/~ автомата A.

Лемма 6. Слабо к-автономный автомат A при $к > L(A)_{уст}$ имеет $(к–L(A)_{уст})$-автономное состояние.

Доказательство. Без ограничения общности будем считать, что A = A/~. Пусть A слабо к-автономен, к>L, $L(A)_{уст} = L$. Это означает, что найдутся состояния $s_P∈S$, $P∈X^к$ и его выходное слово $y_1, y_2, \ldots, y_к$, при которых $A(s_P, P)= y_1, y_2, \ldots, y_к$ для всех $P∈X^к$. В частности, для установочной последовательности $Q∈X^L$ и произвольных слов $U∈X^{к–L}$ имеем

$$A(s_{QU}, QU) = y_1, y_2, \ldots, y_к , U∈X^{к–L} \qquad (5)$$

(QU – конкатенация слов, слово Q – начало слова QU).

Так как Q – установочная последовательность для A, то найдется s∈S, при котором $h(s_{QU},Q) = s$ при всех $U∈X^{к–L}$. Из последних равенств и равенств (5) вытекает

$$A(s,U) = y_{L+1}, y_{L+2}, \ldots, y_к$$

при всех $U∈X^{к-L}$, то есть состояние s (к–L)-автономно.

Обозначим через D(A) – диаметр автомата A, а через R(A) – его степень различимости.

Теорема 7. Слабо к-автономный автомат при $к ≥ L(A)_{уст} + D(A) + R(A) + 1$ имеет автономное состояние.

Доказательство. По лемме 6 автомат имеет $(к–L(A)_{уст})$ – автономное состояние s∈S. Из условий теоремы следует $k` = (к–L(A)_{уст}), (к–L(A)_{уст}) ≥ D(A) + R(A) + 1$. Несложно доказывается, что каждое состояние, достижимое из s, является по крайней мере (R(A)+1)-автономным. Для доказательства теоремы достаточно доказать, что автомат A(s), порожденный состоянием s, является автономным, а это следует из приводимой ниже леммы.

Лемма 7. Если автомат A к-автономен при к≥R(A)+1, то он автономен.

Доказательство. Пусть s – произвольное состояние автомата A, x(1), x(2), …, x(R+t+1); x`(1), x`(2), …, x`(R+t+1), R = R(A), $t \geq 1$ – произвольная пара его входных слов. Предположим, что A (R+t)-автономен при некотором натуральном t. В этом случае очевидно, что состояния h(s, x(1)), h(s, x`(1)) будут (R+t–1)-неотличимы и, следовательно, неотличимы. Используя (R+t)-автономность автомата A и неотличимость указанных состояний, получаем

$$f_{x(R+t+1)}h_{x(R+t)}\ldots h_{x(2)}(h_{\mathbf{x(1)}}s) = f_{x(R+t+1)}h_{x(R+t)}\ldots h_{x(2)}(h_{\mathbf{x`(1)}}s) = f_{x`(R+t+1)}h_{x`(R+t)}\ldots h_{x`(2)}h_{x`(1)}s.$$

Таким образом, доказано, что из (R+t)-автономности автомата A следует его (R+t+1)-автономность, $t \geq 1$, откуда и вытекает утверждение леммы. Утверждение теоремы 7 доказано.

Несложно доказать, что автомат Мура автономен тогда и только тогда, если его приведенная форма внутренне автономна, то есть для любого $s \in S$

$$h_{x(k)}\ldots h_{x(2)}h_{x(1)}s = h_{x`(k)}\ldots h_{x`(2)}h_{x`(1)}s$$

при любых сравнимых словах x(1), …, x(k), x`(1), …, x`(k) из X*.

Следствие 7. Слабо к-автономный сильно связный автомат при

к>$L(A)_{уст}$ +D(A)+R(A)+1

автономен.

В работе [41] Т. Х. Хиббардом показано, что для любого приведенного автомата Мили

$$L(A)_{уст} \leq \frac{|S|(|S|-1)}{2},$$

а для приведенных автоматов Мура

$$L(A)_{уст} \leq \frac{|S|(|S|-1)}{2} - |S|+2,$$

причем эти оценки как функции от числа состояний |S| не могут быть понижены. Известно также [41; 33], что для любого автомата A

$$D(A) \leq |S|-1.$$

Поэтому справедливо следствие 8.

Следствие 8. Для автоматов A, не имеющих автономных состояний,

$\sigma(A) \leq \frac{|S|^2}{2} + \frac{3|S|}{2} - 2$, если A – автомат Мили;

$\sigma(A) \leq \frac{|S|^2}{2} + \frac{|S|}{2}$, если A – автомат Мура.

Следующие примеры показывают, что для автоматов Мили приведенная оценка достижима, а для автоматов Мура – почти достижима.

Пример 3. Пусть $X = \{1, \ldots, |S|\}$, $S = \{s^{(1)}, s^{(2)}, \ldots, s^{(|S|)}\}$, $Y = \{0,1\}$; $h_x s^{(x)} = s^{(x+1)}$, $x \neq |S|$; $h_{|S|} s^{(|S|)} = s^{(|S|)}$; $h_x s^{(x+1)} = s^{(x)}$, $x \neq |S|$; $h_x s^{(j)} = s^{(j)}$, $x \neq j$, $j \neq x+1$, то

$$f_x s^{(j)} = 1 \text{ при } x = j = |S|,$$
$$f_x s^{(j)} = 0 \text{ в противном случае.}$$

Введенный автомат $A = (X, S, Y, h, f)$ является перестановочным автоматом, кроме того, он не имеет автономных состояний. Покажем, что автомат A слабо к-автономен при $к = \frac{|S|^2}{2} + \frac{|S|}{2} - 1$. Пусть слово $P = x(1), x(2), \ldots, x(к)$ таково, что $A(s(x), P) \neq 0$ (не является словом, состоящим сплошь из нулей) для всех $s^{(x)}$ из S. Для каждой пары (i, j) при $1 \leq i \leq j \leq |S|$ очевидно, что найдется целое число $L = L(i, j)$, $1 \leq L \leq к$, при котором

$$h_{x(L-1)} h_{x(L-2)} \ldots h_{x(1)} s^{(i)} = s^{(j)} \text{ и } x(L) = j.$$

Здесь мы положили $h_{x(0)} s^{(i)} = s^{(i)}$. Для различных пар (i, j), (i`, j`) величины L(i, j), L(i`, j`) различны. Действительно, если L(i, j) = L(i`, j`), то j = i(L(i, j)) = i`(L(i`,j`)) = j`. Поэтому (в силу перестановочности автомата A) и i = i`, j = j`. Таким образом, число различных чисел L(i, j) совпадает с числом различных пар (i, j), $1 \leq i \leq j \leq |S|$, которое очевидно равно $\frac{|S|^2}{2} + \frac{|S|}{2}$.

Учитывая, что $L(i, j) \leq к$, имеем $к \geq \frac{|S|^2}{2} + \frac{|S|}{2}$.

Из этой оценки непосредственно вытекает, что для любой последовательности P длины меньшей, чем $\frac{|S|^2}{2} + \frac{|S|}{2}$, найдется состояние $s^{(i)} \in S$ автомата A, при котором $A(s^{(i)}, P)$ есть последовательность, состоящая из нулей. То есть автомат A оказывается по крайней мере слабо к-автономным при

$$к = \frac{|S|^2}{2} + \frac{|S|}{2} - 1.$$

Пример 4. Положим $X = \{1, 2, \ldots, |S|\}$, а S, Y и частичные функции переходов $(h_x)_{x \in X}$ определим, как и в примере 1. Кроме того, примем $f_x = \lambda$ для всех $x \in X$. Рассматриваемый автомат A является перестановочным автоматом Мура, без автономных состояний. Аналогично показывается, что автомат A является слабо к-автономным для

$$к = \frac{|S|^2}{2} - \frac{|S|}{2}.$$

Отличие доказательства состоит в том, что множество чисел вида L(i, j) необходимо рассматривать при $1 \le i \le j \le |S|-1$. Число таких пар (i, j) равно $\frac{|S|^2}{2} - \frac{|S|}{2}$. Поэтому $к \ge \frac{|S|^2}{2} - \frac{|S|}{2} + 1$ и, следовательно,

$$\sigma(A) \ge \frac{|S|^2}{2} - \frac{|S|}{2}.$$

Пример 5. Как видно из приведенных общих утверждений оценки параметра $\sigma(A)$ слабой автономности автоматов в классе автоматов без автономных состояний не могут быть существенно улучшены, например, по порядку. Поэтому естественно возникает вопрос, нельзя ли в общем случае оценку $\sigma(A)$ существенно понизить, если искать ее для почти всех автоматов. Из приведенных результатов и результатов работ [21; 23] по оценкам диаметра D(A), степени различимости R(A) и длины $L(A)_{уст}$ установочного эксперимента следует, что для почти всех приведенных автоматов A = (X, S, У, h, f_x), $|X| \ge 2$, $|У| \ge 2$ без автономных состояний

$$\sigma(A) \le 5\log_{|Y|}|S| + \frac{1}{6}\log_{|X|}|S|.$$

Ниже мы уточним утверждение следствия 8 для некоторых классов автоматов. Пусть A = (X, $V_n(q)\backslash 0$, F_q, $(B_x)_{x\in X}$, $(C_x)_{x\in X}$) – линейный автомат с входным алфавитом X, множеством состояний $V_n(q)\backslash 0$, являющимся векторным пространством $V_n(q)$ над полем F_q с исключенным нулевым вектором, выходным алфавитом F_q, частичными функциями переходов $(B_x)_{x\in X}$, являющимися линейными преобразованиями векторного пространства $V_n(q)$, частичными функциями выхода $(C_x)_{x\in X}$, осуществляющими линейные отображения $V_n(q)$ в F_q.

Лемма 8. Если $s \in V_n(q)\backslash 0$ к-автономное состояние, $к \ge 2n$ автомата A = (X, $V_n(q)\backslash 0$, F_q, $(B_x)_{x\in X}$, $(C_x)_{x\in X}$), то оно автономно.

Доказательство. Рассмотрим систему (CB(j)) векторов:

$$\begin{aligned} &s,\\ &\{B_{x(1)}s\colon x(1)\in X\},\\ &\{B_{x(2)}B_{x(1)}s;\ x(2)x(1)\in X^2\},\\ &\ldots\ldots\ldots\ldots\ldots\ldots\qquad (CB(j))\\ &\{B_{x(j)}\ldots B_{x(1)}s;\ x(j)\ldots x(1)\in X^j\}, \end{aligned}$$

ранг которой будем обозначать через r(j).

Легко видеть, что $1 \le r_1 \le r_2 \le \ldots \le r_j \le r_{j+1} \ldots$, кроме того, из $r_j = r_{j+1}$ для некоторого j следует $r_j = r_{j+к}$ при любом $к \ge 0$. Поэтому $r_{n-1} = r_n \le n$.

Выберем в системе СВ(n–1) $r = r_{n-1}$ линейно независимых векторов: $s, s_1, s_2, \ldots, s_{r-1}$. Если теперь предположить, что состояние s к-автономно, $к \ge 2n$, то, очевидно, должны быть (к–n+1)-автономными состояния $s, s_1, s_2, \ldots, s_{r-1}$. Использовав свойство линейности автомата заключаем, что все достижимые из s состояния автомата A (к–n+1)-автономны. Так, (к-n+1)-автономен автомат A(s), порожденный состоянием s. Так как степень различимости R(A) любого линейного A не превосходит его размерности n, то степень различимости R(A(s)) его подавтомата A(s) не превосходит n. Итак A(s) (к–n+1)-автономен, $к \ge 2n$ и $R(A(s)) \le n$. Следовательно, A(s) К-автономен при некотором $К \ge R(A(s))+1$. Теперь несложно доказывается, что из этого факта следует автономность состояния s автомата линейного автомата A.

Напомним, что *диагностической последовательностью* произвольного автомата (X, S, У, h, f) называется любое его входное слово P (если оно существует), при котором из условия A(s, P) = = A(s`, P), $s, s` \in S$ вытекает

$$s = s`.$$

Отметим, что диагностическая последовательность автомата является одновременно и установочной. Обозначим через $L(A)_{диаг}$ минимальную длину диагностической последовательности для автомата A.

Пример 6. Легко доказывается, что входное слово x(1), x(2), …, x(к) линейного автомата

$$A = (X, Vn(q)\backslash 0, F_q, (B_x)_{x \in X}, (C_x)_{x \in X})$$

является диагностическим, тогда и только тогда, когда ранг системы $C_{x(1)}, C_{x(2)}B_{x(1)}, \ldots, C_{x(к)}B_{x(к-1)})\ldots B_{x(1)}$ линейных функций равен n.

Теорема 8. Пусть $A = (X, V_n(q)\backslash 0, F_q, (B_x)_{x \in X}, (C_x)_{x \in X})$ – линейный автомат без автономных состояний и $L(A)_{диаг} = n$.

Тогда $\sigma(A) \le 3n-1$.

Доказательство. Если выполнены условия теоремы и $\sigma(A) \ge 3n$. Тогда по лемме 1 он имеет 2n-автономное состояние $s \in S$ и тогда, по лемме 7 он имеет автономное состояние, что противоречит условию теоремы.

Следствие 9. Пусть $A = (X, V_n(q)\backslash 0, F_q, (B_x)_{x \in X}, (C_x)_{x \in X})$ – линейный автомат без автономных состояний и линейное преобразо-

вание B_a, $a \in X$ является полноцикловым преобразованием пространства $V_n(q)$.

Тогда $\sigma(A) \le 3n-1$.

3.5. Слабый гомоморфизм автоматов

Установим связи вводимого понятия слабого гомоморфизма автомата с понятиями неотличимости состояний и автономности автоматов.

Определение 13. Пусть $A = (X_A, S_A, Y_A, h^A, f^A)$ и $B = (X_B, S_B, Y_B, h^B, f^B)$ – автоматы.

Тройка отображений (ψ, φ, χ):

$\psi: X_A \to X_B$, $\varphi: S_A \to S_B$, $\chi: Y_A \to Y_B$

называется слабым k-гомоморфизмом автомата A в автомат B, если из условия

$$A(s, x(1), \ldots, x(k)) = y_1, \ldots, y_k,\ x(j) \in X,\ y_j \in Y,\ j \in \{1, \ldots, k\}$$

вытекает

$$B(\varphi(s), \psi(x(1)), \ldots, \psi(x(k))) = \chi(y_1), \ldots, \chi(y_k).$$

Если (ψ, φ, χ) – слабый k-гомоморфизм автомата A в B при любом k , то говорят, что (ψ, φ, χ) – слабый гомоморфизм A в B.

Определение 14. Автомат A вложим по k-неотличимости в автомат B если существует слабый k-гомоморфизм (ψ, φ, χ) A в B, где ψ, χ – инъективные отображения.

Будем говорить, что A вложим по неотличимости в B, если A вложим по k-неотличимости в B для любого k.

Слабый k-гомоморфизм (слабый гомоморфизм) автомата A в B = A будем называть слабым k-эндоморфизмом (слабым эндоморфизмом) автомата A. Обозначим через E-тождественное отображение множества состояний S_A автомата A в себя.

Определение 15. Слабый k-эндоморфизм (слабый эндоморфизм) (ψ, E, χ) автомата A называется внешне отождествляющим слабым k-эндоморфизмом (внешне отождествляющим слабым эндоморфизмом).

Теорема 9. Тогда и только тогда существует слабый k-гомоморфизм автомата A в B, когда найдется образ внешне отождествляющего слабого k-эндоморфизма автомата A, вложимый по k-неотличимости в автомат B.

Доказательство. Достаточность условий теоремы очевидна, докажем их необходимость. Слабый k-гомоморфизм (ψ, φ, χ) авто-

мата A в B определяет разбиения множеств X_A, Y_A, на классы вида $\tilde{x}$, $\tilde{y}$, соответственно. Так класс $\tilde{x} = \{x : \psi(x) = x^B, x \in X_A\}$, $x^B \in X_B$, а класс $\tilde{y} = y : \chi(y) = y^B, y \in Y_A\}$, $y^B \in Y_B$. Пусть $\bar{x}$, $\bar{y}$ – представители классов $\tilde{x}$, $\tilde{y}$. Для краткости будем здесь использовать обозначение $\{\tilde{x}\}$ для множества всех классов $\tilde{x}$, аналогично – $\{\tilde{y}\}$, $\{\bar{x}\}$ и $\{\bar{y}\}$.

Рассмотрим автомат $\bar{A} = (\{\bar{x}\}, S_A, \{\bar{y}\}, (h^{\bar{A}}_{\bar{x}})_{\bar{x}\in\{\bar{x}\}}, (f^{\bar{A}}_{\bar{x}})_{\bar{x}\in\{\bar{x}\}})$, где $h^{\bar{A}}_{\bar{x}} = h^{A}_{\bar{x}}$, $f^{\bar{A}}_{\bar{x}}(s) = \bar{y}$, если $f^{A}_{\bar{x}}(s) \in \tilde{y}$. Определим отображения $\psi` : X_A \to X_A$, $\chi` : Y_A \to Y_A$, положив $\psi`(x) = \bar{x}$, если $x \in \tilde{x}$, $\chi`(y) = \bar{y}$ если $y \in \tilde{y}$.

Покажем, что $(\psi`, E, \chi`)$ внешне отождествляющий слабый k-эндоморфизм автомата A, образом которого является автомат $\bar{A}$. Пусть для входного слова x(1), x(2), …, x(k) автомата A и $s \in S_A$

$$A(s, x(1), ..., x(k) = y_1, ..., y_k,\ A(s, \bar{x}(1), ..., \bar{x}(k) = y`_1, ..., y`_k,$$

тогда

$$B(\phi s, \psi(x(1)), ..., \psi(x(k)) = \chi(y_1), ..., \chi(y_k).$$

Но $\psi(x(j)) = \psi(\bar{x}(j))$, поэтому $\chi(y_j) = \chi(y`_j)$, $j \in \{1, \ldots, k\}$ и, следовательно,

$$\bar{A}(s, \bar{x}(1), ..., \bar{x}(k)) = \bar{y}_1, ..., \bar{y}_k.$$

Покажем теперь, что $\bar{A}$ вложим по k-неотличимости в автомат B. Для этого рассмотрим тройку отображений $(\psi``, \phi, \chi``)$, где $\psi``(\bar{x}) = \psi(\bar{x})$, $\chi``(\bar{y}) = \chi(\bar{y})$. Пусть для некоторого слова $\bar{x}(1), ..., \bar{x}(k)$ и $s \in S_A$

$$\bar{A}(s, \bar{x}(1), ..., \bar{x}(k)) = \bar{y}_1, ..., \bar{y}_k.$$

Поэтому очевидно, что

$$A(s, \bar{x}(1), ..., \bar{x}(k)) = y_1, ..., y_k,$$

где каждая пара символов $y_j, \bar{y}_j$ лежит в одном классе разбиения Y_A и, следовательно,

$$B(\phi s, \psi(\bar{x}(1)), ..., \psi(\bar{x}(k))) = \chi(y_1), ..., \chi(y_k) =$$
$$= \chi(\bar{y}_1), ..., \chi(\bar{y}_k) = \chi``(\bar{y}_1), ..., \chi``(\bar{y}_k) = B(\phi s, \psi``(\bar{x}(1), ..., \psi``\bar{x}(k)),$$

что и требовалось показать.

Пусть (ψ_1, ϕ_1, χ_1) – слабый k-гомоморфизм автомата A_1 в автомат A_2, а (ψ_2, ϕ_2, χ_2) – слабый k-гомоморфизм автомата A_2 в автомат A_3.

Тогда, очевидно, тройка отображений $(\psi_2\psi_1, \phi_2\phi_1, \chi_2\chi_1) = (\psi_2, \phi_2, \chi_2)\,(\psi_1, \phi_1, \chi_1)$:

$$\psi_2\psi_1 : x \mapsto \psi_2(\psi_1(x)),\ x \in X_{A_1},$$

$$\phi_2\phi_1 : s \mapsto \phi_2(\phi_1(x)),\ s \in S_{A_1},$$

$$\chi_2\chi_1 : y \mapsto \chi_2(\chi_1(y)),\ y \in Y_{A_1}$$

является слабым k-гомоморфизмом автомата A_1 в автомат A_3.

Отметим, что если (ψ,ϕ,χ) является слабым k-гомоморфизмом автомата A в B, то согласно доказательству теоремы 9 можно эффективно указать автомат $\bar{A}$, внешне отождествляющий слабый эндоморфизм $(\psi`,E,\chi`)$ автомата A, образом которого является $\bar{A}$ и слабый k-гомоморфизм $(\psi``,\phi,\chi``)$ автомата $\bar{A}$ в B ($\psi``,\chi``$ – инъективное отображения), для которых $(\psi,\phi,\chi)=(\psi``,\phi,\chi``)(\psi`,E,\chi`)$.

Пусть R_B – степень различимости автомата B.

Лемма 9. Если A вложим по k-неотличимости в B для $k \geq R_B+1$, то A вложим по неотличимости в B.

Доказательство. Пусть A вложим по k-неотличимости в B и (ψ,ϕ,χ) – слабый k-гомоморфизм автомата A в B. (Напомним, что ψ,χ – *инъективные отображения.*)

Рассмотрим автоматы:

– автомат $A_{\psi,\chi}$ с входным алфавитом $\{\psi(x): x \in X_A\} = (\psi(x))_{x\in X_A}$, множеством состояний S_A, выходным алфавитом $\{\chi(y): y \in Y_A\} = (\chi(y))_{y\in Y_A}$, частичными функциями переходов и выходов

– $(h_{\psi(x)})_{\psi(x)\in\{\psi(x):x\in X_A\}}$, $(f_{\psi(x)})_{\psi(x)\in\{\psi(x):x\in X_A\}}$,

где $h_{\psi(x)} = h_x^A, f_{\psi(x)} = \chi f_x^A, x \in X_A$;

– автомат $B_{\psi(X)} = (\{\psi(x): x \in X_A\}, S_B, Y_B, (h^B_{\psi(x)})_{x\in X_A}, (f^B_{\psi(x)})_{x\in X_A})$.

Очевидно, автоматы A, $A_{\psi,\chi}$ изоморфны и состояния $s,\varphi(s)$ автоматов $A_{\psi,\chi}$, $B_{\psi(X)}$ неотличимы, то есть

$$A_{\psi,\chi}(s,P) = B_{\psi(X)}(\phi(s),P)$$

при любом входном слове P длины k.

Пусть C – автомат, состоящий из двух компонент $A_{\psi,\chi}$ и $B_{\psi(X)}$. Легко доказывается, что для степеней различимости приведенных автоматов справедливы соотношения:

$$R(A_{\psi,\chi}) \leq R(B_{\psi(X)}) \text{ и } R(C) = R(B_{\psi(X)}) = R(B).$$

Поэтому состояния вида $s,\phi(s)$ неотличимы, что и доказывает справедливость леммы.

Лемма 10. Внешне отождествляющий слабый k-эндоморфизм автомата A при $k \geq R(A)+1$ является слабым эндоморфизмом.

Доказательство. Воспользуемся обозначениями при доказательстве теоремы 9.

Пусть $(\psi`, E, \chi`)$ внешне отождествляющий слабый k-эндоморфизм автомата A, образом которого является автомат

$$\overline{A} = (\{\overline{x}\}, S_A, \{\overline{y}\}, (h_{\overline{x}}^{\overline{A}})_{\overline{x}\in\{\overline{x}\}}, (f_{\overline{x}}^{\overline{A}})_{\overline{x}\in\{\overline{x}\}}).$$

Рассмотрим автомат $\hat{A} = (X_A, S_A, \{\overline{y}\}, (h_x^{\hat{A}})_{x\in X_A}, (f_x^{\hat{A}})_{x\in X_A})$, где $h_{\overline{x}}^{\hat{A}} = h_x^A$, $f_x^{\hat{A}} = \chi` f_x^A$, x∈XA.

Тройка отображений $(E, E, \chi`)$ осуществляет гомоморфизм автомата A на $\hat{A}$, а $(\psi`, E, E)$ осуществляет внешне отождествляющий слабый k-гомоморфизм автомата $\psi`(x(j)) = \psi`(x`(j)),\ j\in\{1,...,k\}$, образом которого является $\overline{A}$. Последний факт равносилен следующему условию: для любой пары слов x(1), …, x(k), x`(1), …, x`(k), для которых $\psi`(x(j)) = \psi`(x`(j)),\ j\in\{1,...,k\}$, справедливы равенства

$$f_{x(j)}^{\hat{A}} h_{x(j-1)}^{\hat{A}} ... h_{x(1)}^{\hat{A}} = f_{x`(j)}^{\hat{A}} h_{x`(j-1)}^{\hat{A}} ... h_{x`(1)}^{\hat{A}},\ \mathrm{j}\in\{1,\ldots,\mathrm{k}\}.$$

Очевидно, что утверждение леммы будет доказано, если мы покажем, что

$$f_{x(k+1)}^{\hat{A}} h_{x(k)}^{\hat{A}} ... h_{x(1)}^{\hat{A}} = f_{x`(k+1)}^{\hat{A}} h_{x`(k)}^{\hat{A}} ... h_{x`(1)}^{\hat{A}},$$

при $\psi`(x(j)) = \psi`(x`(j)),\ j\in\{1,...,k+1\}$.

Обозначим через T(j) все входные слова автомата $\hat{A}$ длины не превосходящей j.

По условию k≥R(A)+1, поэтому функция $f_{x(k+1),x(k),...,x(2)}^{\hat{A}} = f_{x(k+1)}^{\hat{A}} h_{x(k)}^{\hat{A}} ... h_{x(2)}^{\hat{A}}$ *определена* функциями $(f_P^{\hat{A}}:\ P\in T(R_A - 1)$, то есть найдется функция Ф, для которой

$$f_{x(k+1),x(k),...,x(2)}^{\hat{A}} = \Phi((f_P^{\hat{A}}:\ P\in T(R_A - 1)).$$

Тогда

$$f_{x(k+1),x(k),...,x(2),x(1)}^{\hat{A}} = \Phi((f_{x(1)P}^{\hat{A}}:\ P\in T(R_A - 1));$$
$$f_{x(k+1),x(k),...,x(2),x`(1)}^{\hat{A}} = \Phi((f_{x`(1)P}^{\hat{A}}:\ P\in T(R_A - 1)),$$

Так как в этих двух равенствах под знаком Ф стоят одинаковые функции, то при $\psi`(x(j)) = \psi`(x`(j)),\ j\in\{1,...,k+1\}$ получаем

$$f_{x(k+1),x(k),...,x(2),x(1)}^{\hat{A}} = f_{x(k+1),x(k),...,x(2),x`(1)}^{\hat{A}} = f_{x`(k+1),x`(k),...,x`(2),x`(1)}^{\hat{A}},$$

что и требовалось показать.

Проведенное доказательство показывает, в частности, что наличие внешне отождествляющих k-эндоморфизмов (ψ, E, χ) автомата A тесным образом связано с наличием

k-автономных подавтоматов $\hat{A}(\tilde{x}) = (\tilde{x}, S_A, \{\overline{y}\}, (h_x^{\hat{A}})_{x\in\tilde{x}}, (f_x^{\hat{A}})_{x\in\tilde{x}})$ автомата $\hat{A}$.

Из теоремы 9, лемм 9 и 10 вытекает следствие.

Следствие 10. Если (ψ, ϕ, χ) – слабый k-гомоморфизм автомата A в B, k ≥ max(R(A), R(B))+1, то (ψ, ϕ, χ) – слабый гомоморфизм A в B.

Понизить оценку k ≥ max(R(A), R(B))+1 невозможно, так как примеры неавтономных регистров сдвига показывают, что оценки R(B)+1, R(A)+1, данные в леммах 9 и10, не могут быть понижены.

Глава 4. ДЕКОМПОЗИЦИЯ АВТОМАТОВ

Метод, основанный на разбиении большой целой части на меньшие составляющие, объединенные между собой некоторым способом (причем каждая их них представляет собой некоторое целое), называется *декомпозицией*. Мы будем рассматривать декомпозицию конечных автоматов.

Основной целью данной главы[1] является решение следующей задачи. Пусть дан некоторый конечный автомат и некоторое покрытие его множества состояний. Возможно ли осуществить декомпозицию исходного автомата с помощью автомата, множествами состояний которых являются блоки данного покрытия? Для решения поставленной задачи рассмотрим предварительно основные способы декомпозиции конечных автоматов: параллельное и последовательное соединение.

Введем обозначения и напомним некоторые основные определения.

4.1. Разбиения и покрытия множества. Примеры

Определение 4.1.1. Система множеств $H_1, H_2, \ldots, H_n = \{H_i\}_{i=1}^{n}$ называется *разбиением множества* Z, если выполняются следующие условия:

$H_1 \cup H_2 \cup \ldots H_n = Z$ и для всех $i \neq j$, $H_i \cap H_j = \varnothing$.

При этом множества H_i называются *блоками разбиения*.

Разбиение множества Z будем обозначать $\pi = \{H_1, H_2, \ldots, H_n\}$.

Определение 4.1.2. Система множеств $H_1, H_2, \ldots, H_n = \{H_i\}_{i=1}^{n}$ называется покрытием множества Z, если выполняется условие:

$H_1 \cup H_2 \cup \ldots H_n = Z$

и для всех $i \neq j$

$H_i \neq H_j$.

При этом множества H_i называются *блоками покрытия*. Иногда требуют, чтобы в системе блоков не содержались блоки вида

[1] Глава 4 написана с использованием работы [12] и результатов курсовой работы Э. Р. Газизовой, студентки Московского государственного университета имени М. В. Ломоносова (факультет вычислительной математики и кибернетики, кафедра математической кибернетики), выполненной под руководством А. В. Бабаша.

$H_i \subseteq H_j$, i ≠ j. Покрытие множества будем обозначать $\pi^d = \{H_1, H_2, \ldots, H_n\}$.

Пример 4.1.1. Пусть $Z = \{1,2,3,4,5,6,7,8,9\}$ – основное множество. Тогда его разбиениями являются:

$\pi_1 = \{\{1,2\},\{3,4\},\{5,6\},\{7,8,9\}\}$;

$\pi_2 = \{\{1,6\},\{2,3\},\{4,5\},\{7,8\},\{9\}\}$.

Для удобства будем использовать следующую запись:

$\pi_1 = \{\overline{1,2};\overline{3,4};\overline{5,6};\overline{7,8,9}\}$;

$\pi_2 = \{\overline{1,6};\overline{2,3};\overline{4,5};\overline{7,8};\overline{9}\}$.

Таким образом, в дальнейшем будем считать, что $\overline{7,8,9}$ – это блок разбиения множества Z, а $\{7,8,9\}$ – подмножество множества Z, элементы которого образуют блок разбиения.

Покрытиями множества Z являются:

$\pi_1^d = \{\overline{1,2,5};\overline{3,4};\overline{5,6,9};\overline{7,8,9}\}$;

$\pi_2^d = \{\overline{1,4,6};\overline{2,3};\overline{4,5};\overline{7,8};\overline{6,9}\}$.

Введем понятия: *больше, произведения и суммы двух разбиений данного множества.*

Определение 4.1.3. Пусть π_1 и π_2 – два разбиения множества Z. Тогда $\pi_1 \le \pi_2$, если для любого $\overline{H_i} \in \pi_1$ найдется $\overline{H_j} \in \pi_2$, для которого выполняется условие: $H_i \subseteq H_j$.

Пример 4.1.2. Рассмотрим наряду с разбиением $\pi_1 = \{\overline{1,2};\overline{3,4};\overline{5,6};\overline{7,8,9}\}$ еще одно разбиение множества $Z = \{1,2,3,4,5,6,7,8,9\}$ $\pi_3 = \{\overline{1,2};\overline{3};\overline{4};\overline{5,6};\overline{7,8};\overline{9}\}$. Тогда из определения 4.1.3 следует, что $\pi_3 \le \pi_1$.

Определение 4.1.4. Разбиение множества Z, каждый блок которого состоит из одного элемента этого множества, называется *тождественным нулем.*

Пусть $Z = \{1,2,\ldots,n\}$. Тогда разбиение этого множества, являющееся тождественным нулем, будем обозначать $0 = \{\overline{1},\overline{2},\ldots,\overline{n}\}$.

Определение 4.1.5. Разбиение множества Z, представляющее собой единственный блок, состоящий из всех элементов этого множества, называется *тождественной единицей*.

Пусть $Z=\{1,2,\ldots,n\}$. Тогда разбиение этого множества, являющееся тождественной единицей, будем обозначать $1=\{\overline{1,2,\ldots,n}\}$. Из определений 4.1.4 и 4.1.5 следует, что для любого разбиения π: $\pi\le 1$ и $0\le\pi$.

Для того чтобы ввести понятия произведения и суммы разбиений, введем следующее обозначение: $B_\pi(s)$ – блок разбиения π, содержащий элемент s основного множества.

Определение 4.1.6. Произведением разбиений π_1 и π_2 множества Z называется разбиение $\pi_1\bullet\pi_2$ этого множества, блоки которого определяются следующим образом:

$B_{\pi_1\bullet\pi_2}(s)=B_{\pi_1}(s)\cap B_{\pi_2}(s)$.

Определение 4.1.7. Суммой разбиений π_1 и π_2 множества Z называется разбиение $\pi_1+\pi_2$ этого множества, блоки которого определяются следующим рекурсивным способом:

пусть $B_1(s)=B_{\pi_1}(s)\cup B_{\pi_2}(s)$

и пусть для i >1

$B_{i+1}(s)=B_i(s)\cup\{$B: B – это блок разбиения π_1 или π_2, причем $B\cap B_i(s)\ne\varnothing\}$.

Тогда $B_{\pi_1+\pi_2}(s)=B_i(s)$ при таком i, что $B_i(s)=B_{i+1}(s)$.

Пример 4.1.3.

Пусть $\pi_1=\{\overline{1,2};\overline{3,4};\overline{5,6};\overline{7,8,9}\}$ и $\pi_2=\{\overline{1,6};\overline{2,3};\overline{4,5};\overline{7,8};\overline{9}\}$. Тогда

$\pi_1\cdot\pi_2=\{\overline{1};\overline{2};\overline{3};\overline{4};\overline{5};\overline{6};\overline{7,8};\overline{9}\}$,

$\pi_1+\pi_2=\{\overline{1,2,3,4,5,6};\overline{7,8,9}\}$.

4.2. Фактор-автомат. Покрытие автомата

Ниже в данном подразделе мы будем рассматривать *автоматы без выхода*. Напомним определение этого понятия.

Определение 4.2.1. Автоматом (точнее автоматом без выхода) называется тройка $A=\langle X,S,h\rangle$, где X – входной алфавит, S – множество состояний, h – функция перехода $h:S\times X\to S$, и соответствующий закон функционирования.

Напомним, что функция h определяет частичные функции переходов $(h_x)_{x\in X}$, а именно для $x\in X$ и $s\in S$:

$$h_x s = h(s, x).$$

Определение 4.2.2. Пусть дан автомат $A=\langle X^A, S^A, h^A\rangle$ и пусть $\pi=\{\overline{S_i}\}_{i=1}^{n}$ – разбиение множества S^A. Тогда разбиение π называется *согласованным с автоматом* $A=\langle X^A, S^A, \delta^A\rangle$, если блоки разбиения π функцией перехода автомата h^A переводятся в блоки этого разбиения, то есть для всех $x\in X^A, i\in\{1,2,\ldots,n\}$ существует j такое, что $h_x^A(S_i)\subseteq S_j$.

Определение 4.2.3. Пусть дан автомат $A=\langle X^A, S^A, h^A\rangle$ и пусть $\pi=\{\overline{S_i}\}_{i=1}^{n}$ – согласованное разбиение множества S^A. Тогда *фактор-автоматом по согласованному разбиению* π называется автомат $A/\pi=\langle X^{A/\pi}, S^{A/\pi}, h^{A/\pi}\rangle$ такой, что $X^{A/\pi}=X^A$, $S^{A/\pi}=\pi=\{\overline{S_i}\}_{i=1}^{n}$ и для $x\in X^A, i\in\{1,2,\ldots,n\}$

$$h^{A/\pi}(\overline{S_i}, x)=\overline{S_j},$$

где j таково, что $h_x^A S_i\subseteq S_j$ (индекс j определяется по (x ,i) однозначно).

Определение 4.2.4. Пусть дан автомат $A=\langle X^A, S^A, h^A\rangle$ и пусть $\pi^d=\{\overline{S_i}\}_{i=1}^{n}$ – покрытие множества S^A. Тогда покрытие π^d называется *согласованным с автоматом* $A=\langle X^A, S^A, h^A\rangle$, если блоки покрытия π^d функцией перехода автомата h^A переводятся в блоки этого покрытия, т.е. для каждой пары (x,i) $x\in X^A, i\in\{1,2,\ldots,n\}$ существует j такое, что $h_x^A S_i\subseteq S_j$ (j может определиться неоднозначно).

Определение 4.2.5. Пусть дан автомат $A=\langle X^A, S^A, h^A\rangle$ и пусть $\pi^d=\{\overline{S_i}\}_{i=1}^{n}$ – покрытие множества S^A. Тогда *фактор-автоматом по согласованному покрытию* π^d называется *любой* автомат $A/\pi^d=\langle X^{A/\pi^d}, S^{A/\pi^d}, \delta^{A/\pi^d}\rangle$ такой, что $X^{A/\pi^d}=X^A$, $S^{A/\pi^d}=\pi^d=\{\overline{S_i}\}_{i=1}^{n}$ и для каждой пары (x,i), $x\in X^A, i\in\{1,2,\ldots,n\}$

$$h^{A/\pi^d}\overline{S_i}=\overline{S_j},$$

где j такое, что $h_x^A\, S_i\subseteq S_j$.

Замечание. Следует еще раз отметить, что в определениях 4.2.4 и 4.2.5 соответствующий номер блока j может быть не единственным. Если блоков несколько, то они считаются равноправными и выбирается любой из них. В связи с этим наверно лучше определять

фактор-автомат по согласованному покрытию как семейство всех таких автоматов.

Пример 4.2.1. Рассмотрим автомат $A=\langle X^A, S^A, h^A\rangle$ такой, что $X^A=\{x_1,x_2\}$, $S^A=\{1,2,3,4,5,6\}$, а действие функции перехода $h^A: S^A\times X\to S^A$ изображено в табл. 1.

Таблица 1

S^A	X^A	
	x_1	x_2
1	3	2
2	5	4
3	6	2
4	5	1
5	6	1
6	2	6

Разбиение $\pi=\{S_1=\overline{1,2,4}; S_2=\overline{3,5}; S_3=\overline{6}\}$ множества состояний S^A является согласованным с данным автоматом А. Фактор-автомат $A/\pi=\langle X^A, S^{A/\pi}, h^{A/\pi}\rangle$ автомата А по заданному разбиению π определяется следующим образом:

$$X^{A/\pi}=X^A=\{x_1,x_2\},\ S^{A/\pi}=\pi=\{\overline{S_1},\overline{S_2},\overline{S_3}\},$$

а действие функции перехода $h^{A/\pi}: S^{A/\pi}\times X^{A/\pi}\to S^{A/\pi}$ изображено в табл. 2.

Таблица 2

$S^{A/\pi}$	$X^{A/\pi}$	
	x_1	x_2
$\overline{S_1}$	$\overline{S_2}$	$\overline{S_1}$
$\overline{S_2}$	$\overline{S_3}$	$\overline{S_1}$
$\overline{S_3}$	$\overline{S_1}$	$\overline{S_3}$

Напомним общеизвестные обозначения.

Пусть задано бинарное отношение F или функция $F: X\to Y$. Тогда

$pr_1F=\{x\in X\mid \exists y\in Y: F(x)=y\}$ – множество прообразов F;

$pr_2F = \{y \in Y \mid \exists x \in X : F(x) = y\}$ – множество образов F.

Определение 4.2.6. Автомат $B = \langle X^B, S^B, h^B \rangle$ покрывает автомат $A = \langle X^A, S^A, h^A \rangle$ *(обозначение B≥A),* тогда и только тогда, когда определено бинарное отношение $F \subseteq S^A \times S^B$ (возможно не сюръективное т.е. возможно $pr_2F \neq S^B$), причем F^{-1} является *функцией* S^B на S^A (возможно частичной), а также определена функция $\psi : X^A \to X^B$ такая, что для всех $x \in X^A$ выполняется следующее условие: если $s^B \in pr_2F$, то $h^A_x F^{-1} s^B = F^{-1} h^B_{\psi(x)} s^B$.

Если не обращать внимание на функцию $\psi : X^A \to X^B$, например, положить $X^A = X^B$, $\Psi = E$ – тождественное отображение, то определение 4.2.6 говорит о том, что в автомате B имеется подавтомат *B` гомоморфный по состояниям автомату A (при гомоморфизме (E,F-1)).* Если при этом F^{-1} дополнительно является биекцией pr_2F на S^A, то говорят, что *A изоморфно вложим в B.*

Изобразим покрытие B ≥ A автомата A на рис. 7.

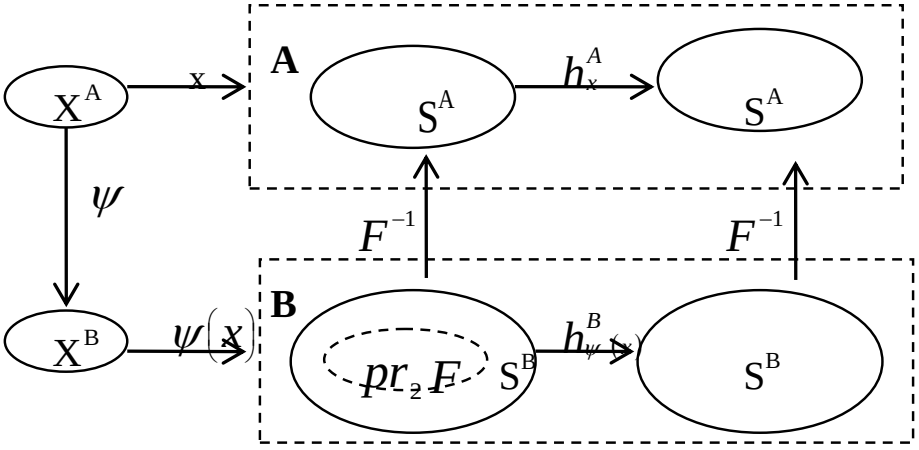

Рис. 7. Автомат B покрывает автомат A

4.3. Параллельное соединение автоматов

Напомним следующее определение.

Определение 4.3.1. Параллельным соединением двух автоматов $A = \langle X^A, S^A, h^A \rangle$ и $B = \langle X^B, S^B, h^B \rangle$ называется автомат $C = \langle X^C, S^C, h^C \rangle$, обладающий следующими свойствами: $X^C = X^A = X^B = X$, $S^C = S^A \times S^B$, функция h^C определена частичными функциями переходов $(h^C_x)_{x \in X}$, причем h^C_x, $x \in X$ определена следующим образом:

$$h_x^C\left\langle s^A, s^B\right\rangle = \left\langle h_x^A s^A, h_x^B s^B\right\rangle,$$

где $s^A \in S^A, s^B \in S^B$.

Параллельное соединение двух автоматов изображено на рис. 8.

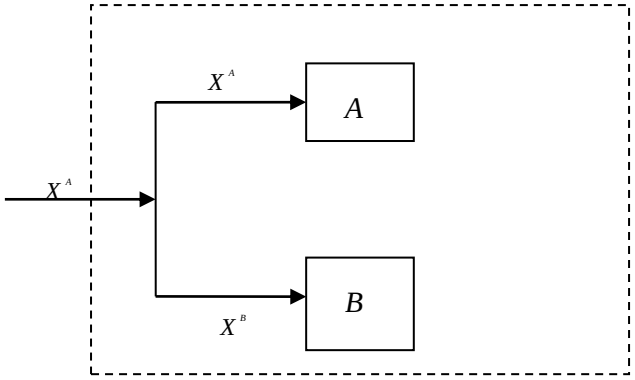

Рис. 8. Параллельное соединение двух автоматов

Поиск составляющих параллельного соединения, а следовательно, и способ декомпозиции автомата с помощью такого соединения описывается в следующей теореме.

Теорема 1. Пусть дан автомат $C = \left\langle X^C, S^C, h^C\right\rangle$. Пусть существуют два согласованных с автоматом С разбиения множества S^C π и τ такие, что π · τ = 0. Тогда автомат $C = \left\langle X^C, S^C, h^C\right\rangle$ может быть покрыт параллельным соединением фактор-автоматов С/π и С/τ (С/π ×С/τ ≥ С).

Доказательство. Пусть $\pi = \left\{\overline{H_i}\right\}_{i=1}^{n}$ и $\tau = \left\{\overline{K_j}\right\}_{i=1}^{m}$. Как и в примере 1, будем считать, что $\overline{H_i}$ – это блок разбиения π множества S^C, а H_i – подмножество множества S^C, элементы которого образуют блок разбиения. Аналогичное обозначение введем и для разбиения τ. Обозначим С/π = А и С/τ = В.

Определим множество $T^{A\times B}$ множества $S^A \times S^B$ следующим образом:

$$T^{A\times B} = \left\{ \ \left\langle \overline{H_i}, \overline{K_j}\right\rangle \mid \overline{H_i} \in S^A, \overline{K_j} \in S^B, H_i \cap K_j \neq \varnothing \ \right\}.$$

Напомним, что по определению 4.2.3 фактор-автомата

$S^A = \pi = \left\{\overline{H_i}\right\}_{i=1}^{n}$ и $S^B = \tau = \left\{\overline{K_j}\right\}_{i=1}^{m}$.

Введем *отображение* $\eta : T^{A\times B} \to S^C$ такое, что

$\eta\left\langle \overline{H_i}, \overline{K_j}\right\rangle = H_i \cap K_j$.

Теперь покажем, что функция $F^{-1} = \eta$ удовлетворяет условию покрытия автоматов.

Вспомним определение 4.1.4 покрытия автоматов.

Автомат $D=\langle X^D, S^D, h^D\rangle$ *покрывает* автомат $C=\langle X^C, S^C, h^C\rangle$ тогда и только тогда, когда определено бинарное отношение $F \subseteq S^C \times S^D$, $pr_1 F = S^C$, причем отношение не обязательно сюръективно, и обратное отношение F^{-1} является функцией $pr_2 F$ на S^C, а также определена функция $\psi : X^C \to X^D$ такая, что для всех $x \in X^C$ выполняется следующее условие:

$$h_x^C F^{-1} s^D = F^{-1} h_{\psi(x)}^D s^D, \qquad (6)$$

где $s^D \in pr_2 F$.

Пусть $D = A \times B$. Тогда по определению параллельного соединения автоматов (определение 4.3.1) и по определению факторавтоматов A и B (определение 4.2.3) автомат $D=\langle X^D, S^D, h^D\rangle$ обладает следующими свойствами:

$$X^D = X^A = X^B = X^C; \quad S^D = S^A \times S^B = \left\{\left\langle \bar{H}_i, \bar{K}_j \right\rangle : \bar{H}_i \in S^A, \bar{K}_j \in S^B\right\},$$

и функция h^D определена частичными функциями переходов $(h_x^D)_{x \in X^D}$, причем функция h_x^D определена следующим образом:

$$h_x^D \left\langle \overline{H_i}, \overline{K_j} \right\rangle = \left\langle h_x^A\left(\overline{H_i}\right), h_x^B\left(\overline{K_j}\right)\right\rangle = \left\langle \overline{H_p}, \overline{K_q}\right\rangle, \; i,p \in \overline{1,n}; j,q \in \overline{1,m}.$$

Необходимо доказать, что автомат $D = A \times B$ покрывает исходный автомат C.

В нашем случае роль функции $F^{-1} \subseteq S^D \times S^C$ (рассматриваемая как бинарное отношение), отображающей некоторое подмножество множества S^D на все множество S^C, играет функция $\eta : T^{A \times B} \to S^C$, поскольку по предположению множество $T^{A \times B}$ – это подмножество множества $S^A \times S^B = S^D$.

Введем два отображения $\phi_\pi : S^C \to \pi$ и $\phi_\tau : S^C \to \tau$, причем

$$\phi_\pi\left(s^C\right) = H_i \Leftrightarrow s^C \in H_i,$$
$$\phi_\tau\left(s^C\right) = K_j \Leftrightarrow s^C \in K_j.$$

Проверим, что выполняется условие (6).

Для всех $\left\langle \overline{H_i}, \overline{K_j}\right\rangle \in T^{A \times B}$ и для всех $x \in X^C$ имеем:

$$h_x^C\left(\eta\left\langle \overline{H_i}, \overline{K_j}\right\rangle\right) = \{\text{по определению функции } \eta\} =$$

$$h_x^C\left(H_i \cap K_j\right) = h_x^C\left(H_i\right) \cap h_x^C\left(K_j\right) = \{\text{по определению функций } \varphi_\pi \text{ и } \varphi_\tau\} =$$

$$\phi_\pi\left(h_x^C\left(H_i\right)\right) \cap \phi_\tau\left(h_x^C\left(K_j\right)\right) = \{\text{по определению функции } \eta\} =$$

$$\eta\left\langle \overline{\phi_\pi\left(h_x^C\left(H_i\right)\right)}, \overline{\phi_\tau\left(h_x^C\left(K_j\right)\right)}\right\rangle = \eta\left\langle h_x^A\left(\overline{H_i}\right), h_x^B\left(\overline{K_j}\right)\right\rangle = \{\text{по определению}$$

$$\text{параллельного соединения автоматов}\} = \eta\left(h_x^{A \times B}\left\langle \overline{H_i}, \overline{K_j}\right\rangle\right).$$

Таким образом доказано, что условие (6) выполнено, следовательно автомат $A \times B$ покрывает автомат С. Теорема доказана.

Докажем, что отображение η, фигурирующее при доказательстве данной теоремы, является биективным (взаимнооднозначным). По условию теоремы $\pi \cdot \tau = 0$. По определению 4.1.6 произведения разбиений следует, что $\pi \cdot \tau = \{H_i \cap K_j\}$. Но по определению 4.1.4 тождественно нулевого разбиения следует, что каждый блок разбиения $\pi \cdot \tau$ состоит из единственного элемента. Отсюда следует, что $H_i \cap K_j = s^c \in S^C$ (пересечение этих множеств состоит из единственного элемента). Кроме этого по элементу $s^c = H_i \cap K_j$ однозначно восстанавливается пара $\langle \overline{H_i}, \overline{K_j} \rangle$, так как по определению 4.1.1 разбиения блоки каждого разбиения не пересекаются, следовательно, элемент s^c принадлежит только одному блоку разбиения π и только одному блоку разбиения τ. Следовательно, η – биективное отображение.

Таким образом, при выполнении условий теоремы 4.3.1 автомат С изоморфно вложим в параллельное соединение факторавтоматов С/π и С/τ .

Замечание. Конструкция параллельного произведения может быть простым способом обобщена на большее количество автоматов. Автоматы должны иметь одинаковый входной алфавит. В целом декомпозиция автомата с помощью параллельного соединения заключается в поиске согласованных с ним разбиений π и τ множества S^C таких, что $\pi \cdot \tau = 0$.

4.4. Последовательное соединение автоматов

Введем следующее определение.

Определение 4.4.1. Последовательным соединением двух автоматов $A = \langle X^A, S^A, h^A \rangle$ и $B = \langle X^B, S^B, h^B \rangle$ называется автомат AωB, обладающий следующими свойствами:

$$X^{A\omega B} = X^A,\ S^{A\omega B} = S^A \times S^B,$$

при этом функция $h_x^{A\omega B}$ определена следующим образом:

$$h_x^{A\omega B}\langle s^A, s^B \rangle = \left\langle h_x^A\left(s^A\right), h_{\omega(s^A, x)}\left(s^B\right) \right\rangle,$$

где $\omega : S^A \times X^A \to X^B$ – функция, используемая при соединении автомата А с В.

Последовательное соединение двух автоматов изображено на рис. 9.

Замечание. Если $X^A = X^B$, то последовательное соединение с функцией $\omega : \langle s^A \times x \rangle \to x$ становится эквивалентным параллельному соединению.

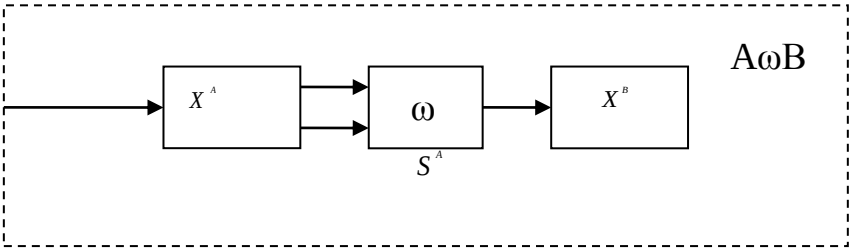

Рис. 9. Последовательное соединение автоматов

Если последовательное соединение осуществляется для большего числа автоматов, то необходимо обратить внимание на то, что автоматы могут последовательно соединяться только при выполнении некоторых условий.

Рассмотрим последовательное соединение трех автоматов. Возьмем три автомата A, B и C.

Пусть $D = (A\omega_1 B)\omega_2 C$ и $E = A\omega_3 (B\omega_4 C)$.

Тогда по определению 4.4.1:

$X^D = X^{A\omega_1 B} = X^A = X^E$, $S^D = S^A \times S^B \times S^C = S^E$,

причем

$$h_x^D \langle s^A, s^B, s^C \rangle = \left\langle h_x^{A\omega_1 B} \langle s^A, s^B \rangle, h^C_{\omega_2 \langle \langle s^A, s^B \rangle, x \rangle} (s^C) \right\rangle = \left\langle h_x^A (s^A), h^B_{\omega_1 \langle s^A, x \rangle} (s^B), h^C_{\omega_2 \langle \langle s^A, s^B \rangle, x \rangle} (s^C) \right\rangle$$

и

$$h_x^E \langle s^A, s^B, s^C \rangle = \left\langle h_x^A (s^A), h^{B\omega_4 C}_{\omega_3 \langle s^A, x \rangle} \langle s^B, s^C \rangle \right\rangle = \left\langle h_x^A (s^A), h^B_{\omega_3 \langle s^A, x \rangle} (s^B), h^C_{\omega_4 \langle s^B, \omega_3 \langle s^A, x \rangle \rangle} (s^C) \right\rangle$$

Легко заметить, что если предположить, что $\omega_1 = \omega_3$ и подобрать ω_2, ω_3 и ω_4 таким образом, что $\omega_2 \langle \langle s^A, s^B \rangle, x \rangle = \omega_4 \langle s^B, \omega_3 \langle s^A, x \rangle \rangle$, тогда

$$h^D = h^E.$$

Приведем без доказательства две леммы, связанные с понятием последовательного соединения автоматов.

Лемма 4.4.1. Если автомат B покрывает автомат A, то для любых функций ω_1 и ω_2 для любого автомата C последовательное соединение $C\omega_1 B$ покрывает последовательное соединение $C\omega_2 A$.

Лемма 4.4.2. Если автомат B покрывает автомат A и отображение $f : X^A \to X^B$ биективно, то для любых функций ω_1 и ω_2 и

для любого автомата C последовательное соединение $B_{\omega_1}C$ покрывает последовательное соединение $A_{\omega_2}C$.

Теперь, как и в случае параллельного соединения, опишем условия, при которых автомат представим в виде декомпозиции двух автоматов, связанных последовательным соединением и покрывающих исходный автомат.

Для формулировки следующей теоремы введем обозначения:

– m(π) – число элементов в максимальном блоке разбиения π;

– CD – последовательное соединение автоматов C и D. Символ ω в записи опущен, поскольку предполагается, что $S^C \times X^C \subseteq X^D$ и функция ω тождественна на $S^C \times X$.

Теорема 4.4.1. Пусть дан автомат $A = \langle X^A, S^A, h^A \rangle$ и система блоков $\pi = \{\overline{H_i}\}_{i=1}^{n}$, являющаяся разбиением множества S^A, согласованным с автоматом A.

Тогда существует автомат $D = \langle X^D, S^D, h^D \rangle$, в котором $|S^D| = m(\pi)$, а также фактор-автомат C = A/π, причем последовательное соединение автоматов C и D покрывает автомат A (CD ≥ A).

Доказательство. Для данного разбиения $\pi = \{\overline{H_i}\}_{i=1}^{n}$ можно подобрать разбиение $\tau = \{\overline{K_j}\}_{i=1}^{m}$ такое, что π · τ = 0 и $|\tau| = m(\pi)$. Идею доказательства этого факта проиллюстрируем на следующем примере: π = ({1,2,3,4}, {5,6}, {7}), тогда в качестве τ можно взять ({1,5,7}, {2,6}, {3}, {4}).

Построим автомат D следующим образом:

$$X^D = S^C \times X = \{\overline{H_i}\}_{i=1}^{n} \times X,\ S^D = \{\overline{K_j}\}_{i=1}^{m},$$

$$h^D : h^D_{\langle \overline{H_i}, x \rangle}(\overline{K_j}) = \phi_\tau(h^A_x(H_i \cap K_j)),$$

где $\phi_\tau : S^A \to \tau$ определим следующим образом: $\phi_\tau(s^A) = \overline{K_j}$, тогда и только тогда, когда $s^A \in K_j$.

В случае, когда $H_i \cap K_j = \varnothing$, будем считать, что значение $h^D_{\langle \overline{H_i}, x \rangle}(\overline{K_j})$ может быть выбрано либо произвольным образом, либо неопределенно.

Докажем, что если автомат D построен таким способом, то исходный автомат A может быть покрыт последовательным соединением автоматов D и C=A/π.

Определим множество T^{CD} как подмножество множества $S^C \times S^D$ следующим образом:

$$T^{CD} = \{\langle \overline{H_i}, \overline{K_j} \rangle \mid \overline{H_i} \in S^C, \overline{K_j} \in S^D, H_i \cap K_j \neq \varnothing\}.$$

Введем отображение $\eta : T^{CD} \to S^A$ такое, что $\eta\langle \overline{H_i}, \overline{K_j} \rangle = H_i \cap K_j$.

Докажем, что выполняются условия покрытия автоматов.

Для всех $\langle \overline{H_i}, \overline{K_j} \rangle \in T^{CD}$ и для всех $x \in X^A$ имеем:

$h_x^A\left(\eta\langle \overline{H_i}, \overline{K_j} \rangle\right)$ (по определению функции η) = $h_x^A(H_i \cap K_j)$;

(по определению отображений ϕ_π и ϕ_τ) = $\phi_\pi(h_x^A(H_i)) \cap \phi_\tau\left(h_x^A(H_i \cap K_j)\right)$

(по определению функции η) =

$= \eta\left\langle \phi_\pi(h_x^A(H_i)), \phi_\tau\left(h_x^A(H_i \cap K_j)\right)\right\rangle = \eta\left\langle h_x^C(\overline{H_i}), h^D_{\langle \overline{H_i}, x\rangle}(\overline{K_j})\right\rangle$ (по определению последовательного соединения) = $\eta\left(h_x^{CD}\langle \overline{H_i}, \overline{K_j} \rangle\right)$.

Таким образом доказано, что автомат CD покрывает автомат A и тем самым доказана теорема.

Аналогично рассуждениям, приведенным после доказательства теоремы 4.3.1, легко получить, что η – биективное отображение. По этой причине можно сказать, что при выполнении условий теоремы 2 автомат A изоморфно вложим в CD.

Приведем еще одну теорему, связывающую понятия последовательного соединения и покрытия автомата. Отметим, что в этой теореме рассматривается не разбиение множества состояний автомата, а покрытие этого множества.

Следующая теорема является основным результатом данного подраздела.

Теорема 4.4.2. Пусть дан автомат $A = \langle X^A, S^A, h^A \rangle$ и согласованное с автоматом A покрытие множества S^A $\pi^d = \{H_i\}_{i=1}^n$. Тогда существуют автоматы C и D такие, что C изоморфен фактор-автомату B = A/π^d, $|S^D| = m(\pi^d)$, причем последовательное соединение автоматов C и D покрывает автомат A (CD≥A).

Доказательство. По условию теоремы можно построить автомат $A' = \langle X`, S`, h` \rangle$ такой, что:

$X' = X^A = X^B$; $S' = \left\{\langle s^A, \overline{H_i} \rangle : s^A \in H_i, \overline{H_i} \in \pi^d\right\}$;

$h` : h`_x\langle s^A, \overline{H_i} \rangle = \left\langle h_x^A(s^A), h_x^B(\overline{H_i})\right\rangle$.

Таким образом, на множестве S' можно определить *разбиение* $\pi` = \{H`_i\}_{i=1}^n$ такое, что каждый его блок $H`_i$ содержит все соответ-

ствующие пары $\langle s^A, \overline{H_i} \rangle, s^A \in H_i$ (произошла нумерация блоков H_i номерами $\overline{H_i}$).

Аналогично теореме 4.4.2 построим автомат D такой, что CD покрывает автомат A`, где C = A'/π' и $|S^D| = m(\pi')$.

Фактор-автомат A'/π' изоморфен фактор-автомату A/π^d (изоморфизм: $H`_i \leftrightarrow H_i$). Отсюда следует, что $m(\pi^d) = m(\pi')$.

Заметим, что автомат A' покрывает автомат A. Отображение η покрытия имеет вид η: $\langle s^A, \overline{H_i} \rangle \to s^A$ при каждом H_i содержащем s^A. Следовательно, и CD покрывает автомат A по лемме 4.4.1. Теорема доказана.

Приведем пример построения декомпозиции автомата при помощи последовательного соединения двух фактор-автоматов по алгоритму.

Данный алгоритм описан в теореме 3.

Пример 4.4.1. Рассмотрим автомат $A = \langle X^A, S^A, h^A \rangle$ такой, что

$$X^A = \{x_1, x_2\}; \quad S^A = \{1,2,3,4,5,6\},$$

а действие функции перехода $h^A : X^A \times S^A \to S^A$ изображено в табл. 3.

Таблица 3

Действие функции перехода h^A

S^A	X^A	
	x_1	x_2
1	5	6
2	2	5
3	3	4
4	4	5
5	5	5
6	6	4

Пусть также дано покрытие множества состояний S^A:

$\pi^d = \{H_1 = \{1,4,5\}; H_2 = \{2,4\}; H_3 = \{3,5,6\}\}$.

Построим автоматы C и D так, чтобы CD ≥ A.

Построим фактор-автомат B = A/π^d.

Он изображен в табл. 4.

Таблица 4

Фактор-автомат A/π^d

S^B	X^B	
	x_1	x_2
$\overline{H_1}$	$\overline{H_1}$	$\overline{H_3}$
$\overline{H_2}$	$\overline{H_2}$	$\overline{H_1}$
$\overline{H_3}$	$\overline{H_3}$	$\overline{H_1}$

В табл. 4 $h^B_{x_2}\left(\overline{H_2}\right)=\overline{H_1}$, но верно и следующее:

$$h^B_{x_2}\left(\overline{H_2}\right)=\overline{H_3}.$$

Далее строим автомат A', разбиение π' и фактор-автомат C = A'/π'.

Разбиение π' будет определяться следующим образом:

$$\pi'=\left\{\overline{H'_1}=\left\{\langle 1,\overline{H_1}\rangle,\langle 4,\overline{H_1}\rangle,\langle 5,\overline{H_1}\rangle\right\},\ \overline{H'_2}=\left\{\langle 2,\overline{H_2}\rangle,\langle 4,\overline{H_2}\rangle\right\},\ \overline{H'_3}=\left\{\langle 3,\overline{H_3}\rangle,\langle 5,\overline{H_3}\rangle,\langle 6,\overline{H_3}\rangle\right\}\right\}$$

Действие автомата A' изобразим в табл. 5.

Таблица 5

Действие автомата A'

$S^{A'}$	$X^{A'}$	
	x_1	x_2
$\langle 1,\overline{H_1}\rangle$	$\langle 5,\overline{H_1}\rangle$	$\langle 6,\overline{H_3}\rangle$
$\langle 4,\overline{H_1}\rangle$	$\langle 4,\overline{H_1}\rangle$	$\langle 5,\overline{H_3}\rangle$
$\langle 5,\overline{H_1}\rangle$	$\langle 5,\overline{H_1}\rangle$	$\langle 5,\overline{H_3}\rangle$
$\langle 2,\overline{H_2}\rangle$	$\langle 2,\overline{H_2}\rangle$	$\langle 5,\overline{H_1}\rangle$
$\langle 4,\overline{H_2}\rangle$	$\langle 4,\overline{H_2}\rangle$	$\langle 5,\overline{H_1}\rangle$
$\langle 3,\overline{H_3}\rangle$	$\langle 3,\overline{H_3}\rangle$	$\langle 4,\overline{H_1}\rangle$
$\langle 5,\overline{H_3}\rangle$	$\langle 5,\overline{H_3}\rangle$	$\langle 5,\overline{H_1}\rangle$
$\langle 6,\overline{H_3}\rangle$	$\langle 6,\overline{H_3}\rangle$	$\langle 4,\overline{H_1}\rangle$

Тогда фактор-автомат C = A'/π' будет определяться данными табл. 6.

Таблица 6

Фактор-автомат C = A'/π'

S^C	X^C	
	x_1	x_2
$\overline{H'_1}$	$\overline{H'_1}$	$\overline{H'_3}$
$\overline{H'_2}$	$\overline{H'_2}$	$\overline{H'_1}$
$\overline{H'_3}$	$\overline{H'_3}$	$\overline{H'_1}$

Подберем разбиение τ таким образом, что $\pi \cdot \tau = 0$. Например, таким образом:

$$\tau = \left\{\overline{K_1} = \left\{\left\langle 1, \overline{H_1}\right\rangle, \left\langle 2, \overline{H_2}\right\rangle, \left\langle 3, \overline{H_3}\right\rangle\right\},\ \overline{K_2} = \left\{\left\langle 4, \overline{H_1}\right\rangle, \left\langle 4, \overline{H_2}\right\rangle, \left\langle 5, \overline{H_3}\right\rangle\right\},\ \overline{K_3} = \left\{\left\langle 5, \overline{H_1}\right\rangle, \left\langle 6, \overline{H_3}\right\rangle\right\}\right\}$$

3. Строим автомат D и последовательное соединение автоматов CD. Автомат D изображен в табл. 7. Автомат CD задан в табл. 8

Таблица 7

Автомат D

S^D	X^C					
	$\langle\overline{H_1}, x_1\rangle$	$\langle\overline{H_1}, x_2\rangle$	$\langle\overline{H_2}, x_1\rangle$	$\langle\overline{H_2}, x_2\rangle$	$\langle\overline{H_3}, x_1\rangle$	$\langle\overline{H_3}, x_2\rangle$
$\overline{K_1}$	$\overline{K_3}$	$\overline{K_3}$	$\overline{K_1}$	$\overline{K_3}$	$\overline{K_1}$	$\overline{K_2}$
$\overline{K_2}$	$\overline{K_2}$	$\overline{K_2}$	$\overline{K_2}$	$\overline{K_3}$	$\overline{K_2}$	$\overline{K_3}$
$\overline{K_3}$	$\overline{K_3}$	$\overline{K_2}$	–	–	$\overline{K_3}$	$\overline{K_2}$

Таблица 8

Автомат CD

S^{CD}	X^{CD}	
	x_1	x_2
$\langle\overline{H'_1}, \overline{K_1}\rangle$	$\langle\overline{H'_1}, \overline{K_3}\rangle$	$\langle\overline{H'_3}, \overline{K_3}\rangle$
$\langle\overline{H'_1}, \overline{K_2}\rangle$	$\langle\overline{H'_1}, \overline{K_2}\rangle$	$\langle\overline{H'_3}, \overline{K_2}\rangle$
$\langle\overline{H'_1}, \overline{K_3}\rangle$	$\langle\overline{H'_1}, \overline{K_3}\rangle$	$\langle\overline{H'_3}, \overline{K_2}\rangle$
$\langle\overline{H'_2}, \overline{K_1}\rangle$	$\langle\overline{H'_2}, \overline{K_1}\rangle$	$\langle\overline{H'_1}, \overline{K_3}\rangle$
$\langle\overline{H'_2}, \overline{K_2}\rangle$	$\langle\overline{H'_2}, \overline{K_2}\rangle$	$\langle\overline{H'_1}, \overline{K_3}\rangle$
$\langle\overline{H'_2}, \overline{K_3}\rangle$	$\langle\overline{H'_2}, -\rangle$	$\langle\overline{H'_1}, -\rangle$
$\langle\overline{H'_3}, \overline{K_1}\rangle$	$\langle\overline{H'_3}, \overline{K_1}\rangle$	$\langle\overline{H'_1}, \overline{K_2}\rangle$

$\langle \overline{H'_3}, \overline{K_2} \rangle$	$\langle \overline{H'_3}, \overline{K_2} \rangle$	$\langle \overline{H'_1}, \overline{K_3} \rangle$
$\langle \overline{H'_3}, \overline{K_3} \rangle$	$\langle \overline{H'_3}, \overline{K_3} \rangle$	$\langle \overline{H'_1}, \overline{K_2} \rangle$

Докажем, что CD покрывает автомат A. Для начала докажем, что CD покрывает A'.

Определим отображение $\eta_1 : T^{CD} \to S^{A'} : \langle \overline{H'_i}, \overline{K_j} \rangle \to H'_i \cap K_j$, для которого

$$T^{CD} = S^{CD} \setminus \{ \langle \overline{H_2}, \overline{K_3} \rangle \}.$$

Изобразим действие этой функции в табл. 9.

Таблица 9

Действие функции η_1

$\langle \overline{H'_1}, \overline{K_1} \rangle$	$\langle \overline{H'_1}, \overline{K_2} \rangle$	$\langle \overline{H'_1}, \overline{K_3} \rangle$	$\langle \overline{H'_2}, \overline{K_1} \rangle$	$\langle \overline{H'_2}, \overline{K_2} \rangle$	$\langle \overline{H'_3}, \overline{K_1} \rangle$	$\langle \overline{H'_3}, \overline{K_2} \rangle$	$\langle \overline{H'_3}, \overline{K_3} \rangle$
$\langle 1, \overline{H_1} \rangle$	$\langle 4, \overline{H_1} \rangle$	$\langle 5, \overline{H_1} \rangle$	$\langle 2, \overline{H_1} \rangle$	$\langle 4, \overline{H_1} \rangle$	$\langle 3, \overline{H_3} \rangle$	$\langle 5, \overline{H_3} \rangle$	$\langle 6, \overline{H_3} \rangle$

Можно проверить, что $h_x^A \eta_1 = \eta_1 h_x^{CD}$, то есть CD ≥ A`.

Автомат A' покрывает A и действие функции $\eta_2 : S^{A`} \to S^A : \langle s^A, \overline{H_i} \rangle \to s^A$ отображено в табл. 10.

Таблица 10

Функция η_2

$\langle 1, \overline{H_1} \rangle$	$\langle 2, \overline{H_2} \rangle$	$\langle 3, \overline{H_3} \rangle$	$\langle 4, \overline{H_1} \rangle$	$\langle 4, \overline{H_2} \rangle$	$\langle 5, \overline{H_1} \rangle$	$\langle 5, \overline{H_3} \rangle$	$\langle 6, \overline{H_3} \rangle$
1	2	3	4	4	5	5	6

Таким образом, функция η:

$$T^{CD} \to S^A, \ \eta = \eta_2 \eta_1,$$

эта функция задается в табл. 11.

Таблица 11

Функция η

$\langle \overline{H'_1}, \overline{K_1} \rangle$	$\langle \overline{H'_1}, \overline{K_2} \rangle$	$\langle \overline{H'_1}, \overline{K_3} \rangle$	$\langle \overline{H'_2}, \overline{K_1} \rangle$	$\langle \overline{H'_2}, \overline{K_2} \rangle$	$\langle \overline{H'_3}, \overline{K_1} \rangle$	$\langle \overline{H'_3}, \overline{K_2} \rangle$	$\langle \overline{H'_3}, \overline{K_3} \rangle$
1	4	5	2	4	3	5	6

Легко заметить, что условие покрытия выполнено:

$$h^A_{x_1}\eta\left\langle\overline{H'_i},\overline{K_j}\right\rangle=\eta h^{CD}_{x_1}\left\langle\overline{H'_i},\overline{K_j}\right\rangle,$$

поскольку функция $h^A_{x_1}\eta$ задается в табл. 12.

Таблица 12

Функция $h^A_{x_1}\eta$

$\left\langle\overline{H'_1},\overline{K_1}\right\rangle$	$\left\langle\overline{H'_1},\overline{K_2}\right\rangle$	$\left\langle\overline{H'_1},\overline{K_3}\right\rangle$	$\left\langle\overline{H'_2},\overline{K_1}\right\rangle$	$\left\langle\overline{H'_2},\overline{K_2}\right\rangle$	$\left\langle\overline{H'_3},\overline{K_1}\right\rangle$	$\left\langle\overline{H'_3},\overline{K_2}\right\rangle$	$\left\langle\overline{H'_3},\overline{K_3}\right\rangle$
5	4	5	2	4	3	5	6

Функция $\eta h^{CD}_{x_1}$ задается в табл. 13.

Таблица 13

Функция $\eta h^{CD}_{x_1}$

$\left\langle\overline{H'_1},\overline{K_1}\right\rangle$	$\left\langle\overline{H'_1},\overline{K_2}\right\rangle$	$\left\langle\overline{H'_1},\overline{K_3}\right\rangle$	$\left\langle\overline{H'_2},\overline{K_1}\right\rangle$	$\left\langle\overline{H'_2},\overline{K_2}\right\rangle$	$\left\langle\overline{H'_3},\overline{K_1}\right\rangle$	$\left\langle\overline{H'_3},\overline{K_2}\right\rangle$	$\left\langle\overline{H'_3},\overline{K_3}\right\rangle$	$\left\langle\overline{H'_2},\overline{K_3}\right\rangle$
5	4	5	2	4	3	5	6	–

Таким образом, *декомпозиция автомата A* построена.

Глава 5. ПЕРИОДИЧНОСТЬ ФУНКЦИОНИРОВАНИЯ КОНЕЧНЫХ АВТОМАТОВ[2]

В работе В. М. Фомичева отмечено, что «одним из важных прикладных вопросов в теории конечных автоматов является периодичность функционирования автомата» [34]. Известно также, что по разным причинам в последнее время получили широкое распространение поточные многоалфавитные шифры [1]. При реализации этих шифров используют так называемый управляющий блок, который вырабатывает последовательность номеров шифрующих преобразований – управляющую гамму. Согласно А. П. Алферову и авторам [1], одно из важнейших требований к управляющему блоку состоит в том, что «период управляющей гаммы должен превышать максимально возможную длину открытых сообщений, подлежащих шифрованию». Кроме того, в различных системах обеспечения безопасности широко применяются генераторы псевдослучайных последовательностей [14]. Так, например, эти генераторы используются в синхронных поточных криптосхемах.

Напомним, что основным результатом по оценке снизу периодов выходных последовательностей конечных автоматов, отвечающих их начальным состояниям и входным периодическим последовательностям является результат, представленный в теореме 2.2. работы [33] и состоящий в том, что минимальный период W выходной последовательности автомата не превосходит величины $k\omega$, где k – число состояний автомата, а ω – минимальный период входной последовательности. В [13] и [20] приведены утверждения, суть которых состоит в том, что W является делителем числа $k`\omega$ при некотором $k` \le k$.

Проблема нахождения нижней оценки периодов выходных последовательностей конечных автоматов при заданных начальном состоянии и входной периодической последовательности является очень сложной. Естественным подходом к ее удовлетворительному решению является выделение тех или иных классов автоматов в качестве объектов исследований. Например, ряд работ посвящен вопросам периодичности выходных последовательностей линейных автономных автоматов, в частности, в этом классе выделяются ра-

[2] Излагаемые в данной главе положения базируются на результатах работ автора, а также дипломника МГУ им. М. В. Ломоносова М. В. Шамшурина.

боты, в которых указываются способы построения линейных рекуррентных последовательностей максимального периода в разнообразных алгебраических структурах.

5.1. Вспомогательное почти тривиальное утверждение

Для любых натуральных чисел a, b из условия (a, b) = d следует: существуют натуральные числа n(1), n(2), при которых

$$an(1) - bn(2) = d.$$

Доказательство. Очевидно, достаточно доказать это утверждение в случае d = 1. Действительно, пусть (a, b) = d и утверждение справедливо при d = 1. Тогда $(\frac{a}{d}, \frac{b}{d}) = 1$, следовательно, найдутся натуральные числа n(1), n(2), при которых $\frac{a}{d}n(1) - \frac{b}{d}n(2) = 1$, где d – тоже натуральное число. Но тогда при натуральных числах n(1), n(2) получаем

$$an(1) - bn(2) = d.$$

Докажем теперь наше утверждение для случая d = 1. Для натуральных чисел a, b имеем

$$(a, b)=1.$$

Рассмотрим следующие возможные случаи:

a<b, a>b, a=b.

В случае a<b в кольце вычетов {0, 1, 2, …, b–1} по модулю b в силу (a, b)=1 для a найдется обратный элемент $n(1) \in \{1, 2, \ldots, b-1\}$:

$$an(1) \equiv 1 \pmod{b}.$$

Возможны два варианта: 1) an(1) – 1 ≠ 0; 2) an(1) – 1 = 0. В первом случае найдется натуральное число n(2), при котором an(1) – 1 = bn(2). Таким образом, в случае 1) доказано, что an(1) – bn(2) = 1 при натуральных числах n(1), n(2). Во втором случае получаем an(1) = 1, следовательно, a = 1 и n(1) = 1. Рассмотрим тождество

$$b + 1 - b = 1.$$

Положим n(1) = b+1, n(2) = 1. Тождество для введенных значений переписываем в виде

$$an(1) - bn(2) = 1.$$

Это равенство и требовалось доказать для рассматриваемого случая.

Пусть a>b, (a, b) = 1. Положим a = kb+r, r<b, к – натуральное число. Если r = 0, то a = 1. Имеем b+1–b =1. Полагая n(1) = b+1, n(2) = 1, получаем

an(1) – bn(2) = 1.

Если r≠0, то из (a,b) = 1 следует (r, b) =1. Для r, b мы попадаем в рамки доказанного выше случая r<b, r и b – натуральные числа. Поэтому для них найдутся натуральные числа n(1), n(2), при которых

$$rn(1) – bn(2) = 1.$$

Тогда

$$rn(1) + kbn(1) – kbn(1) – bn(2) = 1;$$
$$(r +kb)n(1) – b(kn(1) + n(2)) = 1;$$
$$an(1) – b(kn(1) + n(2)) = 1.$$

Числа n(1) и kn(1) + n(2) – натуральные. Мы получили требуемое равенство для a, b.

Рассмотрим случай a = b. По условию (a,b) = 1, поэтому a = b = 1. Записываем 2 – 1 = 1. Полагаем n(1) = 2, n(2) = 1, получаем

$$an(1) – bn(2) = 1.$$

Доказательство вспомогательного утверждения завершено.

5.2. Основные теоретико-автоматные обозначения

Пусть A = (X, S, Y, h, f) – конечный автомат |X|≥2, |Y|≥2. Наряду с введенными функциями h, f автомата будем в случае необходимости использовать и его частичные функции переходов $(h_x)_{x\in X}$ и выходов $(f_x)_{x\in X}$, h_x: S→S, f_x: S→Y. Пусть, как и ранее:

– X* – множество всех слов конечной длины в алфавите X;

– $A_M(s, P) = s_1, s_2, \ldots, s_j, \ldots$ – последовательность состояний автомата A, отвечающая его входной последовательности P и начальному состоянию s = s_1 из S;

– $A(s, P) = y_1, y_2, \ldots, y_j, \ldots$ – выходная последовательность автомата A;

– для P = x(1), x(2), …, x(j), … и s∈S:

$s_j = h_{x(j-1)}\ldots h_{x(1)}s_1$, $y_j = f_j\, h_{x(j-1)}\ldots h_{x(1)}s_1$,

(ω, ω`) – наибольший общий делитель чисел ω, ω`,

D|ω – D делит ω.

Под периодической последовательностью элементов конечного алфавита Y ниже понимается чисто периодическая последовательность $y_1, y_2, ..., y_j, ...$: существует d, при котором $y_j = y_{j+d}$, j∈{1, 2, ...}.

Под периодом последовательности понимается ее минимальный период.

Через $A\langle s\rangle = (X, S_s, Y, h, f)$ обозначим связную компоненту автомата A, порожденную состоянием $s \in S$.

5.3. Оценка периодов последовательностей состояний автомата при заданной периодической входной последовательности

Теорема 1. Если для перестановочного автомата $A = (X, S, Y, h, f)$ при любых $x, x' \in X$, $x \neq x'$ и любом $s \in S_{s_1}$ выполнено $h_x s \neq h_{x'} s$, то период t последовательности состояний $A_M(s_1, P) = s_1, s_2, \ldots, s_j, \ldots$ кратен периоду ω входной последовательности $P = x(1), x(2), \ldots$.

Доказательство. Так как автомат A – перестановочный ($(h_x)_{x \in X}$ – биекции S в S), то $A_M(s_1, P) = s_1, s_2, \ldots, s_j, \ldots$ – чисто периодическая последовательность. Пусть $(\omega, t) = d$. По определению функции перехода

$$h_{x(j)} s_j = s_{j+1}.$$

Так t период последовательности $A_M(s_1, P)$, то при любом k и любом j

$$s_{j+1} = s_{j+1+kt}.$$

Поэтому

$$h_{x(j+kt)} s_{j+kt} = s_{j+1+kt} = s_{j+1}.$$

Так как $(\omega, t) = d$, то существуют натуральные числа k(1), k(2) такие, что

$$k(2)t - k(1)\omega = d.$$

Или, что то же самое, $ck(2)t - ck(1)\omega = cd$ при любом c. Положим $k = ck(2)$, тогда получим $kt = cd + ck_1\omega$, и так как ω – период входной последовательности P, то $x(j+cd+ck(1)\omega) = x(j+cd)$. Поэтому из

$$h_{x(j+cd+ck(1)\omega)} s_{j+k} = h_{x(j)} s_j,$$

следует

$$h_{x(j+cd)} s_{j+kt} = h_{x(j+cd)} s_j = h_{x(j)} s_j.$$

По условию это возможно только при

$$x(j+cd) = x(j).$$

Так как c, j – произвольные постоянные, то период ω делит $d = (\omega, t)$, следовательно, t кратно ω. Теорема доказана.

Определение 1. Состояние s автомата $A = (X, S, Y, h, f)$ называется внутренне автономным состоянием, если для любой пары слов

одинаковой длины P = x(1), x(2), ..., x(t), P` = x`(1), x`(2), ..., x`(t) из X*

$$h_{x(j)}h_{x(j-1)}...h_{x(1)}s = h_{x`(j)}h_{x`(j-1)}...h_{x`(1)}s.$$

Приводимые ниже теоремы ранее были получены В. А. Башевым и позднее обобщены автором (А. В. Бабаш) на случай приближенных и локальных периодов.

Теорема 2. Пусть ω – простое число и P = x(1), x(2), … – входная последовательность перестановочного автомата A = (X, S, Y, h, f) периода ω, содержащая все буквы алфавита X. Если автомат $A<s_1> = (X, S_{s_1}, Y, h, f)$ не имеет внутренне автономных состояний, то последовательность состояний $A_M(s_1,P) = s_1, s_2, \ldots, s_j, ...$ имеет период, кратный ω.

Доказательство. Из условий теоремы вытекает, что последовательность $A_M(s_1, P) = s_1, s_2, \ldots, s_j, \ldots$ – периодическая. Пусть t ее период, и предположим, что t не кратно ω. Тогда, в силу простоты числа ω, имеем (ω, t) = d = 1. Как и при доказательстве теоремы 1, получим

$$s_{j+1} = s_{j+1+kt},$$
$$h_{x(j+kt)}s_j = h_{x(j)}s_j.$$

Так как (ω, t) = d = 1, то существуют натуральные числа k(1), k(2) такие, что

$$k(2)t - k(1)\omega = 1.$$

Или, что то же самое ck(2)t – ck(1)ω = c при любом c. Положим k = ck(2), тогда получим $kt = c+ck_1\omega$ и, так как ω – период входной последовательности P, то x(j+c+ck(1)ω) = x(j+c). Поэтому

$$h_{x(j+c)}s_j = h_{x(j)}s_j$$

при любом c и любом j. Так как последовательность P содержит все буквы алфавита, то из последнего равенства получаем

$$h_x s_j = h_{x'}s_j$$

при любых x, x’∈X, что равносильно внутренней автономности состояния s_1 автомата A. Получили противоречие с условиями теоремы. Следовательно, t кратно ω. Теорема доказана.

Обобщите утверждения теорем на случай произвольных автоматов.

Глава 6. ГОМОМОРФИЗМЫ НЕАВТОНОМНЫХ ДВОИЧНЫХ РЕГИСТРОВ СДВИГА[3]

6.1. Основные понятия

Пусть имеются два автомата Мура $A = (X, S, Y, h, \lambda)$ и $A' = (X', S', Y', h', \lambda')$, где X, X' – входные алфавиты, S, S'– множества состояний, Y, Y' – выходные алфавиты, h, h' – функции перехода, λ, λ'– функции выхода. Напомним, что автомат A гомоморфно отображается на автомат A', если существуют сюръективные отображения (ψ, φ, η):

$\psi: X \to X'$, $\varphi: S \to S'$, $\eta: Y \to Y'$,

такие, что для любых $s \in S$ и $x \in X$

$\varphi(h(s,x)) = h'(\varphi(s), \psi(x))$,

$\eta(\lambda(s)) = \lambda'(\varphi(s))$.

При этом тройка отображений (ψ,φ,η) называется гомоморфизмом автомата A на A'. В случае, когда (ψ,φ,η) – биекции, гомоморфизм называют изоморфизмом, а автоматы называют изоморфными. В данном пункте, говоря о гомоморфизмах, мы будем предполагать, что $|S| > |S'| > 1$, $|Y| = |Y'|$.

Понятие гомоморфизма, как Вы знаете, определено и *для автоматов без выхода*. В этом случае рассматривается лишь отображения ψ и φ при этом требуется выполнение лишь условия

$$\varphi(h(s, x)) = h'(\varphi(s), \Psi(x)).$$

Докажите, что перестановочный автомат $A = (X, S, Y, h , \lambda)$, имеющий транзитивную группу $G = \langle (h_x)_{x \in X} \rangle$, порожденную частичными функциями перехода $\{h_x, x \in X\}$, имеет гомоморфный образ $A' = (X', S', Y', h', \lambda')$, $|S'| < |S|$ тогда и только тогда, когда группа G импримитивна и функция λ постоянна на каждом блоке некоторой системы импримитивности группы G.

Это утверждение переносится и на случай гомоморфизма автоматов без выхода путем исключения условий на функцию выхода λ. Заметим, что если (ψ, φ, η) – гомоморфизм автомата A на A', указанная в утверждении система блоков будет служить системой полных прообразов состояний автомата A' при отображении φ.

---

[3] В. И. Солодовников любезно предоставил автору основные материалы данного раздела. Он же высказал ряд полезных замечаний, которые были полностью учтены.

Пусть F_2 поле из двух элементов $\{0, 1\}$, F_2^n – координатное векторное пространство над F_2. Обозначим через $\Psi(x_1, x_2, \ldots, x_n)$ произвольную двоичную функцию на F_2^n. Напомним, что неавтономным регистром сдвига (без выхода) с обратной связью Ψ называется автомат $A = (X, S, (h_x^\psi)_{x\in X})$, где $X = F_2$, $S = F_2^n$,

$$h_0^\psi(v_1, v_2, \ldots, v_n) = (v_2, \ldots, v_n, \Psi(v_1, \ldots, v_n)),$$

$$h_1^\psi(v_1, v_2, \ldots, v_n) = (v_2, \ldots, v_n, 1\oplus\Psi(v_1, \ldots, v_n)),$$

$$(v_1, v_2, \ldots, v_n) \in F_2^n.$$

Перестановочный регистр сдвига называют регулярным регистром сдвига. Докажите, что регистр сдвига с функцией обратной связи Ψ будет регулярным регистром сдвига, тогда и только тогда, когда функция Ψ имеет вид

$$\Psi(x_1, \ldots, x_n) = \Phi(x_2, \ldots, x_n)\oplus x_1.$$

Ниже говоря о гомоморфизмах регистра сдвига, мы будем иметь ввиду внутренние сюръективные гомоморфизмы (гомоморфизмы по состояниям), то есть сюръективные гомоморфизмы вида (E, φ), где $E: F_2 \to F_2$ – тождественное отображение. Ниже рассматриваются лишь регулярные регистры сдвига. Такой регистр с обратной связью $\Phi(x_2, \ldots, x_n)\oplus x_1$ далее будет обозначаться через *РС(Ф, n).*

6.2. Теорема А. Я. Прососова

Теорема А. Я. Прососова. Если автомат $A' = (X', S', h')$, $|S'|>1$ является гомоморфным образом регулярного неавтономного регистра сдвига $РС(\Phi, n) = (X, S, h)$, $|S'|<|S|$ при некотором гомоморфизме (E, φ), то он изоморфен некоторому неавтономному регулярному регистру сдвига.

Доказательство. Пусть φ – гомоморфизм автомата $РС(\Phi, n)$ на автомат A'. Тогда группа $G_{РС(\Phi, n)}$ неавтономного регистра сдвига $РС(\Phi, n)$ – импримитивна. Рассмотрим систему $\{\phi^{-1}(s^{A'}) : s^{A'} \in S^{A'}\}$ блоков импримитивности группы $G_{РС(\Phi, n)}$, соответствующую гомоморфизму φ.

Так как группа $G_{РС(\Phi, n)}$ регистра сдвига транзитивна, то мощность каждого блока есть число $2^к$, где $1<к<n$. Обозначим блоки $\{\phi^{-1}(s^{A'}) : s^{A'} \in S^{A'}\}$ через $W(0), W(1), \ldots, W(2^{n-к}-1)$. Будем считать, что $(0, 0, 0, \ldots, 0)\in W(0)$.

Докажите, что можно считать, что $h_o(W(0)) = W(0)$. Для этого докажите, что регистр РС(Ф, n) изоморфен регистру РС(Ф⊕1, n). Поэтому без ограничения общности можно считать, что Ф(0, 0, 0, …, 0) = 0. Следовательно, $h_o(W(0)) = W(0)$.

Пронумеруем векторы в каждом блоке системы импримитивности числами от 1 до $2^к$:

$$W(i) = \{V^j(i): j\in\{1, \ldots, 2^к\}\} =$$

$$= \{(v^j{}_1(i), v^j{}_2(i), \ldots, v^j{}_n(i)): \ j\in\{1, \ldots, 2^к\}\}, \ i\in\{0, \ldots, 2^{n-к}-1\}.$$

Обозначим через $W_a{}^r(i)$ следующую систему векторов:

$$W_c{}^r(i) = \{V_c{}^{j,\,r}(i): j\in\{1, \ldots, 2^к\}\} = \{(v_c{}^j(i), v^j{}_{c+1}(i), \ldots, v^j{}_{c+r-1}(i):$$

$$j\in\{1, \ldots, 2^к\}\}, \ 1\le c\le n-r+1.$$

Докажите следующий факт: система векторов $W_1{}^к$ (0) совпадает с пространством $F_2{}^к$ размерности k над полем F_2.

Построим отображение θ пространства $F_2{}^n$ на пространство $F_2{}^{n-к}$, постоянное на блоках W_0, W_1, …, $W_{2^{n-k}-1}$ импримитивности группы $G_n(Ф)$ и такое, что преобразования $h^\wedge{}_x = \theta h_x^{\Phi} \theta^{-1}$ являются частичными функциями перехода неавтономного регистра сдвига, где $\theta^{-1}(v)$ – прообраз некоторого элемента v из $F_2{}^{n-к}$.

Тогда изоморфное отображение ν множества состояний автомата A’ на пространство $F_2{}^{n-к}$, являющееся множеством состояний регистра сдвига, можно задать следующим образом: $\varphi(W_i) \overset{\nu}{\leftrightarrow} \theta(W_i)$. Отображение ν осуществляет изоморфное отображение автомата A’ на некоторый неавтономный регистр сдвига.

Напомним, что $h_0(W(0)) = W(0)$. Так как в силу доказанного Вами факта, в совокупности векторов $W_1{}^к(0)$ каждый вектор из пространства $F_2{}^к$ встречается ровно по одному разу, то легко доказать, что преобразование h_0 индуцирует некоторое преобразование пространства $F_2{}^к = W_1{}^к(0)$. Докажите, что это преобразование является биекцией, реализуемой некоторым регулярным регистром сдвига длины k. Поэтому для некоторой двоичной функции ω от k–1 переменных имеем равенство:

$$v_{k+1}^j(0) = v_1^j(0) + \omega(v_2^j(0), v_3^j(0), \ldots, v_k^j(0)). \qquad (7)$$

Двоичная функция ω представляет собой обратную связь построенного регистра сдвига РС(k) на множестве состояний $F_2{}^к$.

Определим *отображение* θ пространства $F_2{}^n$ в пространство $F_2{}^{n-к}$ следующим образом: вектор $(v_1, v_2, \ldots, v_n)$ переходит в

$$(v_1+\omega(v_2, \ldots, v_k)+ v_{к+1}, v_2 +\omega(v_3, \ldots, v_{к+1})+v_{k+2}, \ldots,$$

$$v_{n-k}+\omega(v_{n-k+1}, \ldots, v_{n-1})+v_n) \qquad (8)$$

Докажите, что это гомоморфизм РС(Ф, n) на РС(k). Для этого сначала докажите, что отображение θ постоянно на блоке W(0) и отображает каждый вектор из W(0) в нулевой вектор. Будем говорить, что блок W(j) находится на расстоянии C от блока W(0), если C – минимальная длина слова произведения $h_{\varepsilon_1}, h_{\varepsilon_2}, \ldots, h_{\varepsilon_C}$, переводящего блок W(0) в W(j).

Докажем теперь, что θ постоянно и на любом другом блоке. Допустим, что это не так. Пусть отображение θ непостоянно на некоторых блоках и W(i) такой блок, что θ не постоянно на W(i) и W(i) находится на минимальном расстоянии C от W(0) среди всех блоков, на которых θ не постоянно. Тогда, как нетрудно увидеть, в блоке W(i) найдутся два вектора $V^{j_1}(i)$ и $V^{j_2}(i)$ такие, что $\theta V^{j_1}(i) \neq \theta V^{j_2}(i)$. Из условия минимальности C следует, что $\theta V^{j_1}(i)$ отличается от $\theta V^{j_2}(i)$ по последней координате. Проверим это. Если это не так, то блок $h_{\varepsilon_C}(W(i))$ находится на расстоянии C–1 от W(0) и отображение θ на этом блоке не постоянно. Это противоречит выбору области W(i). Следовательно,

$$v_{n-k}^{j_1}(i)+\omega(v_{n-k+1}^{j_1}(i), v_{n-k+2}^{j_1}(i), \ldots, v_{n-1}^{j_1}(i))+v_n^{j_1}(i) \neq$$

$$\neq v_{n-k}^{j_2}(i)+\omega(v_{n-k+1}^{j_2}(i), v_{n-k+2}^{j_2}(i), \ldots, v_{n-1}^{j_2}(i))+v_n^{j_2}(i). \qquad (9)$$

В силу доказанного вами факта (9) вектор $v_{n-k}^{j_1}(i), v_{n-k+1}^{j_1}(i), \ldots, (i)$ содержится в совокупности векторов $W_1^{\kappa}(0)$:

$(v_{n-k}^{j_1}(i), v_{n-k+1}^{j_1}(i), \ldots, v_{n-1}^{j_1}(i)) = (v_1^{\alpha}(0), v_2^{\alpha}(0), \ldots, v_k^{\alpha}(0))$.

Обозначим через τ_n подстановку $(h_0)^{-1}h_1$. Предположим, что $v_{k+1}^{\alpha}(0) \neq v_n^{j_1}(i)$. Тогда из (8) и (9) вытекает, что в блоке $\tau_n W(i)$ найдутся два вектора, значения θ на которых различаются по последней координате, так как из

$\theta V^{j_1}(i) \neq \theta V^{j_2}(i)$

вытекает

$\theta\tau_n V^{j_1}(i) \neq \theta\tau_n V^{j_2}(i)$.

Следовательно, можно считать, что $v_{k+1}^{\alpha_1}(0) = v_n^{j_1}(i)$. Докажите теперь, что найдется двоичная последовательность $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{n-к-1}$ длины n–к–1 такая, что $h_{\varepsilon_1}, h_{\varepsilon_2}, \ldots, h_{\varepsilon_{n-k-1}} = \zeta$ переводит вектор $V^{j_1}(i)$ в вектор $V^{\alpha}(i)$. Вследствие этого $\zeta(W(i)) = W(0)$. Поэтому векторы $\theta\zeta(V^{j_1}(i))$ и $\theta\zeta(V^{j_2}(i))$ будут различаться по первой координате и

$\zeta(V^{j_1}(i))$, $\zeta(V^{j_2}(i)) \in W(0)$, что противоречит соотношению (7). Таким образом доказано, что отображение θ постоянно на всех блоках W_i, $i \in \{0, \ldots, 2^{n-\kappa}-1\}$. Теперь докажите, что из равенства (8) следует, что преобразования $\theta h_x \theta^{-1}$ пространства $F_2^{n-\kappa}$ являются преобразованиями регистра сдвига. Доказательство теоремы завершено.

6.3. Теорема В. А. Башева

Теорема В. А. Башева. Неавтономный регулярный регистр сдвига РС(Ф, n) гомоморфен регулярному регистру сдвига с 2^k состояниями, тогда и только тогда, когда функция $\Phi(x_2, \ldots, x_n)$ представима в виде

$$\Phi(x_2, \ldots, x_n) = x_{k+1} + \omega(x_{k+2}, x_{k+3}, \ldots, x_n) + \omega(x_2, x_3, \ldots, x_{n-k}) + x_{n-k+1}$$

$$+ \Phi''(x_2+\omega(x_3,x_4, \ldots, x_{n-k+1}) + x_{n-k+2},$$

$$x_3 + \omega(x_4, x_4, \ldots, x_{n-k+2}) + x_{n-k+3}, \ldots, x_k + \omega(x_{k+1}, x_{k+2}, \ldots, x_{n-1}) + x_n)),$$

где ω, Φ'' – некоторые двоичные функции от n–k–1 и k–1 переменных.

Докажите теорему самостоятельно.

При доказательстве теоремы А. Я. Прососова использовалось утверждение: система векторов $W_1^{\kappa}(0)$ совпадает с пространством F_2^{κ} размерности k над полем F_2.

Приведем его доказательство. Так как $h_o(W(0)) = W(0)$, то

$$W_a^r(0) = W_b^r(0)$$

для любых r, c, b таких, что $1 \le r \le n$, $1 \le c \le n-r+1$, $1 \le b \le n-r+1$.

Пусть L – максимальное число такое, что $W_1^L(0)$ содержит два одинаковых вектора, причем если $W_1^L(0)$ содержит все различные векторы, то $L=0$. Для доказательства утверждения нам будет достаточно показать, что $W^{L+1}{}_1(0)$ совпадает с пространством $F^{\kappa}{}_2$. Отсюда сразу будет следовать, что $L+1 = k$. Заметим, что при $L = 0$ утверждение очевидно.

Из максимальности L следует, что в $W^{L+1}{}_1(0)$ найдутся два вектора $V_1^{j_1,L+1}(0)$ и $V_1^{j_2,L+1}(0)$ такие, что $v_k^{j_1}(0) = v_k^{j_2}(0)$ при $1 \le k \le L$, и $v_{L+1}^{j_1}(0) = v_{L+1}^{j_2}(0) \oplus 1$.

Докажите, что подстановка $\tau_n = (h_o)^{-1} h_1$, принадлежат группе регистра РС(Ф,n) и осуществляет преобразование вида:

$$\tau_n(v_1, v_2, \ldots, v_n) = (v_1 \oplus 1, v_2, \ldots, v_n).$$

Поскольку $W^{L+1}_{n-L}(0)=W^{L+1}{}_1(0)$, то $(v^{j_1}_1(0), v^{j_1}_2(0), \ldots, v^{j_1}_{L+1}(0)) \in W^{L+1}_{n-L}(0)$.

Пусть $V^m(0) = (v^m_1(0), v^m_2(0), \ldots, v^m_n(0)) =$

$= (v^m_1(0), v^m_2(0), \ldots, v^m_{n-L-1}(0), v^{j_1}_1(0), v^{j_1}_2(0), \ldots, v^{j_1}_{L+1}(0))$.

Тогда легко заметить, что существует слово $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{n-L-1}$; $\varepsilon_i \in \{0, 1\}$ такое, что подстановка $h_{\varepsilon_1} h_{\varepsilon_2} h_{\varepsilon_{n-L-1}}$ переводит вектор $\tau_n(V^m(0))$ в вектор $V^{j_2}(0)$. Следовательно, подстановка $h_{\varepsilon_1} h_{\varepsilon_2} \ h_{\varepsilon_{n-L-1}} \tau_n$ оставляет область W(0) на месте. Поэтому, если в системе векторов $W^{L+1}_{n-L}(0)$ содержится вектор $(y_1, y_2, \ldots, y_{L+1})$, то в $W^{L+1}_1(0)$ содержится вектор $(y_1, y_2, \ldots, y_{L+1} \oplus 1)$, а так как $W^{L+1}_1(0) = W^{L+1}_{n-L}(0)$, то в блоке $W^{L+1}_1(0)$ вместе с каждым вектором $(v^j_1(0), v^j_2(0), \ldots, v^j_{L+1}(0))$ содержится и вектор $(v^j_1(0), v^j_2(0), \ldots, v^j_l(0), v^j_{l+1}(0) \oplus 1)$. Так как $h_0(W(0)) = W(0)$, то $W^{l+1}_1(0)$ содержит также и вектор $(v^j_2(0), v^j_3(0), \ldots, v^j_{L+1}(0), v^j_{L+2}(0))$.

Таким образом, мы показали, что из $(y_1, y_2, \ldots, y_{L+1}) \in W^{L+1}_1(0)$ вытекает, что $(y_2, y_3, \ldots, y_{L+1}, \varepsilon) \in W^{L+1}_1(0)$ для некоторого $\varepsilon \in F_2$ и $(y_1, y_2, \ldots, y_L, y_{L+1} \oplus 1) \in W^{L+1}_1(0)$. Отсюда сразу следует, что любой вектор $(\alpha_1, \alpha_2, \ldots, \alpha_{L+1})$ из F^{L+1}_2 принадлежит системе $W^{L+1}_1(0)$. Так как L было выбрано максимально возможным, то каждый вектор в совокупности $W^{L+1}_1(0)$ встречается не более одного раза и, следовательно, $W^{L+1}_1(0) = F^{\kappa}_2$, $k = L+1$, что и доказывает утверждение.

В связи с весьма неожиданным результатом, полученным в теореме А. Я. Прососова, представляют интерес и другие результаты в этом направлении. Мы приводим эти результаты в обзорном виде, сохранив авторство В. И. Солодовникова даже в обозначениях, сознавая, что у читателя наверняка возникнет в связи с новыми обозначениями определенное неудобство.

6.4. Обзор по работе В. И. Солодовникова «Гомоморфизмы двоичных регистров сдвига»

В. И. Солодовников рассматривает гомоморфизмы двоичных регистров сдвига с линейной по входной переменной функцией обратной связи, то есть гомоморфизмы автоматов, вырабатывающих

двоичные линейно управляемые усложненные *рекуррентные* последовательности. Доказывается, что всякий гомоморфизм такого регистра разлагается в композицию гомоморфизма на регистр и некоторого гомоморфизма, близкого к изоморфизму. При описании этого разложения основную роль играет некая операция, распространяющая операцию произведения многочленов на множество всех двоичных функций. Вопрос о гомоморфизмах регистра сводится к вопросу о поиске общих делителей его функции обратной связи и выходной функции.

Приняты следующие обозначения и терминология:

V_n – множество всех двоичных строк длины n, $n \geq 0$.

F_n – множество всех двоичных функций от n переменных. Функции из F_n мы будем отождествлять с представляющими их многочленами Жегалкина от переменных $x_1, \ldots, x_n$.

F_{n+1} – множество всех линейных по последней (то есть $(n+1)$-й) переменной функций из F_{n+1}, то есть функций вида $f=f^*\oplus x_{n+1}$, где $f^* \in F_n$.

Через $\psi\varphi$ обозначается композиция отображений, при которой φ действует первым. Аналогично, BA – последовательное соединение автоматов A и B, при котором выход с автомата A подается на вход автомата B.

Следуя терминологии работы [39], двоичным *регистром сдвига длины n с функцией обратной связи f и выходной функцией h*, где $f, h \in F_{n+1}$, будем называть автомат $R(h, f) = (V_1, V_n, V_1, \rho, \mu)$, у которого функция переходов ρ и функция выходов μ определяются равенствами

$$\rho((x_1, \ldots, x_n), x) = (x_2, \ldots, x_n, f(x_1, \ldots, x_n, x));$$

$$\mu((x_1, \ldots, x_n), x) = h(x_1, \ldots, x_n, f(x_1, \ldots, x_n, x))$$

для любых $x_1, \ldots, x_n, x \in V_1$. Регистр сдвига без выхода с функцией обратной связи f будем обозначать через $R(f)$.

Обозначим также

$$R_0(h) = R(h, x_{n+1}),$$

$$R'(f) = R(x_{n+1}, f).$$

Автомат $A = (X, S, Y, \delta, \lambda)$ (здесь δ: S×X→S, λ: S×X→Y) называется *обратимым*, если все его автоматные отображения биективны, что равносильно биективности частичной функции выходов λ_s (λ_s(x) = λ(s,x)) для всех $s \in S$. В этом случае *обратным* к автомату A называется автомат $A^{-1} = (Y, S, X, \delta', \lambda')$, где $\delta'(s, y) = \delta(s, \lambda_s^{-1}(y))$,

$\lambda'(s,y)=\lambda_s^{-1}(y)$ для всех $s\in S$, $y\in Y$. В частности, для f, $h\in F_{n+1}$ *регистр* $R(h, f)$ *обратим тогда и только тогда, когда* $f,h\in F^*_{n+1}$. *При этом* $R(h, f)^{-1}=R(f, h)$ *и, следовательно,* $R'(f)^{-1}=R_0(f)$.

Как и в [30], для любых $n_i\geq 0$, $f_i\in F_{n_i+1}$, $i=1, 2$ определим функцию $f_2\triangleleft f_1\in F_{n_1+n_2+1}$ и отображение $\pi_{f_1,n_2}: V_{n_1+n_2}\to V_{n_2}$ равенствами:

$$f_2\triangleleft f_1(x_1,\ldots,x_{n_1+n_2+1}) = f_2(f_1(x_1,\ldots,x_{n_1+1}), f_1(x_2, \ldots, x_{n_1+2}), \ldots, f_1(x_{n_2+1}, \ldots, x_{n_1+n_2+1})),$$

$$\pi_{f_1,n_2}(x_1, \ldots, x_{n_1+n_2}) = (f_1(x_1, \ldots,x_{n_1+1}), f_1(x_2,\ldots,x_{n_1+2}),\ldots,f_1(x_{n_2},\ldots,x_{n_1+n_2}))$$

для любых $x_1, \ldots, x_{n_1+n_2+1}\in V_1$, так что $f_2\triangleleft f_1=f_2\pi_{f_1,n_2+1}$.

Ниже приводится описание гомоморфизмов двоичных регистров сдвига с линейной по *входной* (то есть последней) переменной функцией обратной связи в терминах операции $\triangleleft$, отображения π_{f_1,n_2} и бинарного отношения «совпадение состояний с задержкой», которое будет введено позже.

Сразу отметим, что, как и для любых автоматов, любой гомоморфизм регистра $R(h, f)$ (α, β, γ): $R(h, f)\to A$ в автомат $A = (V_1, S, V_1, \delta, \lambda)$ сводится к *внутреннему* гомоморфизму (то есть на входном и выходном алфавитах соответствующие отображения действуют тождественно)

$\beta: R(\gamma h, f)\to A'$,

где $A' = (V_1, S, V_1, \delta', \lambda')$, $\delta'(s, x) = \delta(s, \alpha(x))$, $\lambda'(s, x) = \lambda(s, \alpha(x))$. Поэтому далее мы будем рассматривать только внутренние гомоморфизмы, причем термин «внутренний» будем опускать.

Начнем с описания гомоморфизмов регистра *на регистр*.

В 1967 г. К. Г. Таболовым была обнаружена связь между операцией, схожей с операцией $\triangleleft$ и гомоморфизмами регистров без выхода на регистры без выхода. Эту связь описывает следующая теорема, очевидно вытекающая из введенных определений.

Теорема 1. Пусть $n_i\geq 0$, $f_i\in F^*_{n_i+1}$, i = 1, 2. Тогда $\pi_{f_1,n_2}: R(f_2\triangleleft f_1)\to$ $\to R(f_2)$ – сюръективный гомоморфизм.

В. А. Башевым в 1972 г. было доказано, что других гомоморфизмов регистра на регистр нет. Следующая теорема несколько уточняет этот результат.

Теорема 2. Пусть $n_1, n_2\geq 0$, $f\in F^*_{n_1+n_2+1}$, $f_2\in F_{n_2+1}$, $\beta: R(f)\to R(f_2)$ – гомоморфизм. Тогд $\beta = \pi_{f_1,n_2}$ для некоторой $f_1\in F_{n_1+1}$. При этом, если $f_2\in F^*_{n_2+1}$, то $f_1\in F^*_{n_1+1}$ и $f = f_2\triangleleft f_1$.

Следующая теорема описывает гомоморфизмы регистров на регистры с произвольными выходными функциями.

Теорема 3. Пусть $n \geq 0$, $n_2 \geq 0$, $f \in F^*_{n+1}$, $h \in F_{n+1}$, $f_2 \in F^*_{n_2+1}$, $h_2 \in F_{n_2+1}$, $\beta: V_n \to V_{n_2}$. Тогда следующие утверждения равносильны:

(1) $\beta: R(h, f) \to R(h_2, f_2)$ – гомоморфизм;

(2) $n \geq n_2$ и для некоторой $f_1 \in F^*_{n_1+1}$, где $n_1 = n - n_2$, выполняются равенства:

$$\beta = \pi_{f1, n2},\ f = f_2 \lhd f_1,\ h = h_2 \lhd f_1.$$

Следствие 1. Пусть $n \geq 0$; $f, f' \in F^*_{n+1}$; $h, h' \in F_{n+1}$; $\beta: V_n \to V_n$. Тогда следующие утверждения равносильны:

(1) $\beta : R(h, f) \to R(h', f')$ – изоморфизм;

(2) для некоторого $c \in V_1$ и любых $x_1, \ldots, x_{n+1} \in V_1$ выполняются равенства:

$$\beta(x_1, \ldots, x_n) = (x_1 \oplus c, \ldots, x_n \oplus c);$$

$$f(x_1, \ldots, x_{n+1}) = f'(x_1 \oplus c, \ldots, x_{n+1} \oplus c);$$

$$h(x_1, \ldots, x_{n+1}) = h'(x_1 \oplus c, \ldots, x_{n+1} \oplus c).$$

Из этого следствия получаем, что для порядка группы автоморфизмов (не обязательно внутренних) регистра справедливо равенство

$$|\mathrm{Aut}(R(h, f))| = 2$$

для любых $f \in F^*_{n+1}$, $h \in F_{n+1}$.

Следующее утверждение описывает гомоморфизмы регистров на последовательное соединение регистров.

Следствие 2. Пусть $n, n_2, n'_2 \geq 0$; $f, h \in F^*_{n+1}$; $f_2, h_2 \in F^*_{n_2+1}$; $f'_2, h'_2 \in F^*_{n'_2+1}$; $\beta: V_n \to V_{n'_2} \times V_{n_2}$. Тогда следующие утверждения равносильны:

(1) $\beta: R(h, f) \to R(h'_2, f'_2)\ R(h_2, f_2)$ – гомоморфизм;

(2) $n_1 = n - n_2 \geq 0$, $n'_1 = n - n'_2 \geq 0$ и существуют $f_1 \in F^*_{n_1+1}$, $h'_1 \in F^*_{n'_1+1}$ такие, что выполняются равенства:

а) $\beta(\bar{x}) = \left(\pi_{h'_1, n'_2}(\bar{x}), \pi_{f_1, n_2}(\bar{x})\right)$ для любого $\bar{x} \in V_n$,

б) $f = f_2 \lhd f_1$, $h = h'_2 \lhd h'_1$,

в) $f'_2 \lhd h'_1 = h_2 \lhd f_1$.

Частным случаем этого следствия является следующее утверждение.

Следствие 3. Если $n_i \geq 0$, f_i , $h_i \in F^*_{n_i+1}$, i = 1, 2, $f_2 \triangleleft h_1 = h_1 \triangleleft f_2$, то отображение $\beta: V_{n_1+n_2} \to V_{n_2} \times V_{n_1}$, определяемое равенством

$$\beta(\bar{x}) = \left(\pi_{h_1,n_2}(\bar{x}), \pi_{f_2,n_1}(\bar{x})\right),$$

является гомоморфизмом автоматов

$\beta : R(h_2 \triangleleft h_1, f_1 \triangleleft f_2) \to R(h_2, f_2)\, R(h_1, f_1)$.

Состояние автомата *A* назовем *существенным*, если оно может появляться в любом такте его работы. Поскольку множество всех существенных состояний замкнуто относительно действия функции переходов, то оно является множеством состояний подавтомата, который назовем *существенным подавтоматом* автомата *A*.

Следствие 4. Если $n_i \geq 0$, f_i, $h_i \in F^*_{n_i+1}$, i = 1, 2 и хотя бы одна из функций f_2^*, h_1^* нулевая, то отображение β: $V_{n_1+n_2} \to V_{n_2} \times V_{n_1}$, определяемое равенством

$$\beta(\bar{x}) = \left(\pi_{h_1,n_2}(\bar{x}), \pi_{f_2,n_1}(\bar{x})\right)$$

является гомоморфизмом автоматов

$\beta : R(h_2 \triangleleft h_1, f_1 \triangleleft f_2) \to R(h_2, f_2)\, R(h_1, f_1)$,

образ которого совпадает с существенным подавтоматом автомата $R(h_2, f_2)\, R(h_1, f_1)$, причем в автомате $R(h_2, f_2)\, R(h_1, f_1)$ после такта с номером $\max(n_1, n_2)$ появляются только существенные состояния.

Для того чтобы перейти к описанию гомоморфизмов на произвольный автомат, нам потребуются следующие понятия.

Определение. Состояния $s, s' \in S$ автомата $A = (X, S, Y, \delta, \lambda)$ назовем совпадающими с задержкой k ($k \geq 0$) и этот факт будем обозначать через $s \sigma_k s'$, если любая входная последовательность длины k переводит их в одинаковые состояния. Через $s \sigma s'$ будем обозначать тот факт, что $s \sigma_k s'$ для некоторого k, и такие состояния назовем совпадающими с задержкой. Минимальное k, для которого бинарные отношения σ_k и σ равны ($\sigma_k = \sigma$) назовем задержкой совпадения состояний в автомате A и обозначим через $\Delta(A)$.

Очевидно, что σ_k и σ являются бинарными отношениями эквивалентности на множестве *S* и для любого $k \geq 0$

$$\equiv = \sigma_0, \quad \sigma_0 \subseteq \sigma_k \subseteq \sigma_{k+1} \subseteq \sigma,$$

(здесь и далее $\equiv$ – это совпадение состояний, = – это знак равенства), причем если $\sigma_{k'} = \sigma_{k'+1}$ для некоторого k', то $\sigma_{k'} = \sigma_{k+1}$ для любого $k \geq k'$.

Следовательно, $0 \le \Delta(A) \le |S| - 1$, так что для автомата с конечным числом состояний задержка совпадения состояний всегда конечна.

Определение. Внутренний гомоморфизм автоматов $\beta: A \to A'$ назовем изоморфизмом с задержкой, если отображение β сюръективно и все состояния любого полного прообраза совпадают с задержкой (то есть для любых $s, s' \in S$ из равенства $\beta(s) = \beta(s')$ следует, что $s \sqcup s'$).

Если A – автомат без выхода, то отношения $\sqcup_k$ и $\sqcup$ являются конгруэнциями автомата A и, следовательно, естественные гомоморфизмы $\bar{\beta}_k : A \to A/\sqcup_k$ и $\bar{\beta} : A \to A/\sqcup$ являются изоморфизмами с задержкой. При этом любой изоморфизм с задержкой $\beta : A \to A'$ автоматов без выхода продолжается до гомоморфизма $\bar{\beta}$ (то есть $\beta'\beta = \bar{\beta}$ для некоторого изоморфизма с задержкой β': $A' \to A/\sqcup$).

Следующие два очевидных утверждения описывают случай, когда отношение $\sqcup$ тривиально, то есть совпадает с отношением совпадения $\equiv$.

Утверждение 1. Для любого автомата $A = (X, S, Y, \delta, \lambda)$ следующие свойства равносильны:

1) $\sqcup = \equiv$ (указанные отношения совпадают);

2) $\Delta(A) = 0$;

3) для любых различных $s, s' \in S$ существует $x \in X$ такой, что $\delta(s, x) \ne \delta(s', x)$ (то есть все строки таблицы функции переходов δ различны).

Следствие 5. Если хотя бы одна из частичных функций переходов автомата A является подстановкой, то $\Delta(A) = 0$.

Следующее утверждение устанавливает связь отношения $\sqcup$ с некоторыми характеристиками графа автомата.

Утверждение 2. Пусть $A = (X, S, Y, \delta, \lambda)$ – произвольный автомат, $l \ge 1$, $\bar{x} = (x_1,\ldots,x_l) \in X^l$, $c_{\bar{x}}$ – число циклических точек преобразования $\delta_{\bar{x}} = \delta_{x_l} \ldots \delta_{x_1}$ множества S. Тогда $|S/\sqcup| \ge c_{\bar{x}}$, причем выполняется равенство, если A – автономный. Если $l \ge \Delta(A)$, то $|S/\sqcup| \ge |\delta_{\bar{x}}(S)|$.

В заключение рассмотрения общих свойств отношения $\sqcup$ приведем один достаточно очевидный алгоритм получения факторавтомата $A/\sqcup$, который естественно назвать табличным алгоритмом. Пусть $A = (X, S, \delta)$ – произвольный автомат без выхода, который задан таблицей своей функции переходов δ, то есть матрицей размера

|S|×|X|, строки которой занумерованы множеством S, столбцы – множеством X, а на пересечении s-й строки и x-го столбца стоит δ(s, x). В этой таблице выделим все классы одинаковых строк. В каждом классе выберем одну строку, а остальные удалим. В полученной таблице каждое состояние, являющееся номером удаленной строки, заменим на номер выбранной строки в классе, содержащем эту удаленную строку. Очевидно, что мы получили таблицу автомата, изоморфного автомату $A/\sqsubset_1$. Ясно, что повторяя эту процедуру еще $\Delta(A)-1$ раз (пока не придем к таблице с различными строками) мы получим таблицу автомата, изоморфного автомату $A/\sqsubset$.

Вернемся теперь к регистрам сдвига. Всюду далее через $\sim$ обозначается отношение *эквивалентности* (неотличимости) состояний соответствующего автомата.

Теорема 4. Для любых $n \geq 0$, $f \in F^*_{n+1}$ бинарные отношения $\sqsubset$ и $\sim$ для автомата R'(f) совпадают и $\Delta(R(f)) \leq n$, причем равенство выполняется тогда и только тогда, когда

$$f^* = \text{const}.$$

Следствие. Если $n \geq 0$, $f \in F^*_{n+1}$, $\bar{s}$, $\bar{s}' \in V_n$, то для автомата R(f) справедливы следующие утверждения:

1) если $f^*(\bar{s}) \neq f^*(\bar{s}')$, то не выполняется $\bar{s} \sqsubset \bar{s}'$;

2) если $f^* \neq \text{const}$ и последние координаты векторов $\bar{s}$ и $\bar{s}'$ различны, то не выполняется $\bar{s} \sqsubset \bar{s}'$;

3) $|V_n/\sqsubset| = 1$ тогда и только тогда, когда $f^* = \text{const}$;

4) $|V_n/\sqsubset_1| = 2^{n-1} + ||f_1||$, где $f^*(x_1, \ldots, x_n) = x_1 \cdot f_1(x_2, \ldots, x_n) \oplus f_0(x_2, \ldots, x_n)$, $||f_1|| = |f_1^{-1}(1)|$.

Следующее утверждение описывает все изоморфизмы с задержкой регистра на регистр.

Теорема 5. Пусть $n, n_2 \geq 0$, $f \in F^*_{n+1}$, $f_2 \in F^*_{n_2+1}$, $\beta: V_n \to V_{n_2}$. Тогда следующие утверждения равносильны:

1) $\beta: R(f) \to R(f_2)$ – изоморфизм с задержкой;

2) $n_1 = n - n_2 \geq 0$, $\beta = \pi_{f_1, n_2}$, $f = f_2 \lhd f_1$, где $f_1 = c \oplus x_{n_1+1}$, $c \in V_1$;

при этом, если функция f существенно зависит от 1-й переменной, то утверждение (1) равносильно следующему:

3) $\beta: R(f) \to R(f_2)$ – изоморфизм.

Основным результатом настоящей работы является следующая теорема о разложении произвольного гомоморфизма регистра в композицию гомоморфизма на регистр и изоморфизма с задержкой, причем разложении, по существу, однозначном.

Теорема 6. Пусть $n \geq 0$, $f \in F^*_{n+1}$, $h \in F_{n+1}$, $A = (V_1, S, V_1, \delta, \lambda)$, $\overline{A} = (V_1, S, \delta)$, $\beta: R(f) \to \overline{A}$ – сюръективный гомоморфизм. Тогда существуют $n_1 \in \{0, \ldots, n\}$, $f_1 \in F^*_{n_1+1}$, $f_2 \in F^*_{n_2+1}$, где $n_2 = n - n_1$, и изоморфизм с задержкой $\beta_2: R(f_2) \to \overline{A}$ такие, что $f = f_2 \triangleleft f_1$, $\beta_1 = \pi_{f_1, n_2}: R(f) \to R(f_2)$ – сюръективный гомоморфизм, и выполняются следующие свойства:

1) $\beta = \beta_2 \beta_1$;

2) если $\beta = \beta_2' \beta_1'$, где $\beta_1': R(f) \to R(f_2')$ – гомоморфизм, $\beta_2': R(f_2') \to A$ – изоморфизм с задержкой, $f_2' \in F^*_{n_2'+1}$, $n_2' \in \{0, \ldots, n\}$, то $m = n_2 - n_2' \geq 0$, и для некоторого $c \in V_1$ выполняются равенства:

$$\beta_1' = \pi_{f_1', n_2'} = \pi_{(c \oplus x_{m+1}), n_2'} \beta_1, \; f_1' = (c \oplus x_{m+1}) \triangleleft f_1,$$

$$\beta_2 = \beta_2' \pi_{(c \oplus x_{m+1}), n_2'}, \; f_2 = f_2' \triangleleft (c \oplus x_{m+1});$$

3) если $\beta: R(h, f) \to A$ – гомоморфизм, то существует $h_2 \in F_{n_2+1}$ такая, что $h = h_2 \triangleleft f_1$ и $\beta_1: R(h, f) \to R(h_2, f_2)$, $\beta_2: R(h_2, f_2) \to A$ – гомоморфизмы.

При этом если f существенно зависит от 1-й переменной, то в пункте (2) $n_2 = n_2'$ и

$$f_1' = f_1 \oplus c,$$
$$f_2' = f_2(x_1 \oplus c, \ldots, x_{n_2+1} \oplus c),$$
$$\beta_2' = \beta_2(x_1 \oplus c, \ldots, x_{n_2} \oplus c).$$

Теорема 6 сводит описание гомоморфизмов регистров к описанию разложений функций обратной связи по операции $\triangleleft$ и описанию соответствующих изоморфизмов с задержкой. Одним из следствий этой теоремы является следующее: *при $f \in F^*_{n+1}$ всякий сюръективный гомоморфизм регистра $R(f)$ может быть продолжен до гомоморфизма на фактор-автомат $R(f_2)/\simeq$, где $f = f_2 \triangleleft f_1$, а конгруэнция $\simeq$ описывается следующей леммой из доказательства теоремы* 11.

Лемма. При условии теоремы 11 для любых $0 \leq k \leq n$, $\bar{s}, \bar{s}' \in V_n$, $\bar{s} = (s_1, \ldots, s_n)$, $\bar{s}' = (s'_1, \ldots, s'_n)$ следующие утверждения равносильны:

1) $\bar{s} \; \square_k \; \bar{s}'$;

2) $s_j = s'_j$ для всех $j = k + 1, \ldots, n$;

3) $(s_i, \ldots, s_n, s_{n+1}, \ldots, s_{n+i}) = f(s'_i, \ldots, s'_n, s_{n+1}, \ldots, s_{n+i})$ для любых $i = 1, \ldots, k$ и $s_{n+1}, \ldots, s_{n+i} \in V_1$.

Напомним, что автомат называют *подстановочным (перестановочным)*, если все его частичные функции переходов являются

подстановками множества состояний. Очевидно, что для двоичного регистра сдвига ненулевой длины перестановочность равносильна *линейности функции обратной связи по* 1-*й переменной*, а в случае линейности функции обратной связи по последней переменной равносильна еще и отсутствию различных совпадающих с задержкой состояний (4 утверждения следствия из теоремы 4). Следовательно, неподстановочный регистр сдвига без выхода длины 2 и более с линейной по последней переменной функцией обратной связи всегда имеет нетривиальные изоморфизмы с задержкой.

Следствие 1. Любой гомоморфный образ подстановочного двоичного регистра сдвига с линейной по последней переменной функцией обратной связи изоморфен некоторому подстановочному двоичному регистру сдвига с линейной по последней переменной функцией обратной связи.

Заметим, что данное следствие для случая регистров без выхода было доказано А. Я. Прососовым в 1977 г.

Следствие 2. Любой гомоморфный образ двоичного регистра сдвига с линейной по последней переменной функцией обратной связи и линейной по первой и последней переменным выходной функцией изоморфен некоторому двоичному регистру сдвига с линейной по последней переменной функцией обратной связи и линейной по первой и последней переменным выходной функцией.

Рассмотрим теперь *множество всех двоичных функций* $\mathrm{F} = \bigcup_{n=0}^{\infty} F_{n+1}$. Относительно операции $\triangleleft$ оно является моноидом с единичным элементом $x_1 \in \mathrm{F}_1$. Следовательно, на множестве F возникает соответствующее транзитивное и рефлексивное бинарное отношение делимости (справа) |, которое определяется следующим образом: $f_1 \mid f$, *тогда и только тогда, когда* $f = f_2 \triangleleft f_1$ *для некоторой* $f_2 \in F$ *(которая называется частным от деления* f *на* f_1, *а* f_1 – *делителем* f*)*. Это отношение не является симметричным, поскольку $\mathrm{f}_1 \mid \mathrm{f}$ и $\mathrm{f} \mid \mathrm{f}_1$ только в случае, когда f и f_1 являются функциями от одинакового количества переменных и $\mathrm{f} \oplus \mathrm{f}_1 = \mathrm{const}$.

Кроме того, частное не всегда определено однозначно. Точнее, справедливо следующее свойство: частное от деления на функцию f_1 всегда определено однозначно тогда и только тогда, когда f_1 является *функцией без запретов* (то есть отображение π_{f_1, n_2} является сюръективным для любого $n_2 \geq 0$, что равносильно возможности появления на выходе регистра $R_0(f_1)$ любой двоичной последовательности

[31]). В частности, все функции из подмоноида $F^* = \bigcup_{n=0}^{\infty} F^*_{n+1}$ моноида F являются функциями без запретов.

Введенное отношение делимости функций является продолжением отношения делимости многочленов в следующем смысле. Обозначим через L^* подмоноид моноида F^*, состоящий из всех линейных функций из F^*, а через $GF(2)[x]^*$ – моноид всех ненулевых многочленов над полем GF(2). Тогда отображение $GF(2)[x]^* \to L^*$, где

$$c_0 \oplus c_1 x \oplus \ldots \oplus c_n x^n \mapsto c_0 x_1 \oplus c_1 x_2 \oplus \ldots \oplus c_n x_{n+1},$$

является изоморфизмом и, следовательно, сохраняет отношение делимости.

Наибольшим общим делителем функций $h, f \in F$ назовем любой их общий делитель от наибольшего количества переменных. Множество всех наибольших общих делителей функций h и f обозначим через (h, f). Оно не пусто, поскольку функции x_1, $1 \oplus x_1 \in F_1$ являются делителями любой функции из F. Функции $h, f \in F$ назовем *взаимно простыми*, если $(h, f) = \{x_1, 1 \oplus x_1\}$.

Теорема 7. Пусть $n \geq 0$, $f \in F^*_{n+1}$, $h \in F_{n+1}$. Тогда $(h, f) \in \{f_1, 1 \oplus f_1\}$, где $f_1 \in F^*_{n_1+1}$, $n_1 \leq n$, причем для любой функции $f_1' \in F$ следующие утверждения равносильны:

1) $f_1' \mid h$, $f_1' \mid f$;
2) $f_1' \mid f_1$.

При этом существует коммутативная диаграмма гомоморфизмов автоматов рис. 10.

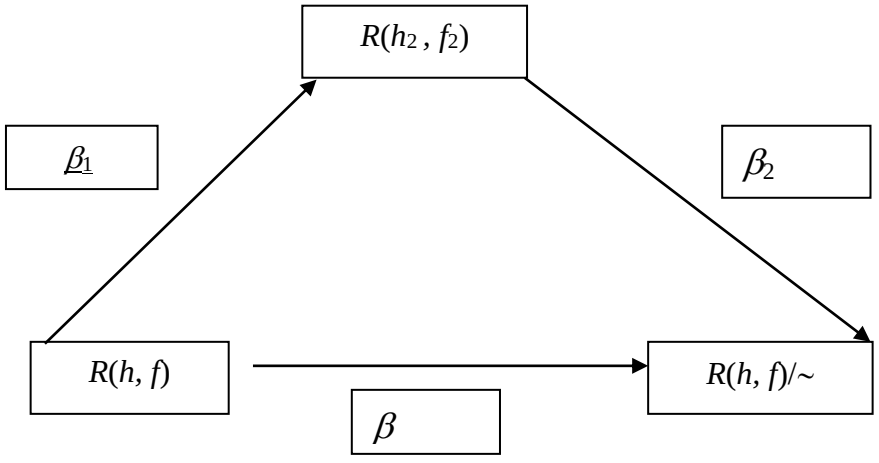

Рис. 10

Здесь β – естественный гомоморфизм автомата $R(h, f)$ на свою приведенную форму $R(h, f)/\sim$;

$\beta_1 = \pi_{f_1, n_2}$;

$n_2 = n - n_1$;

$f_2 \in F^*_{n_2+1}$;

$h_2 \in F_{n_2+1}$;

$f = f_2 \lhd f_1$;

$h = h_2 \lhd f_1$;

β_2 – изоморфизм с задержкой.

Следствие 1. Пусть $n \geq 0$, $f \in F^*_{n+1}$, $h \in F_{n+1}$ и выполнено хотя бы одно из условий:

а) f линейна по 1-й переменной;

б) h линейна по 1-й и (n+1)-й переменным.

Тогда следующие утверждения равносильны:

1) автомат $R(h, f)$ не имеет различных эквивалентных состояний (минимален);

2) функции h и f взаимно просты.

В качестве примеров применения теоремы 7 приведем еще два следствия, описывающие некоторые неэквивалентные состояния регистров.

Следствие 2. *Пусть* $n \geq 1$, $f, h \in F^*_{n+1}$, $f \oplus h \neq \text{const}$. Тогда $(\alpha_1, \ldots, \alpha_{n-1}, 0) \nsim (\alpha_1, \ldots, \alpha_{n-1}, 1)$ в $R(h, f)$ для любых $\alpha_1, \ldots, \alpha_{n-1} \in V_1$.

Следствие 3. Пусть $n \geq 1$, $f, h \in F^*_{n+1}$, $f \oplus h \neq \text{const}$ и выполнено одно из следующих условий:

а) хотя бы одна из функций f, h принимает разные значения на $(0, \ldots, 0), (1, \ldots, 1) \in V_{n+1}$;

б) $f_1(0, \ldots, 0) \neq f_1(1, \ldots, 1)$, где $f_1 \in (h, f)$.

Тогда $(0, \ldots, 0) \nsim (1, \ldots, 1)$ в $R(h, f)$.

В заключение укажем на возможные обобщения изложенных результатов на случай регистра $R(h, f)$, где $f: X^{n+1} \to X$, $h: X^{n+1} \to Y$, X, Y – произвольные конечные множества. Так, теоремы 1, 2, 3 без особых затруднений могут быть обобщены следующим образом.

Функцию $\varphi : X^{m+1} \to X$ назовем *биективной по последней* (то есть (m+1)-й) *переменной*, если при любой фиксации всех остальных переменных получаемое отображение $X \to X$ является биекцией. В этом случае через φ^{-1} обозначим функцию, *обратную к функции к функции* φ *по последней переменной*, то есть

$\varphi^{-1} : X^{m+1} \to X$ и $\varphi^{-1}(x_1, \ldots, x_m, \varphi(x_1, \ldots, x_{m+1})) = x_{m+1}$

для любых $x_1, \ldots, x_{m+1} \in X$.

Теорема 8. Пусть $n, n_2 \geq 0$, $f: X^{n+1} \to X$, $f_2: X^{n_2+1} \to X$ – биективные по последней переменной функции, $h: X^{n+1} \to X$, $h_2: X^{n_2+1} \to X$, $\beta : X^n \to X^{n_2}$. Тогда следующие утверждения равносильны:

1) $\beta : R(h, f^{-1}) \to R(h_2, f_2^{-1})$ – гомоморфизм;

2) $n \geq n_2$, $\beta = \pi_{f_1, n_2}$, $f = f_2 \triangleleft f_1$, $h = h_2 \triangleleft f_1$ для некоторой биективной по последней переменной функции $f_1: X^{n_1+1} \to X$, где $n_1 = n - n_2$.

Глава 7. ВЕРХНЯЯ ОЦЕНКА СТЕПЕНИ РАЗЛИЧИМОСТИ СВЯЗНЫХ ПЕРЕСТАНОВОЧНЫХ АВТОМАТОВ С ЗАДАННЫМ ДИАМЕТРОМ

В разделе описан метод получения верхней оценки степени различимости связных перестановочных автоматов с заданным диаметром [2].

7.1. Формулировка основных результатов

Известна (например, [27]) следующая достижимая оценка степени различимости R конечного автомата с числом состояний |S|:

$$R \le |S| - 1.$$

Кроме того, в [22] показано, что почти все автоматы имеют степень различимости, асимптотически равную $\log_{|X|}\log_{|Y|}|S|$, где |X|, |Y| – мощности, соответственно, входного и выходного алфавитов автомата.

Положим $N_0 = \{0, 1, \ldots\}$.

Показано [2], что для связного перестановочного автомата с диаметром D

$$R \le (l_0 + 1)(D+1) + \left[\frac{|S|}{2^{l_0+1}}\right] - 1,$$

где $[\nu]$ – целая часть числа ν, а l_0 – максимальное $l \in N_0$, если оно существует, при котором $\left[\frac{|S|}{2^l}\right] - \left[\frac{|S|}{2^{l+1}}\right] > D+1$, в противном случае $l_0 = -1$. Данная оценка достижима для следующих параметров перестановочного связного автомата Мура:

1) $D = 1,\ |S| = 3\cdot 2^m,\ m \in N_0$;
2) $D = 1,\ |S| = 5\cdot 2^m,\ m \in N_0$;
3) $D = 2,\ |S| = 5\cdot 2^m,\ m \in N_0$.

7.2. Доказательство основной оценки

Обозначим через $A(|S|, D)$ класс приведенных связных перестановочных автоматов Мура с числом состояний |S|, выходным алфавитом Y, |Y| = 2 и диаметром D. Доказано, что тогда и только тогда R<|S|–1 для любого автомата из $A(|S|, D)$, когда $D < n+1$, если $|S| = 2(n+1)+1$, и $D < 2(n+1)$, если $|S| = 4(n+1)$, $n \in N_0$. Если $|S| = 4(n+1)+2$ и $R = 4(n+1)+1$, то $D \ge 2(n+1)+2,\ n \in N_0$.

Пусть A = (X, S, Y, h, f) – конечный автомат с частичными функциями перехода $(h_x)_{x\in X}$ и частичными функциями выхода $(f_x)_{x\in X}$. В даль-

нейшем предполагается, что рассматриваемый автомат A является связным с числом состояний |S|>1. Кроме того, предполагается, что hx осуществляет взаимно-однозначное отображение S в себя при любом x∈X, то есть рассматриваемый автомат перестановочный (раздел 5.1 и [34]). Для собственного подмножества M множества S обозначим через D_M минимальное d такое, что для любого $s \in S \backslash M$ существует $s' \in M$, из которого s достижимо входным словом длины, не превосходящей d. Положим $D_k = maxD_M$, где максимум берется по всем подмножествам M мощности k множества S. Очевидно, $D_k \geq D_{k+1}$ при $1 \leq k \leq |S| - 2$ и D = D1 – диаметр графа переходов автомата A.

Представим |S| в виде $|S| = K_l 2^l + h_l$, где $K_l = \left[\frac{|S|}{2^l}\right]$. Обозначим через l^* максимальное число l, если оно существует, при котором $K_j - K_{j+1} > D_{2^{j+1}} + 1$, j∈[0, l]. В противном случае полагаем $l^* = -1$. Пусть R – степень различимости автомата A. Обозначим через l_0 максимальное $l \in N_0$, если оно существует, при котором $K_l - K_{l+1} > D + 1$. В противном случае полагаем $l_0 = -1$.

Теорема 1. Для приведенного связного перестановочного автомата A

$$R \leq (l_0 + 1)(D + 1) + K_{l_0+1} - 1.$$

Доказательство проведем с помощью следующей вспомогательной леммы.

Лемма 1. Для приведенного связного перестановочного автомата A

$$R \leq \sum_{j=1}^{l^*+1} (D_{2^j} + 1) + K_{l^*+1} - 1.$$

Доказательство. При $l^* = -1$ доказываемое неравенство следует из известной оценки $R \leq |S| - 1$. Пусть $l^* \neq -1$ и предположим, что

$$R > \sum_{j=1}^{l^*+1} (D_{2^j} + 1) + K_{l^*+1} - 1.$$

Обозначим через $\alpha_1^m, \alpha_2^m, ..., \alpha_{P_m}^m$ классы m – неотличимых состояний автомата A и через P_m – число этих классов. Очевидно, существует $i \in [1, P_{R-1}]$, для которого $|\alpha_i^{R-1}| \geq 2^2$. Поэтому, в силу связности и перестановочности автомата A, $|\alpha_j^{R-1-D_2}| \geq 2$ при любом $j \in [1, P_{R-1-D_2}]$. Следовательно, найдется $i \in [1, P_{R-2-D_2}]$ при котором $|\alpha_i^{R-2-D_2}| \geq 2$. Если $l^* > 0$, в силу связности и перестановочности A, будем иметь $|\alpha_j^{R-2-D_2-D_4}| \geq 2^2$ при любом $j \in [1, P_{R-1-D_2-D_4}]$. Продолжая аналогично, получим для $t \leq l^* + 1$

$$|\alpha_j^{R-\sum_{j=1}^{t}(D_{2^j}+1)}| \geq 2^t$$

при любом $i \in \left[1, P_{R-\sum_{j=1}^{t}(D_{2^j}+1)}\right]$. Непосредственно усматривается, что $R-\sum_{j=1}^{t}(D_{2^j}+1) \leq K_{l^*+1}$ и поэтому $P_{R-\sum_{j=1}^{t}(D_{2^j}+1)-K_{l^*+1}+1} = 1$, что противоречит приведенности автомата A.

Следовательно, $R \leq \sum_{j=1}^{l^*+1}(D_{2^j}+1)+K_{l^*+1}-1$.

При $l_0 = -1$ доказываемое в теореме неравенство следует из известной оценки R≤|S|–1. Пусть $l_0 \neq -1$. Так как $D \geq D_k$, то $l^* \geq l_0$. Согласно лемме 1 имеем

$$R \leq \sum_{j=1}^{l^*+1}(D_{2^j}+1)+K_{l^*+1}-1 = \sum_{j=1}^{l_0+1}(D_{2^j}+1)+\sum_{j=l_0+2}^{l^*+1}(D_{2^j}+1)+K_{l^*+1}-1 \leq$$

$$\leq (l_0+1)(D+1)+\sum_{j=l_0+2}^{l^*+1}(K_{j-1}+K_j)+K_{l^*+1}-1 = (l_0+1)(D+1)+K_{l_0+1}-1.$$

Замечание 1. Степени различимости неотличимых автоматов равны. Поэтому утверждение теоремы 1 позволяет оценивать степени различимости и неприведенных связных перестановочных автоматов. Из приведенного доказательства леммы 1 легко получить более простую, но менее точную оценку: R≤(D+1)[$\log_2$|S|]. Действительно, если R–k(D+1)≥1, то каждый класс (R–k(D+1))-неотличимых состояний приведенного связного перестановочного автомата содержит, по крайней мере, 2^k состояний. Пусть k(0) – максимальное натуральное число k, при котором R–k(D+1)≥1.

Тогда:

1) число классов (R–k(0)(D+1))-неотличимых состояний не меньше двух и каждый из них содержит по крайней мере $2^{k(0)}$ состояний;

2) R–(k(0)+1)(D+1)≤0.

Поэтому $2^{k(0)+1} \leq |S|$, $k(0)+1 \leq \log_2|S|$, $k(0)+1 \leq [\log_2|S|]$ и R≤k(0)(D+1).

Следовательно, в рассматриваемом случае:

$$R \leq [\log_2|S|](D+1).$$

В случае, когда R–(D+1) ≤ 0, указанная оценка также выполняется.

7.3. О роли диаметра перестановочного связного приведенного автомата в его оценки степени различимости

Ниже приводятся условия, при которых оценка $(l_0+1)(D+1)+K_{l_0+1}-1$ степени различимости перестановочных связных приведенных автоматов лучше известной оценки R≤|S|–1.

Теорема 2. Неравенство

$$(l_0+1)(D+1)+K_{l_0+1}-1\le|\mathrm{S}|-1$$

имеет место тогда и только тогда, когда $D<\frac{1}{2}(|S|-2)$ при четном |S| и $D<\frac{1}{2}(|S|-1)$ при нечетном |S|.

Доказательство. Если $(l_0+1)(D+1)+K_{l_0+1}-1<|\mathrm{S}|-1$, то $l_0\ne-1$. Имеем $\frac{|S|-K_{l_0+1}}{l_0+1}>D$. При $l_0=0$ это неравенство принимает вид $D<\frac{1}{2}(|S|+\varepsilon)-1$, где $\varepsilon=0$ при четном |S| и $\varepsilon=1$ при нечетном |S|.

Рассмотрим теперь случай $l_0>0$. Имеем

$$\frac{1}{2}|S|-1\ge\frac{|S|-K_{l_0+1}}{l_0+1}-1>D.$$

Таким образом, необходимость утверждения теоремы 2 доказана. Предположим теперь, что имеет место неравенство $\frac{1}{2}(|S|+\varepsilon)-1>D$. Тогда $l_0\ge0$ и $K_{l_0}-K_{l_0+1}>D+1$. Следовательно,

$$\frac{1}{2}(K_{l_0}+\varepsilon')>D+1,$$

где $\varepsilon'=0$ при четном K_{l_0} и $\varepsilon'=1$ при нечетном K_{l_0}. Имеем

$$(l_0+1)(D+1)+K_{l_0+1}-1<(l_0+1)\frac{K_{l_0}+\varepsilon'}{2}+K_{l_0+1}-1<(l_0+1)\frac{K_{l_0}+\varepsilon'}{2}+\frac{K_{l_0}-\varepsilon'}{2}-1=$$

$$=l_0\frac{K_{l_0}+\varepsilon'}{2}+K_{l_0}-1.$$

При $l_0=0$ правая часть неравенства равна |S|–1.

Пусть $l_0>0$. Из определения величины l_0 получаем, что $K_{l_0+1}\le2D+2$ при любом l_0. Тогда $K_{l_0}-K_{l_0+1}>D+1\ge2$, и, следовательно, $K_{l_0+1}\ge1$. Поэтому $K_{l_0}>2+K_{l_0+1}\ge3$ и $K_{l_0}\ge4$. Используя последнее неравенство и равенство

$$l_0\frac{1}{2}(K_{l0}+\varepsilon')+K_{l_0}-1=\frac{1}{2}(l_0+2)K_{l_0}+\frac{l_0}{2}\varepsilon'-1,$$

индукцией по l_0 легко доказывается, что

$$\frac{1}{2}(l_0+2)K_{l_0}+\frac{l_0}{2}\varepsilon'-1<2^{l_0}K_{l_0}-1\le|S|-1,$$

что и требовалось доказать.

Лемма 2. Если наибольший общий делитель мощностей классов 1-неотличимых состояний перестановочного связного автомата A равен единице, то автомат A является приведенным.

Справедливость леммы 2 следует из известных утверждений:

– мощности классов неотличимых состояний связного перестановочного автомата равны,

– каждый класс (k-1)-неотличимых состояний является объединением некоторых классов k-неотличимых состояний [16; 27].

Теорема 3. Для любого автомата из класса $A(2n+1,D)$ тогда и только тогда R<2n, когда $D < n$.

Доказательство. Достаточность приведенных условий доказана теоремой 2. Докажем необходимость этих условий. Для этого покажем, что при любом $D \geq n$, $D \leq 2n$ существует автомат в классе $A(2n+1,D)$ со степенью различимости, равной $2n$. Построим семейство автоматов (A_n), $n \in \{1, 2, \ldots\}$, $A_n \in A(2n+1,n)$. В качестве автомата A_1 возьмем автомат Мура $\mathbf{A_1} = (\mathrm{X_1}, \mathrm{S_1}, \mathrm{Y_1}, \mathrm{h^{(1)}}, \lambda^{(1)})$ с параметрами $X_1 = \{1, 2, 3\}$, $S_1 = \{1, 2, 3\}$, $Y_1 = \{0, 1\}$, $\lambda^{(1)} = f_x$ для любого $x \in X$.

$$h_1^{(1)}: \begin{matrix} 1 \leftrightarrow 2 \\ 3 \leftrightarrow 3 \end{matrix},\ h_2^{(1)}: \begin{matrix} 1 \leftrightarrow 3 \\ 2 \leftrightarrow 2 \end{matrix},\ h_3^{(1)}: \begin{matrix} 1 \leftrightarrow 1 \\ 2 \leftrightarrow 3 \end{matrix},\ \lambda^{(1)}(2) = \lambda^{(1)}(3) = 1,\ \lambda^{(1)}(1) = 0.$$

Здесь и далее двусторонняя стрелка между двумя состояниями s_1, s_2 с пометкой x, то есть $\mathbf{s_1} \overset{\mathbf{x}}{\longleftrightarrow} \mathbf{s_2}$ или h_x: $s_1 \leftrightarrow s_2$ означает, что частичная функция переходов h_x переводит s_1 в s_2, s_2 в s_1.

Автоматы $\mathbf{A_n}$, $\mathbf{n \geq 2}$, строим индуктивно. Именно если построен автомат $\mathbf{A_{n_0-1}}$, то для автомата $\mathbf{A_{n_0}} = (\mathrm{X_{n_0}}, \mathrm{S_{n_0}}\mathrm{Y_{n_0}}, \mathrm{h^{(n_0)}}, \lambda^{(n_0)})$ полагаем

$$X_{n_0} = \{1, 2, \ldots, 3 \cdot n_0\},\ S_{n_0} = \{1, 2, \ldots, 2 \cdot n_0 + 1\},\ Y_{n_0} = \{0, 1\},$$

$h_x^{(n_0)} s = h_x^{(n_0-1)} s$, если $s \in \{1, \ldots, 2(n_0 - 1) + 1\}$, $h_x^{(n_0)} s = s$, если $s \in \{2n_0, 2n_0 + 1\}$, для всех $x \in \{1, 2, \ldots, 3(n_0 - 1)\}$ и

$$h_{3(n_0-1)+1}^{(n_0)}: \begin{matrix} 2n_0 - 2 \leftrightarrow 2n_0 \\ 2n_0 + 1 \leftrightarrow 2n_0 - 1 \\ j \leftrightarrow j,\ j \neq 2n_0 - 2,\ 2n_0 - 1,\ 2n_0,\ 2n_0 + 1 \end{matrix},$$

$$h_{3(n_0-1)+2}^{(n_0)}: \begin{matrix} 2n_0 \leftrightarrow 2n_0 - 1 \\ 2n_0 + 1 \leftrightarrow 2n_0 - 2 \\ j \leftrightarrow j,\ j \neq 2n_0 - 2,\ 2n_0 - 1,\ 2n_0,\ 2n_0 + 1 \end{matrix},$$

$$h_{3(n_0-1)+3}^{(n_0)}: \begin{matrix} 2n_0 \leftrightarrow 2n_0 + 1 \\ j \leftrightarrow j,\ j \neq 2n_0,\ 2n_0 + 1 \end{matrix},$$

$$\lambda^{(n_0)}(2n_0)=\lambda^{(n_0)}(2n_0+1)=1;\ \lambda^{(n_0)}(1)=\lambda^{(n_0)}(2)=...=\lambda^{(n_0)}(2n_0-1)=0.$$

Ясно, что построенный автомат A_{n_0} является связным, перестановочным автоматом с диаметром n_0. Согласно лемме 2, автомат A_{n_0} не имеет различных неотличимых состояний. Если $x_1, x_2, ..., x_{k_0}$ – входное слово автомата A_{n_0}, для которого выходные последовательности с состояний $2n_0, 2n_0+1$ различны и k_0 минимальное, то, как нетрудно видеть,

$x_1 \in \{3n_0-2, 3n_0-1\}$, $x_2 \in \{3n_0-5, 3n_0-4\}$, …, $x_{n_0-2} \in \{7,8\}$, $x_{n_0-1} \in \{4,5\}$.

При этом

$h^{(n_0)}_{x_{n_0-1}} \cdot h^{(n_0}_{x_{n_0-2}} \cdot \ldots \cdot h^{(n_0)}_{x_1} 2n_0 \in \{2,3\}$;

$h^{(n_0)}_{x_{n_0-1}} \cdot h^{(n_0}_{x_{n_0-2}} \cdot \ldots \cdot h^{(n_0)}_{x_1} (2n_0+1) \in \{2,3\}$.

Теперь ясно, что, во-первых, $x_{n_0} \in \{1,2\}$, $x_{n_0+1} \in \{4,5\}, x_{n_0+2} \in \{7,8\}$, $x_{n_0+3} \in \{10,11\}$ … , $x_{2n_0-1} \in \{3n_0-2, 3n_0-1\}$, во-вторых, $k_0 = 2n_0$, а символ x_{2n_0} может быть любым из X_{n_0}. Таким образом, состояния $2n_0, 2n_0+1$ автомата A_{n_0} являются $(2n_0-1)$-неотличимыми состояниями и $R_{n_0} = 2n_0$.

Для любого фиксированного числа n построим семейство автоматов $\left(A_{2n+1,n+j}\right)_{j\in[0,n]}$, $A_{2n+1,n+j} \in A(2n+1, n+j)$.

Построение выполним следующим способом. В качестве автомата $A_{2n+1,2n}$ возьмем автомат с параметрами $X_{2n+1,2n} = \{1,2\}$, если n=1 и $X_{2n+1,2n} = \{1,2,4,7,10,...,3n_0-2\}$ при n>1; $S_{2n+1,2n} = \{1,2,...,2n+1\}$, $Y_{2n+1,2n} = \{0,1\}$ и частичными функциями переходов $h_x^{2n+1,2n}$ и выходов $\lambda^{2n+1,2n}$, равными соответствующим функциям автомата A_n

$$h_x^{2n+1,2n} = h_x^{(n)},\ \lambda^{2n+1,2n} = \lambda^{(n)}.$$

При n>1 автоматы $(A_{2n+1,2n-1})_{i\in[0,n]}$ строятся аналогично. Их входные алфавиты даются в приводимой ниже табл. 14.

Частичные функции переходов $h_x^{2n+1,2n-i}$ и функции выходов $\lambda^{2n+1,2n-i}$ этих автоматов равны соответствующим функциям автомата A_n:

$$h_x^{2n+1,2n-i} = h_x^n,$$
$$\lambda^{2n+1,2n-i} = \lambda^{(n)}.$$

Таблица 14

Входные алфавиты автоматов

$A_{2n+1,2n-i}$	$X_{2n+1,2n-i}$
$A_{2n+1,2n-1}$	$X_{2n+1,2n-1} = X_{2n+1,2n} \cup \{3\}$
$A_{2n+1,2n-2}$	$X_{2n+1,2n-2} = X_{2n+1,2n} \cup \{3,5\}$
$A_{2n+1,2n-3}$	$X_{2n+1,2n-3} = X_{2n+1,2n} \cup \{3,5,6\}$
$A_{2n+1,2n-4}$	$X_{2n+1,2n-4} = X_{2n+1,2n} \cup \{3,5,6,8\}$
…	…
$A_{2n+1,2n-2i}$	$X_{2n+1,2n-2i} = X_{2n+1,2n} \cup \{3,5,6,\ldots,(i-1)\cdot 3+5\}$
$A_{2n+1,2n-2i-1}$	$X_{2n+1,2n-2i-1} = X_{2n+1,2n} \cup \{3,5,6,\ldots,(i-1)\cdot 3+6\}$
…	…
$A_{2n+1,2n-n}$	$X_{2n+1,2n-n} = X_{2n+1,2n} \cup \{3,5,6,\ldots,\left(\left[\frac{n}{2}\right]-1\right)\cdot 3+5+\varepsilon\cdot 1\ ,\varepsilon = \begin{cases}1, & n-\text{нечетное}\\ 0, & n-\text{четное}\end{cases}$

Автомат $A_{2n+1,2n-i}, i \in [0,n]$, является, очевидно, связным перестановочным автоматом с диаметром $D = 2n-i$. Согласно лемме 1, автоматы $A_{2n+1,2n-i}, i \in [0,n]$ приведенные. Для доказательства теоремы 3 остается доказать, что степень различимости автомата $A_{2n+1,2n-i}, i \in [0,n]$ равна 2n. Для этого достаточно показать, что состояния $2n, 2n+1$ автомата $A_{2n+1,2n-i}$ $(2n-1)$-неотличимы. Согласно законам построения автомата $A_{2n+1,2n-i}$

$$X_{2n+1,2n-i} \subseteq X_n$$

и любая выходная последовательность автомата $A_{2n+1,2n-i}$, отвечающая его входному слову J и начальному состоянию $s \in S_{2n+1,2n-i}$, совпадает с выходной последовательностью автомата A_n, отвечающей входному слову J и начальному состоянию $s \in S_{2n+1,2n-i}$, автомата A_n. Следовательно, k-неотличимые состояния автомата A_n будут и k-неотличимыми состояниями автомата $A_{2n+1,2n-i}$. В частности, состояния 2n, 2n+1 автомата $A_{2n+1,2n-i}$ (2n-1)-неотличимы.

При доказательстве приводимых ниже теорем будет использовано утверждение, доказанное С. В. Гинсбургом в [17], которое мы формулируем в виде отдельной леммы.

Лемма 3. Пусть A – перестановочный приведенный автомат со степенью различимости |S|–1. Тогда каждое разбиение $\wp_k$ на классы k-неотличимых состояний имеет один из следующих видов:

а) $\wp_k$ состоит из двух классов B_1 и B_2 мощности t и |S|-t, соответственно, причем как t, так и |S|-t взаимно просто с |S|;

б) $\wp_{|S|-1}$ состоит из |S| классов, каждый из которых состоит только из одного состояния;

в) $\wp_k$ состоит из k + 1 классов $N_1^k, N_2^k, ..., N_{\alpha(k)}^k, R_1^k, R_2^k, ..., R_{\beta(k)}^k$, где каждый класс N_i^k имеет мощность ν_k, а каждый класс R_i^k имеет мощность z_k, причем $z_k < v_k$. Тогда $\wp_{k+1}$ получается из $\wp_k$ разбиением одного из N_i^k на два класса C_k и $C`_k$ из $\wp_{k+1}$ мощности z_k и ν_k-z_k, соответственно;

г) $\wp_k$ состоит из k+1 классов $N_1^k, N_2^k, ..., N_{\alpha(k)}^k, Q_1^k, Q_2^k, ..., Q_{\beta(k)}^k R_1^k, R_2^k, ..., R_{\gamma(k)}^k$, где каждый класс N_i^k имеет мощность ν_k, каждый класс Q_i^k имеет мощность $v_k - z_k$ и каждый класс R_i^k имеет мощность x_k, причем $z_k < \nu_k$. Тогда $\wp_{k+1}$ получается из $\wp_k$ разбиением одного из N_i^k на два класса C_k и C'_k из $\wp_{k+1}$ мощности z_k и $\nu_k - z_k$ соответственно.

Теорема 4. Для любого автомата из класса $A(4n, D)$ тогда и только тогда R<4n–1, когда D<2n.

Доказательство. Если $D < 2n-1$, то $R < 4n-1$ согласно теореме 2.

Пусть $R = 4n-1$ для некоторого $A \in A(4n, 2n-1)$. Аналогично доказательству теоремы 1 легко показывается, что мощности классов $(R-2n)$-неотличимых состояний автомата A удовлетворяют неравенству $\left|\alpha_i^{R-2n}\right| \geq 2,\ i \in \{1,2,...,P_{R-2n}\}$, где P_{R-2n} – число классов $(R-2n)$-неотличимых состояний. Так как $R = 4n-1$, то $P_{R-2n} = 2n$, и, следовательно, $\left|\alpha_i^{R-2n}\right| = 2,\ i \in \{1,2,...,P_{R-2n}\}$. Согласно лемме 3, это противоречит приведенности автомата A.

Для доказательства необходимости условий теоремы 4 покажем, что при любом $D \geq 2n, D \leq 4n-1$ существует автомат в классе $A(4n, D)$, для которого $R = 4n-1$. При $D = 4n-1$ в качестве такого автомата можно взять автономный автомат с выходным алфавитом $Y = \{0,1\}$, функцией переходов

$$h: \begin{matrix} i \to i+1, i \neq 4n \\ 4n \to 1 \end{matrix}$$

и функцией выхода $\lambda: \lambda(1) = 1, \lambda(2) = \lambda(3) = ... = \lambda(4n) = 0$. Элементарная проверка показывает, что для данного автомата $R = 4n-1$. Для нахождения искомых автоматов при 4n–2≥D≥2n построим семейство автоматов $(A_{4n,4n-2})_{n=1,2...}$. В качестве автомата $A_{4,2}$ возьмем автомат $A_{4,2} = \left(X_{4,2}, S_{4,2}, Y_{4,2}, h^{4,2}, \lambda^{4,2}\right)$

$$X_{4,2}=\{1,2,3\},\ S_{4,2}=\{1,2,3,4\},\ Y_{4,2}=\{0,1\},$$

$$h_1^{4,2}:\begin{matrix}1\to 3\\2\to 2\\3\to 1\\4\to 4\end{matrix},\quad h_2^{4,2}:\begin{matrix}1\to 1\\2\to 3\\3\to 2\\4\to 4\end{matrix},\quad h_2^{4,2}:\begin{matrix}1\to 1\\2\to 2\\3\to 4\\4\to 3\end{matrix},$$

$$\lambda^{4,2}(1)=1\quad \lambda^{4,2}(2)=\lambda^{4,2}(3)=\lambda^{4,2}(4)=0.$$

Для $n=2$ определим автомат $A_{8,6}=\left(X_{8,6},S_{8,6},Y_{8,6},h^{8,6},\lambda^{8,6}\right)$ следующим образом:

$$X_{8,6}=\{1,2,3\},\ S_{8,6}=\{1,2,...,8\},\ Y_{8,6}=\{0,1\},$$

$$h_1^{8,6}:\begin{matrix}5\to 7\\7\to 5\\j\to j,\ j\neq 5,7\end{matrix},\quad h_2^{8,6}:\begin{matrix}6\to 7\\7\to 6\\j\to j,\ j\neq 6,7\end{matrix},\quad h_3^{8,6}:\begin{matrix}1\to 3\\2\to 4\\3\to 5\\4\to 6\\5\to 1\\6\to 2\\7\to 8\\8\to 7\end{matrix},$$

$$\lambda^{8,6}(1)=\lambda^{8,6}(2)=\lambda^{8,6}(8)=1,$$

$$\lambda^{8,6}(3)=\lambda^{8,6}(4)=\lambda^{8,6}(5)=\lambda^{8,6}(6)=\lambda^{8,6}(7)=0.$$

При $n\geq 3$ в качестве автомата $A_{4n,4n-2}$ возьмем автомат

$$A_{4n,4n-2}=(X_{4n,4n-2},S_{4n,4n-2},Y,h,\lambda)$$

$$X_{4n,4n-2}=\{1,2,3,4\},\ S_{4n,4n-2}=\{1,2,...,4n\}$$

$$h_1:\begin{matrix}4n-3\leftrightarrow 4n-1\\j\to j,\ j\neq 4n-3,4n-1\end{matrix},\quad h_2:\begin{matrix}4n-2\leftrightarrow 4n-1\\j\to j,\ j\neq 4n-2,4n-1\end{matrix},$$

$$h_3:\begin{matrix}1\to 3\\3\to 5\\5\to 1\\2\to 4\\4\to 6\\6\to 2\end{matrix}$$

$$7\leftrightarrow 9,\ 11\leftrightarrow 13,...,\ 7+4k\leftrightarrow 7+4k+2,...,\ 4n-5\leftrightarrow 4n-3$$

$$8\leftrightarrow 10,\ 12\leftrightarrow 14,...,\ 8+4k\leftrightarrow 8+4k+2,...,\ 4n-4\leftrightarrow 4n-2$$

$$4n-1\leftrightarrow 4n$$

$$h_4:\ \begin{array}{c} 1\to 1\\ 2\to 2\\ 3\to 3\\ 4\to 4\\ 4n\to 4n\\ 4n-1\to 4n-1\\ 4n-2\to 4n-2\\ 4n-3\to 4n-3 \end{array}$$

$$5\leftrightarrow 7,\ 9\leftrightarrow 11,\ldots,\ 5+4k\leftrightarrow 5+4k+2,\ldots,\ 4n-7\leftrightarrow 4n-5$$

$$6\leftrightarrow 8,\ 10\leftrightarrow 12,\ldots,\ 6+4k\leftrightarrow 6+4k+2,\ldots,\ 4n-6\leftrightarrow 4n-4$$

Выходная функция $\lambda=\lambda^{4n,4n-2}$ автомата $A_{4n,4n-2}$ зависит от n. При четном n она такова:

$$\lambda(1)=\lambda(2)=1,\quad \lambda(4n)=1,$$
$$\lambda(9)=\lambda(10)=\lambda(11)=\lambda(12)=1,$$
$$\lambda(9+8)=\lambda(10+8)=\lambda(11+8)=\lambda(12+8)=1,$$
$$\ldots$$
$$\lambda(9+k8)=\lambda(10+k8)=\lambda(11+k8)=\lambda(12+k8)=1,$$
$$\ldots$$
$$\lambda(4n-7)=\lambda(4n-6)=\lambda(4n-5)=\lambda(4n-4)=1.$$

На остальных состояниях значение функции λ равно нулю.

При нечетном n λ имеет вид

$$\lambda(1)=\lambda(2)=1,\quad \lambda(4n-1)=\lambda(4n-2)=\lambda(4n-3)=1,$$
$$\lambda(9)=\lambda(10)=\lambda(11)=\lambda(12)=1,$$
$$\ldots$$
$$\lambda(9+k8)=\lambda(10+k8)=\lambda(11+k8)=\lambda(12+k8)=1,$$
$$\ldots$$
$$\lambda(4n-11)=\lambda(4n-10)=\lambda(4n-9)=\lambda(4n-8)=1.$$

На остальных состояниях значение функции λ равно нулю.

При n > 1 строим автомат

$$A_{4n,4n-2-i}=(X_{4n,4n-2-i},S_{4n,4n-2-i},Y,h^{4n,4n-2-i},\lambda^{4n,4n-2-i}).$$

Положим $\lambda^{4n,4n-2-i}=\lambda^{4n,4n-2}$, $i\in[1,2n-2]$,

$$X_{4n,4n-2-i}=X_{4n,4n-2}\cup\{4+1,4+2,\ldots,4+i\};$$
$$h_1^{4n,4n-2-i}=h_1;\ h_2^{4n,4n-2-i}=h_2;\ h_3^{4n,4n-2-i}=h_3;\ h_4^{4n,4n-2-i}=h_4;$$

$$h_{4+1}^{4n,4n-2-i}:\ \begin{array}{c} 4n-2-1\leftrightarrow 4n-2\\ j\to j,\ j\neq 4n-3,4n-2 \end{array},\qquad h_{4+2}^{4n,4n-2-i}:\ \begin{array}{c} 4n-4-1\leftrightarrow 4n-2\\ 4n-4\leftrightarrow 4n-2-1\\ j\to j,\ j\neq 4n-5,4n-4,4n-3,4n-2 \end{array}$$

$$h_{4+3}^{4n,4n-2-i}:\begin{matrix}4n-2\cdot 2-1\leftrightarrow 4n-2\cdot 4\\ j\to j,\ j\neq 4n-5,4n-8\end{matrix},\quad h_{4+4}^{4n,4n-2-i}:\begin{matrix}4n-2\cdot 3-1\leftrightarrow 4n-2\cdot 2\\ 4n-2\cdot 3\leftrightarrow 4n-2\cdot 2-1\\ j\to j,\ j\neq 4n-6,4n-7,4n-4,4n-5\end{matrix}.$$

При нечетном i

$$h_{4+i}^{4n,4n-2-i}:\begin{matrix}4n-2-i\leftrightarrow 4n-1-i\\ j\to j,\ j\neq 4n-2-i,4n-1-i\end{matrix}.$$

При четном i

$$h_{4+i}^{4n,4n-2-i}:\begin{matrix}4n-3-i\leftrightarrow 4n-i\\ 4n-2-i\leftrightarrow 4n-1-i\\ j\to j,\ j\neq 4n-3-i,4n-i,4n-2-i,4n-1-i\end{matrix}.$$

Очевидно, построенные автоматы $A_{4n,4n-2-i}, i\in\{0,2,...,2n-2\}$, являются перестановочными связными автоматами с диаметрами $4n-2-i$. По лемме 2 автоматы $A_{4n,4n-2-i}, i\in\{0,2,...,2n-2\}$ являются приведенными. Сравнительно легко проверяется, что состояния 1, 2 $(4n-2)$-неотличимы в автомате $A_{4n,2n}$, и поэтому они $(4n-2)$-неотличимы в автомате $A_{4n,4n-2-i}, i\in\{0,2,...,2n-2\}$, так как $X_{4n,4n-2-i}\subseteq X_{4n,2n}$.

Таким образом, доказано, что степень различимости построенных автоматов равна $4n-1$.

Теорема 5. Если для автомата A из класса $A(4n+2,D)$ $R=4n+1$, то $D\geq 2n+2$.

Доказательство. Пусть $\alpha_1^m,...,\alpha_{P_m}^m$ – классы m-неотличимых состояний автомата A, P_m – число этих классов. В силу перестановочности, связности автомата A и условия $R=4n+1$, имеем

$$P_{4n-D}=4n-D+1,\ \left|\alpha_i^{4n-D}\right|\geq 2,\ i\in\{1,2,...,P_{4n-D}\}.$$

Поэтому $2\cdot P_{4n-D}\leq 4n-2$, то есть $D\geq 2n$. Если $D=2n$, то $P_{2n}=2n+1$ и $\left|\alpha_i^{2n}\right|=2, i\in\{1,2,...,P_{2n}\}$, что противоречит, согласно лемме 3, условию $R=4n+1$.

Следовательно, $D\geq 2n+1$.

Предположим теперь, что $D=2n+1$. Тогда $P_{2n-1}=2n$, $\left|\alpha_i^{2n-1}\right|\geq 2, i\in\{1,2,...,2n\}$.

Возможны два случая: 1) имеется один класс $(2n-1)$-неотличимых состояний мощности 4 и $2n-1$ классов мощности 2; 2) имеется два класса (2n−1)-неотличимых состояний мощности 3 и $2n-2$ класса мощности 2. Случай 1 и случай 2 при n = 1 противоречат условию R = 4n−1 (см. лемму 3). Остается рассмотреть случай 2 при n > 1. Для его отсева достаточно доказать следующее утвержде-

ние. Если для некоторого m мощности классов m-неотличимых состояний автомата A имеют вид

$$\left|\alpha_1^m\right| = \left|\alpha_2^m\right| = \ldots = \left|\alpha_{P'_m}^m\right| = t_m \quad \left|\alpha_{P'_m+1}^m\right| = \left|\alpha_{P'_m+2}^m\right| = \ldots = \left|\alpha_{P_m}^m\right| = r_m, \; t_m \neq r_m \qquad (10)$$

и $R = 4n-1$, то P'_m, P_m не являются одновременно четными.

Докажем это утверждение. Пусть $\bar{m}$ – минимальное целое, при котором выполняется (10) и $P'_{\bar{m}}, P_{\bar{m}}$ одновременно четные. Очевидно, существуют m_i, при которых выполняются (10) и P'_{m_i}, P_{m_i} не являются одновременно четными. В качестве такого m_i можно взять, например, 1. Из чисел m_i фиксируем максимальное, не превосходящее $\bar{m}$. Пусть это будет $\tilde{m}$. Имеем, что $\left|\alpha_1^{\tilde{m}}\right| = \left|\alpha_2^{\tilde{m}}\right| = \ldots = \left|\alpha_{P'_{\tilde{m}}}^{\tilde{m}}\right| = t_{\tilde{m}}$, $\left|\alpha_{P'_{\tilde{m}}+1}^{\tilde{m}}\right| = \left|\alpha_{P'_{\tilde{m}}+2}^{\tilde{m}}\right| = \ldots = \left|\alpha_{P_{\tilde{m}}}^{\tilde{m}}\right| = r_{\tilde{m}}$ и $P'_{\tilde{m}}, P_{\tilde{m}}$ не являются одновременно четными. Без ограничения общности предположим, что $t_{\tilde{m}} > r_{\tilde{m}}$. Используя лемму 3, можно заключить, что имеется $P'_{\tilde{m}}$ классов $(\tilde{m} - P'_{\tilde{m}})$-неотличимых состояний мощности $t_{\tilde{m}} - r_{\tilde{m}}$ и $P_{\tilde{m}}$ классов $(\tilde{m} + P'_{\tilde{m}})$-неотличимых состояний мощности $r_{\tilde{m}}$.

Из условий выбора $\tilde{m}$, $\bar{m}$ имеем $\tilde{m} + P'_{\tilde{m}} = \bar{m}$. Без ограничения общности доказательства можно считать, что $P'_{\tilde{m}} = P'_{\bar{m}}$, $P_{\bar{m}} = P'_{\tilde{m}} + P_{\tilde{m}}$. Следовательно, одновременная четность $P'_{\bar{m}}, P_{\bar{m}}$ влечет одновременную четность $P'_{\tilde{m}}, P_{\tilde{m}}$, что противоречит выбору $\tilde{m}$.

Таким образом, требуемое утверждение доказано, и вместе с ним завершено доказательство теоремы 5.

7.4. Доказательство достижимости полученной оценки степени различимости

Ниже приводятся примеры автоматов с достижимой оценкой степени различимости, данной в теореме 1.

Теорема 6. Для любого автомата A из класса $A(3\cdot 2^m, 1)$ $m \in N_0$

$$R \leq 2(m+1),$$

причем при любом $m \in N$ существует автомат из $A(3\cdot 2^m, 1)$ со степенью различимости, равной $2(m+1)$.

Доказательство. Первое утверждение теоремы непосредственно вытекает из теоремы 1. Докажем, что при любом целом $m \geq 0$ можно указать автомат из класса $A(3\cdot 2^m,1)$ со степенью различимости R_m, равной 2(m+1). Доказательство проведем индукцией по m. Определим автомат $A_0 = (X^0, S^0, Y, h^0, \lambda^0)$ следующим образом: $Y = \{0, 1\}$, $X^0 = \{1, 2\}$, $S^0 = \{1, 2, 3\}$, $\lambda^0(1) = \lambda^0(2) = 0$, $\lambda^0(3) = 1$,

$$h_1^0: \begin{matrix} 1\to 2 \\ 2\to 3, \\ 3\to 1 \end{matrix} \quad h_2^0: \begin{matrix} 1\to 3 \\ 2\to 1. \\ 3\to 2 \end{matrix}$$

Автомат A_0 является связным перестановочным автоматом Мура с диаметром $D = 1$. Разбиение S^0 на классы $\alpha_1^k, \ldots, \alpha_{P_k}^k$ k-неотличимых состояний состоит из классов

$$\{\alpha_1^1, \ldots, \alpha_{P_1}^1\} = \{(1, 2), (3)\},$$
$$\{\alpha_1^2, \ldots, \alpha_{P_2}^2\} = \{(1), (2), (3)\}.$$

Таким образом, A_0 – приведенный автомат со степенью различимости $R_0 = 2$.

Предположим, что у нас построен автомат A_{m_0} из класса $A(3\cdot 2^{m_0},1)$, для которого $R_{m_0} = 2(m_0+1)$. Построим автомат $\mathrm{A_{m_0+1}} = (\mathrm{X^{m_0+1}}, \mathrm{S^{m_0+1}}, \mathrm{Y}, \mathrm{h^{m_0+1}}, \lambda^{\mathrm{m_0+1}})$ следующим образом:

$$X^{m_0+1} = \{1, 2, \ldots, 2\cdot|X^{m_0}| + 2\};$$
$$S^{m_0+1} = \{1, 2, \ldots, 3\cdot 2^{m_0+1}\}; \mathrm{Y} = \{1, 2\}.$$

Если для $i \in X^{m_0}$ $h_i^{m_0}: j \to k_j^i$, $\mathrm{j} \in \{1, 2, \ldots, 3\cdot 2^{m_0}\}$, то для автомата A_{m_0+1} положим:

$$h_{2i-1}^{m_0+1}: \begin{matrix} 2j\to 2k_j^i \\ 2j-1\to 2k_j^i-1 \end{matrix}, \quad h_{2i}^{m_0+1}: \begin{matrix} 2j\to 2k_j^i-1 \\ 2j-1\to 2k_j^i \end{matrix},$$
$$h_{2|X^{m_0}|+1}^{m_0+1}: 2j \leftrightarrow 2j-1.$$

В классах $(R_{m_0}-1)$-неотличимых состояний автомата выбираем класс мощности 2 вида $\{t-1, t\}$ при четном t. При этом, конечно, мы дополнительно предполагаем наличие класса такого вида у автомата A_{m_0}. Отметим, что для автомата $\mathrm{A_0}$ такой класс существует – это класс $\{1, 2\}$. Положим

$$h_{2|X^{m_0}|+2}^{m_0+1}: \begin{matrix} 2(t-1)\leftrightarrow 2t-1 \\ j\to j,\ j\in X^{m_0+1},\ j\neq 2(t-1), 2t-1; \end{matrix}$$
$$\lambda^{m_0+1}(1)= \lambda^{m_0+1}(2)=\ldots= \lambda^{m_0+1}(2^{m_0+2})=0;$$
$$\lambda^{m_0+1}(2^{m_0+2}+1)=\lambda^{m_0+1}(2^{m_0+2}+2)=\ldots=\lambda^{m_0+1}(3\cdot 2^{m_0+2})=1.$$

Автомат A_{m_0+1}, очевидно, перестановочный. Покажем, что автомат A_{m_0+1} связный и его диаметр равен единице. Для этого фиксируем произвольную пару состояний $\mathrm{s}, \mathrm{u} \in S^{m_0+1}$, $\mathrm{s} \neq \mathrm{u}$. Для произвольного целого $j \geq 1$ положим

$$\overline{j} = \begin{cases} \dfrac{j}{2}, \text{ если } j \text{ четное} \\ \dfrac{j+1}{2}, \text{ если } j \text{ нечетное} \end{cases}.$$

По предположению, автомат A_{m_0} связный и его диаметр равен единице, следовательно, если $\overline{s} \neq \overline{u}$, то найдется $i \in X^{m_0}$, при котором $h_i^{m_0} : \overline{s} \to \overline{u}$, но тогда

$$h_{2i-1}^{m_0+1} : \begin{matrix} 2\overline{s} \to 2\overline{u} \\ 2\overline{s}-1 \to 2\overline{u}-1 \end{matrix}, \; h_{2i}^{m_0+1} : \begin{matrix} 2\overline{s} \to 2\overline{u}-1 \\ 2\overline{s}-1 \to 2\overline{u} \end{matrix};$$

таким образом, одна из этих подстановок переведет s в u. Если $\overline{s} = \overline{u}$, то

$$s = \begin{cases} u+1, \text{ если } s \text{ четное} \\ u-1, \text{ если } s \text{ нечетное} \end{cases},$$

и тогда

$$h_{2|X^{m_0}|+1}^{m_0+1} : s \to u.$$

Определим вспомогательный автомат $\tilde{A}_{m_0+1}$, положив

$$\tilde{A}_{m_0+1} = (\tilde{X}^{m_0+1}, S^{m_0+1}, Y, \tilde{h}^{m_0+1}, \tilde{\lambda}^{m_0+1}),$$

где

$$\tilde{X}^{m_0+1} = \{1, 2, \ldots, 2\cdot|X^{m_0}|\},$$
$$\tilde{h}_i^{m_0+1} = h_i^{m_0+1}, \quad i \in \{1, 2, \ldots, 2\cdot|X^{m_0}|\}, \; \tilde{\lambda}^{m_0+1} = \lambda^{m_0+1}.$$

Обозначим через ψ и φ отображения множеств $\tilde{X}^{m_0+1}$ и S^{m_0+1} соответственно в множества X^{m_0} и S^{m_0}

$$\psi: \; j \to \overline{j}, \; \overline{j} = \begin{cases} \dfrac{j}{2}, \text{ если } j \text{ четное} \\ \dfrac{j+1}{2}, \text{ если } j \text{ нечетное} \end{cases}$$

$$\varphi: \; s \to \overline{s}, \; \overline{s} = \begin{cases} \dfrac{s}{2}, \text{ если } s \text{ четное} \\ \dfrac{s+1}{2}, \text{ если } s \text{ нечетное.} \end{cases}$$

Непосредственно проверяется, что при любом $s \in S^{m_0+1}$ и $j \in \tilde{X}^{m_0+1}$

$$\phi h_j^{m_0+1} s = h_{\psi(j)}^{m_0} \phi s, \quad \lambda^{m_0+1} s = \lambda^{m_0} \phi s.$$

Поэтому при любом входном слове $x_1, x_2, \ldots, x_l$ автомата A_{m_0+1} справедливо равенство

$$\tilde{\lambda}^{m_0+1} \tilde{h}_{x_l}^{m_0+1} \tilde{h}_{x_{l-1}}^{m_0+1} \ldots \tilde{h}_{x_1}^{m_0+1} s = \lambda^{m_0} \phi h_{x_l}^{m_0+1} h_{x_{l-1}}^{m_0+1} \ldots h_{x_1}^{m_0+1} s =$$
$$= \lambda^{m_0} h_{\psi(x_l)}^{m_0} h_{\psi(x_{l-1})}^{m_0} \ldots h_{\psi(x_1)}^{m_0} \phi s,$$

из которого следует, что каждому классу k-неотличимых состояний автомата A_{m_0} вида $\{s_1, s_2, \ldots, s_r\}$ соответствует в разбиении множе-

ства состояний S^{m_0+1} автомата $\tilde{A}_{m_0+1}$ на классы k-неотличимых состояний класс вида $\{2s_1-1, 2s_1, 2s_2-1, 2s_2, \ldots, 2s_r-1, 2s_r\}$. Учитывая дополнительное предположение о наличии у автомата A_{m_0} класса $(R_{m_0} - 1)$ – неотличимых состояний вида $\{(t-1), t\}$, где t – четное, получаем, что у автомата $\tilde{A}_{m_0+1}$ имеется класс $(R_{m_0} - 1)$-неотличимых состояний вида $\{2(t-1)-1, 2(t-1), 2t-1, 2t\}$, а классы R_{m_0}-неотличимых состояний имеют вид $\{2j-1, 2j\}$, $j \in S^{m_0}$. Автомат A_{m_0+1} отличается от автомата $\tilde{A}_{m_0+1}$ наличием дополнительных подстановок $h^{m_0+1}_{2|X^{m_0}|+1}$, $h^{m_0+1}_{2|X^{m_0}|+2}$, причем данные подстановки переводят любой класс $(R_{m_0}-1)$-неотличимых состояний автомата $\tilde{A}_{m_0+1}$ в себя. Поэтому все классы k-неотличимых состояний автомата $\tilde{A}_{m_0+1}$ при $k \le R_{m_0}$ будут классами k-неотличимых состояний автомата A_{m_0+1}. Каждая из подстановок $h_i^{m_0+1}$, $i \in \{1,2,\ldots,2\cdot|X^{m_0}|+1\}$ переводит любой класс R_{m_0}-неотличимых состояний автомата A_{m_0+1} в себя, а подстановка $h^{m_0+1}_{2|X^{m_0}|+2}$ «разбивает» классы R_{m_0} – неотличимых состояний $\{2(t-1)-1,2(t-1)\}$ и $\{2t-1, 2t\}$ на четыре одноэлементных класса. Остальные же классы R_{m_0}-неотличимых состояний автомата A_{m_0+1} данная подстановка переводит в себя. Следовательно, классами $(R_{m_0} + 1)$-неотличимых состояний автомата A_{m_0+1} являются пары $\{2j - 1, 2j)$ при $j \ne t, t - 1$ и одноэлементные множества $\{2(t - 1) - 1\}$, $\{2(t - 1)\}$, $\{2t - 1\}$, $\{2t\}$. Классы же $(R_{m_0} + 2)$-неотличимых состояний автомата A_{m_0+1} состоят, очевидно, из одноэлементных множеств. Таким образом, $R_m = 2(m + 1)$ при любом целом $m > 0$.

Следующие автоматы могут служить иллюстрацией проведенного доказательства. Для автомата $A_1 = (X^1, S^1, Y, \delta^1, \lambda^1)$ положим

$$X^1 = \{1, 2, 3, 4, 5, 6\},\ S^1 = \{1, 2, 3, 4, 5, 6\},$$

$$\lambda^1(1) = \lambda^1(2) = \lambda^1(3) = \lambda^1(4) = 0,\ \lambda^1(5) = \lambda^1(6) = 1,$$

а функцию переходов δ^1_j определим подстановками

$$h^1_1 = \begin{pmatrix} 123456 \\ 345612 \end{pmatrix},\ h^1_2 = \begin{pmatrix} 123456 \\ 436521 \end{pmatrix},\ h^1_3 = \begin{pmatrix} 123456 \\ 561234 \end{pmatrix},$$

$$h^1_4 = \begin{pmatrix} 123456 \\ 652143 \end{pmatrix},\ h^1_5 = \begin{pmatrix} 123456 \\ 214365 \end{pmatrix},\ h^1_6 = \begin{pmatrix} 123456 \\ 132456 \end{pmatrix}.$$

Разбиение S^1 на классы k-неотличимых состояний автомата A_1 имеют вид, представленный в табл. 15.

Таблица 15

K	$\alpha_1^k,\ \alpha_2^k,\ \alpha_3^k,\ \ldots,\ \alpha_{P_k}^k$					
1	{1, 2, 3, 4}				{5, 6}	
2	{1, 2}		{3, 4}		{5, 6}	
3	{1}	{2}	{3}	{4}	{5, 6}	
4	{1}	{2}	{3}	{4}	{5}	{6}

Определим автомат $A_2 = (X^2, S^2, Y, h^2, \lambda^2)$ следующим образом: $X^2 = \{1, 2, \ldots, 14\}$, $S^2 = \{1, 2, \ldots, 12\}$. Нижние строки подстановок $h_j^2 = \begin{pmatrix} i \\ k_i \end{pmatrix}$ зададим в табл. 16.

Таблица 16

j	k_1	k_2	k_3	k_4	k_5	k_6	k_7	k_8	k_9	k_{10}	k_{11}	k_{12}
1	5	6	7	8	9	10	11	12	1	2	3	4
2	6	5	8	7	10	9	12	11	2	1	4	3
3	7	8	5	6	11	12	9	10	3	4	1	2
4	8	7	6	5	12	11	10	9	4	3	2	1
5	9	10	11	12	1	2	3	4	5	6	7	8
6	10	9	12	11	2	1	4	3	6	5	8	7
j	k_1	k_2	k_3	k_4	k_5	k_6	k_7	k_8	k_9	k_{10}	k_{11}	k_{12}
7	11	12	9	10	3	4	1	2	7	8	5	6
8	12	11	10	9	4	3	2	1	8	7	6	5
9	3	4	1	2	7	8	5	6	11	12	9	10
10	4	3	2	1	8	7	6	5	12	11	10	9
11	1	2	5	6	3	4	7	8	9	10	11	12
12	2	1	6	5	4	3	8	7	10	9	12	11
13	2	1	4	3	6	5	8	7	10	9	12	11
14	1	2	3	4	5	6	7	8	9	11	10	12

Положим $\lambda^2(s) = 0$ для $s \in \{1, 2, \ldots, 8\}$ и $\lambda^2(s) = 1$ для $s \in \{9, 10, 11, 12\}$. Разбиения S^2 на классы k-неотличимых состояний имеют вид, указанный в табл. 17.

Таблица 17

k	$\alpha_1^k, \alpha_2^k, \alpha_3^k, \ldots, \alpha_{P_k}^k$											
1	{1, 2, 3, 4, 5, 6, 7, 8}								{9, 10, 11, 12}			
2	{1, 2, 3, 4}				{5, 6, 7, 8}				{9, 10, 11, 12}			
3	{1, 2}		{3, 4}		{5, 6}		{7, 8}		{9, 10, 11, 12}			
4	{1, 2}		{3, 4}		{5, 6}		{7, 8}		{9, 10}		{11, 12}	
5	{1, 2}		{3, 4}		{5, 6}		{7, 8}		{9}	{10}	{11}	{12}
6	{1}	{2}	{3}	{4}	{5}	{6}	{7}	{8}	{9}	{10}	{11}	{12}

Теорема 7. Для любого автомата A из класса A($5\cdot 2^m$, 1), $m \in \{0, 1, \ldots\}$

$$R \le 2m + 3.$$

При любом $m \in N$ существует автомат из A($5\cdot 2^m$, 1) со степенью различимости R=$2m$ + 3.

Доказательство этой теоремы проводится с помощью рассуждений, аналогичных доказательству теоремы 6. Основное отличие состоит в том, что в качестве автомата $A_0 = (X^0, S^0, Y, h^0, \lambda^0)$ можно взять автомат с параметрами

$$X^0 = \{1, 2, 3, 4, 5\},\ S^0 = \{1, 2, 3, 4, 5\},$$

$$\lambda^0(1) = \lambda^0(2) = 0,\ \lambda^0(3) = \lambda^0(4) = \lambda^0(5) = 1,$$

$$h_1^0 = \begin{pmatrix} 12345 \\ 34125 \end{pmatrix},\ h_2^0 = \begin{pmatrix} 12345 \\ 45312 \end{pmatrix},\ h_3^0 = \begin{pmatrix} 12345 \\ 53241 \end{pmatrix},$$

$$h_4^0 = \begin{pmatrix} 12345 \\ 21453 \end{pmatrix},\ h_5^0 = \begin{pmatrix} 12345 \\ 21534 \end{pmatrix}.$$

Теорема 8. Для любого автомата A из класса A($5\cdot 2^m$, 2) $m \in \{0, 1, \ldots\}$

$$R \le 3m + 4.$$

При любом $m \in \{0, 1, \ldots\}$ существует автомат из A($5\cdot 2^m$, 2) со степенью различимости, равной $3m$ + 4.

Доказательство. По теореме 1 для любого автомата из класса A($5\cdot 2^m$, 2) степень различимости $R_m \le 3m+4$. Докажем, что при любом целом $m \ge 0$ можно указать автомат из класса $A(5\cdot 2^m, 2)$, для которого достижима указанная оценка. Для m = 0 рассмотрим автомат $A_0 = (X^0, S^0, Y, h^0, \lambda^0)$, у которого

$$X^0 = \{1, 2, 3\},\ S^0 = \{1, 2, 3, 4, 5\},$$

$$\lambda^0(1) = \lambda^0(2) = \lambda^0(3) = 0,\ \ \lambda^0(4) = \lambda^0(5) = 1,$$

$$h_1^0 = \begin{pmatrix} 12345 \\ 15432 \end{pmatrix},\ h_2^0 = \begin{pmatrix} 12345 \\ 31254 \end{pmatrix},\ h_3^0 = \begin{pmatrix} 12345 \\ 23145 \end{pmatrix}.$$

Автомат $A_0 \in A(5\cdot 2^0, 2)$ и разбиения множества его состояний на классы k-неотличимых состояний имеют вид, показанный в табл. 18.

Таблица 18

K	$\alpha_1^k,\ \alpha_2^k,\ \alpha_3^k,\ \ldots, \alpha_{P_k}^k$				
1	{1, 2, 3}			{4, 5}	
2	{1}	{2, 3}		{4, 5}	
3	{1}	{2}	{3}	{4, 5}	
4	{1}	{2}	{3}	{4}	{5}

Таким образом, для автомата A_0

$$R_0 = 4.$$

Предположим теперь, что у нас построен автомат $\mathbf{A_{m_0}} = (\mathbf{X^{m_0}, S^{m_0}, Y, h^{m_0}, \lambda^{m_0}})$ из класса $A(5\cdot 2^{m_0},\ 2)$, для которого $R_{m_0} = 3m_0+4$. Причем у автомата A_{m_0} при нечетном m_0 состояния {1, 2} образуют класс $(R_{m_0} - 1)$-неотличимых состояний, а при четном m_0 – множество состояний $\{5\cdot 2^{m_0} - 1,\ \ 5\cdot 2^{m_0}\}$ является классом $(R_{m_0} - 1)$-неотличимых состояний.

Построим автомат $\mathbf{A_{m_0+1}} = (X,\ S,\ Y,\ h,\ \lambda)$ следующим образом:

$$X = \{1, 2, \ldots, 2\cdot|X^{m_0}|+2\},\ S = \{1, 2, \ldots, 5\cdot 2^{m_0+1}\}.$$

Если для $x \in X^{m_0}$

$$h_x^{m_0} : j \to k_j^{(x)},\ j \in \{1,2,\ldots,\ 5\cdot 2^{m_0}\},$$

то для автомата A_{m_0+1} положим

$$h_{2x-1} : \begin{matrix} 2j \to 2k_j^{(x)} \\ 2j-1 \to 2k_j^{(x)} - 1 \end{matrix},\quad h_{2x} : \begin{matrix} 2j \to 2k_j^{(x)} - 1 \\ 2j-1 \to 2k_j^{(x)} \end{matrix},$$

$$h_{2\cdot|X^{m_0}|+1} : \begin{matrix} 2j \to 2j-1 \\ 2j-1 \to 2j \end{matrix}.$$

В классах $(R_{m_0} - 1)$-неотличимых состояний автомата A_{m_0} выбираем класс {t−1, t}, где t = 2 при m_0 нечетном и $t = 5\cdot 2^{m_0}$ при четном m_0, и полагаем

$$\mathbf{h_{2|X^{m_0}|+2}}: \begin{matrix} 2(t-1) \leftrightarrow 2t-1 \\ j \to j,\ j \in X,\ j \neq 2(t-1),\ 2t-1; \end{matrix}$$
$$\lambda(1) = \lambda(2) = \ldots = \lambda(3\cdot 2^{m_0+1}) = 0;$$

$$\lambda(3\cdot 2^{m_0+1}+1) = \ldots = \lambda(5\cdot 2^{m_0+1}) = 1.$$

Автомат A_{m_0+1}, очевидно, перестановочный. Покажем, что он связный с диаметром 2. Для произвольного целого $j \geq 1$ положим:

$$\bar{j} = \begin{cases} \dfrac{j}{2}, \text{ если } j \text{ четное} \\ \dfrac{j+1}{2}, \text{ если } j \text{ нечетное.} \end{cases}$$

Фиксируем произвольную пару состояний s, u, $s \neq u$ автомата A_{m_0+1}. По предположению A_{m_0} связный с диаметром 2. Поэтому если $\bar{s} \neq \bar{u}$, то существует входное слово $\bar{j}_1, \ldots, \bar{j}_l$ автомата A_{m_0} длины $l \in \{1, 2\}$, при котором

$$h^{m_0}_{\bar{j}_l} \ldots h^{m_0}_{\bar{j}_1} \bar{s} = \bar{u}.$$

При $l = 1$ одна из следующих подстановок автомата A_{m_0+1} переведет s в u:

$$h_{2\bar{j}_1-1}: \begin{matrix} 2\bar{s} \to 2\bar{u} \\ 2\bar{s}-1 \to 2\bar{u}-1 \end{matrix}, \quad h_{2\bar{j}_1}: \begin{matrix} 2\bar{s} \to 2\bar{u}-1 \\ 2\bar{s}-1 \to 2\bar{u} \end{matrix}.$$

При $l = 2$ имеем

$$\delta^{m_0}_{\bar{j}_1} \bar{s} = \bar{a}, \; h^{m_0}_{\bar{j}_2} \bar{a} = \bar{u},$$

и, по доказанному выше, одна из подстановок $h_{2\bar{j}_1-1}$, $h_{2\bar{j}_1}$ переведет s в a, и одна из подстановок $h_{2\bar{j}_2-1}$, $h_{2\bar{j}_2}$ переведет a в u. Если $\bar{s} = \bar{u}$, то $h_{2\cdot|X|^{m_0}+1} s = u$.

Определим вспомогательный автомат $\tilde{A} = (\tilde{X}, S, Y, \tilde{h}, \tilde{\lambda})$, положив

$$\tilde{X} = \{1, 2, \ldots, 2\cdot|X|^{m_0}\}, \; \tilde{h}_x = h_x, \; x \in \tilde{X}, \; \tilde{\lambda} = \lambda.$$

Обозначим через ψ и φ отображения множеств $\tilde{X}$ и $S = \{1, 2, \ldots, 5\cdot 2^{m_0+1}\}$ соответственно в множество X^{m_0} и $S^{m_0} = \{1, 2, \ldots, 5\cdot 2^{m_0}\}$:

$$\psi: \; j \to \bar{j}, \; j \in \tilde{X}; \; \varphi: \; s \to \bar{s}, \; s \in S.$$

Легко видеть, что

$$\varphi \tilde{h}_j s = h_{\psi(j)} \varphi s, \; j \in \tilde{X}, \; s \in S; \; \tilde{\lambda} s = \lambda^{m_0} \varphi s.$$

Поэтому при любом входном слове $x_1, x_2, \ldots, x_l$ автомата $\tilde{A}$ справедливо равенство

$$\tilde{\lambda} \tilde{h}_{x_l} \tilde{h}_{x_{l-1}} \ldots \tilde{h}_{x_1} s = \lambda^{m_0} h^{m_0}_{\psi(x_l)} h^{m_0}_{\psi(x_{l-1})} \ldots h^{m_0}_{\psi(x_1)} \varphi s.$$

Из этого равенства вытекает, что каждому классу k-неотличимых состояний автомата A_{m_0} вида $\{s_1, s_2, \ldots, s_r\}$ соответствует в разбиении множества состояний автомата $\tilde{A}$, класс $\{2s_1-1, 2s_1, 2s_2-1, 2s_2, \ldots, 2s_r-1, 2s_r\}$. В частности, классы $(R_{m_0} - 1)$-

неотличимых состояний автомата $\tilde{A}$ содержат класс {2(t − 1) − 1, 2(t − 1), 2t − 1, 2t}, где t = 2 при нечетном m_0 и $t = 5\cdot 2^{m_0}$ при четном m_0, а классы R_{m_0}-неотличимых состояний автомата $\tilde{A}$ имеют вид

$$\{1, 2\};\ \{3, 4\};\ \{5, 6\};\ \ldots;\ \{5\cdot 2^{m_0+1}-1,\ 5\cdot 2^{m_0+1}\}.$$

Заметим, что подстановка $h_{2\cdot|X|^{m_0}+1}$ переводит каждый класс R_{m_0}–неотличимых состояний автомата $\tilde{A}$ в себя, а $h_{2\cdot|X|^{m_0}+2}$ переводит каждый класс $\{R_{m_0}-1)$-неотличимых состояний в себя и «разбивает» классы {2(t−1)−1, 2{t−1)} и {2t−1, 2t} R_{m_0}-неотличимых состояний на четыре одноэлементных класса {2(t−1)−1}, {2(t−1)}, {2t−1}, {2t}. В силу изложенного можно сделать вывод о том, что классы R_{m_0}-неотличимых состояний автоматов A_{m_0+1} и $\tilde{A}$ совпадают, а классы (R_{m_0} + 1)-неотличимых состояний автомата A_{m_0+1} имеют вид при нечетном m_0

$$\{1\};\ \{2\};\ \{3\};\ \{4\};\ \{5, 6\};\ \{7, 8\};\ \ldots;\ \{5\cdot 2^{m_0+1}-1,\ 5\cdot 2^{m_0+1}\},$$

а при четном m_0

$$\{1, 2\};\ \{3, 4\};\ \ldots;\ \{5\cdot 2^{m_0+1}-5,\ 5\cdot 2^{m_0+1}-4\};\ \{5\cdot 2^{m_0+1}-3\};\ \{5\cdot 2^{m_0+1}-2\};$$
$$\{5\cdot 2^{m_0+1}-1\};\ \{5\cdot 2^{m_0+1}\}.$$

Покажем, что классы (R_{m_0} + 2)-неотличимых состояний автомата A_{m_0+1} содержат класс $\{5\cdot 2^{m_0+1}-1,\ 5\cdot 2^{m_0+1}\}$ при m_0 – нечетном и класс {1, 2} при четном m_0. Для этого, очевидно, достаточно показать, что при любом $x\in X$ выполняются соотношения:

$h_x(5\cdot 2^{m_0+1}-1)\notin\{1, 2, 3, 4\}$, $h_x(5\cdot 2^{m_0+1})\notin\{1, 2, 3, 4\}$, если m_0 нечетное, и

$$h_x(1)\notin\{5\cdot 2^{m_0+1}-3,\ 5\cdot 2^{m_0+1}-2,\ 5\cdot 2^{m_0+1}-1,\ 5\cdot 2^{m_0+1}\},$$

$h_x(2)\notin\{5\cdot 2^{m_0+1}-3,\ 5\cdot 2^{m_0+1}-2,\ 5\cdot 2^{m_0+1}-1,\ 5\cdot 2^{m_0+1}\}$, если m_0 четное.

Доказательство этого утверждения проведем индукцией по m_0. При $m_0 = 0$ рассмотрим автомат A_1. Согласно законам построения автоматов A_m, автомат $A_1 = (X^1, S^1, Y, h^1, \lambda^1)$ имеет вид $X^1 = \{1, 2, 3, \ldots, 8\}$, $S^1 = \{1, 2, 3, \ldots, 10\}$. Нижние строки подстановок $h^1_j = \begin{pmatrix} i \\ k_i \end{pmatrix}$ задаются табл. 19.

Функция выхода λ^1 принимает значения:

$$\lambda^1\{1) = \lambda^1\{2)=\lambda^1\{3) = \lambda^1\{4) = \lambda^1\{5) = \lambda^1\{6) = 0,$$
$$\lambda^1\{7)=\lambda^1\{8) =\lambda^1\{9) =\lambda^1\{10) =1.$$

Элементарная проверка показывает, что при любом $x\in X^1$

$$h_x(1)\notin\{7, 8, 9, 10\},\ h_x(2)\notin\{7, 8, 9, 10\}.$$

Таблица 19

j	k_1	k_2	k_3	k_4	k_5	K_6	k_7	k_8	k_9	k_{10}
1	1	2	9	10	7	8	5	6	3	4
2	2	1	10	9	8	7	6	5	4	3
3	5	6	1	2	3	4	9	10	7	8
4	6	5	2	1	4	3	10	9	8	7
5	3	4	5	6	1	2	7	8	9	10
6	4	3	6	5	2	1	8	7	10	9
7	2	1	4	3	6	5	8	7	10	9
8	1	2	3	4	5	6	7	8	9	10

При $m_0 = 1$ рассмотрим автомат $\mathrm{A_2} = (\mathrm{X^2}, \mathrm{S^2}, \mathrm{Y}, \mathrm{h^2}, \lambda^2)$: $X^2 = \{1, 2, \ldots, 18\}$, $S^2 = \{1, 2, \ldots, 20\}$.

Нижние строки подстановок h_j^2 задаются в табл. 20.

Таблица 20

j	*k*1	*k*2	*k*3	*k*4	*k*5	*k*6	*k*7	*K*8	*k*9	*k*10	*k*11	*k*12	*k*13	*k*14	*k*15	*k*16	*k*17	*k*18	*k*19	*k*20
1	1	2	3	4	17	18	19	20	13	14	15	16	9	10	11	12	5	6	7	8
2	2	1	4	3	18	17	20	19	14	13	16	15	10	9	12	11	6	5	8	7
3	3	4	1	2	19	20	17	18	15	16	13	14	11	12	9	10	7	8	5	6
4	4	3	2	1	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5
5	9	10	11	12	1	2	3	4	5	6	7	8	17	18	19	20	13	14	15	16
6	10	9	12	11	2	1	4	3	6	5	8	7	18	17	20	19	14	13	16	15
7	11	12	9	10	3	4	1	2	7	8	5	6	19	20	17	18	15	16	13	14
8	12	11	10	9	4	3	2	1	8	7	6	5	20	19	18	17	16	15	14	13
9	5	6	7	8	9	10	11	12	1	2	3	4	13	14	15	16	17	18	19	20
10	6	5	8	7	10	9	12	11	2	1	4	3	14	13	16	15	18	17	20	19
11	7	8	5	6	11	12	9	10	3	4	1	2	15	16	13	14	19	20	17	18
12	8	7	6	5	12	11	10	9	4	3	2	1	16	15	14	13	20	19	18	17
13	3	4	1	2	7	8	5	6	11	12	9	10	15	16	13	14	19	20	17	18
14	4	3	2	1	8	7	6	5	12	11	10	9	16	15	14	13	20	19	18	17
15	1	2	3	4	5	6	7	8	9	10	11	12	13	14	17	18	15	16	19	20
16	2	1	4	3	6	5	8	7	10	9	12	11	14	13	18	17	16	15	20	19
17	2	1	4	3	6	5	8	7	10	9	12	11	14	13	16	15	18	17	20	19
18	1	3	2	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20

Функция выхода λ^2 принимает следующие значения:

$\lambda^2(1) = \lambda^2(2) = \ldots = \lambda^2(12) = 0$; $\lambda^2(13) = \lambda^2(14) = \ldots = \lambda^2(20)$ 1.

Непосредственно проверяется, что при любом $x \in X^2$

$$h_x(1) \notin \{17, 18, 19, 20\}; h_x(2) \notin \{17, 18, 19, 20\};$$
$$h_x(19) \notin \{1, 2, 3, 4\}; h_x(20) \notin \{1, 2, 3, 4\}.$$

Предположим теперь, что при некотором $m_0 \geq 1$ выполняются соотношения

$$h_x(1) \notin \{5\cdot 2^{m_0+1} - 3,\ 5\cdot 2^{m_0+1} - 2,\ 5\cdot 2^{m_0+1} - 1,\ 5\cdot 2^{m_0+1}\},$$
$$h_x(2) \notin \{5\cdot 2^{m_0+1} - 3,\ 5\cdot 2^{m_0+1} - 2,\ 5\cdot 2^{m_0+1} - 1,\ 5\cdot 2^{m_0+1}\},$$
$$h_x(5\cdot 2^{m_0+1} - 1) \notin \{1, 2, 3, 4\},\ h_x(5\cdot 2^{m_0+1}) \notin \{1, 2, 3, 4\},\ x \in X,$$

а для $m_0 + 1$ нашлось $x_0 \in X^{m_0+2}$, для которого справедливо одно из соотношений:

1) $h_{x_0}^{m_0+2}(1) \in \{5\cdot 2^{m_0+2} - 3,\ 5\cdot 2^{m_0+2} - 2,\ 5\cdot 2^{m_0+2} - 1,\ 5\cdot 2^{m_0+2}\}$;
2) $h_{x_0}^{m_0+2}(2) \in \{5\cdot 2^{m_0+2} - 3,\ 5\cdot 2^{m_0+2} - 2,\ 5\cdot 2^{m_0+2} - 1,\ 5\cdot 2^{m_0+2}\}$;
3) $h_{x_0}^{m_0+2}(5\cdot 2^{m_0+2} - 1) \in \{1, 2, 3, 4\}$;
4) $h_{x_0}^{m_0+2}(5\cdot 2^{m_0+2}) \in \{1, 2, 3, 4\}$.

Из этих условий и того, что $m_0 \geq 1$, следует $x_0 \in [1, 2\cdot|X|] \subset X^{m_0+2}$. Поэтому, согласно законам функционирования автоматов A_{m_0+1}, A_{m_0+2}, должно выполняться одно из следующих включений:

1) $h_{\bar{x}_0}(1) \in \{5\cdot 2^{m_0+1} - 1,\ 5\cdot 2^{m_0+1}\}$;
2) $h_{\bar{x}_0}(5\cdot 2^{m_0+1}) \in \{1, 2\}$.

Эти соотношения противоречат начальному предположению. Таким образом, требуемые соотношения для автомата A_{m_0+1} доказаны.

Очевидно, автомат A_{m_0+1} приведенный, а ранее было показано, что он имеет (R_{m_0} +2)-неотличимые различные состояния, и кроме того отмечено, что степень различимости автомата A_{m_0+1} удовлетворяет неравенству $R_{m_0+1} \leq R_{m_0} + 3$. Поэтому для автомата A_{m_0+1}

$$R_{m_0+1} = R_{m_0} + 3 = 3(m_0 + 1) + 4.$$

Теорема 8 полностью доказана.

Глава 8. НЕОТЛИЧИМОСТЬ СОСТОЯНИЙ ПЕРЕСТАНОВОЧНЫХ, АФФИННЫХ И АВТОНОМНЫХ НЕЛИНЕЙНЫХ ВЕКТОРНЫХ АВТОМАТОВ

В главе приводятся методы расчета классов k-неотличимых и неотличимых состояний автоматов – перестановочных, аффинных и автономных нелинейных векторных.

8.1. Основные понятия

Пусть A = (X, S, Y, h, f) – конечный автомат. Напомним некоторые обозначения: h_x: S→S – частичная функция переходов автомата A соответствующая входному символу x∈X, задаваемая соотношением $h_x(s) = h(s, x)$, s∈S (для удобства ниже в этой записи мы опускаем скобки при h_x: $h_x s = h(s, x)$); f_x: S→Y – частичная функция выхода соответствующая входному символу x∈X, задаваемая соотношением $f_x(s) = f(s, x)$, s∈S (для удобства ниже в этой записи мы опускаем скобки при f_x : $f_x s = f(s, x)$). Если f(s,x)=λ(s) для любых x∈X, s∈S, где λ: S→Y, автомат Мили A может рассматриваться как автомат Мура и он будет обозначаться через A = (X, S, Y, h, λ). Если же f(s, x) = s для любых x∈X и s∈S (в этом случае, очевидно Y = S), то автомат A может рассматриваться как автомат Медведева и будет обозначаться через A_M = (X, S, h). Напомним также, что если X состоит из одного элемента |X| = 1, то такой автомат называется автономным и он будет обозначаться через A = (S, Y, h, λ).

Положим для краткости:

1) $h_P = h_{x(k-1)}\, h_{x(k-1)} \ldots h_{x(1)}$ – отображение S→S, осуществляемое автоматом A в результате приложения к нему входного слова P = x(1), x(2), ..., x(k);

2) $f_P = f_{x(k)}\, h_{x(k-1)}\, h_{x(k-1)} \ldots h_{x(1)}$ – отображение S→Y, осуществляемое автоматом A в результате приложения к нему входного слова P= x(1), x(2), …., x(k);

3) [a, b] – наименьшее общее кратное чисел a, b.

Имея дело с несколькими автоматами, будем отмечать пятерки X, S, Y, h, f различными символами (верхними и нижними), например, A = (X_A, S_A, Y_A, h_A , f_A). Если же автомат обозначается символом A с каким-нибудь индексом, например A’, то иногда для простоты мы будем помечать элементы его пятерки тем же индексом, например, (X’, S’, Y’, h’, f’). Аналогичным образом мы будем по-

ступать и для различения введенных параметров автоматов, например, полугруппу автоматов A и B удобно обозначать через G_A и G_B соответственно. Чаще всего мы будем иметь дело непосредственно с частичными функциями переходов $(h_x)_{x\in X}$ и выхода $(f_x)_{x\in X}$ автомата A = (X, S, Y, h, f), в связи с чем для автомата A будет использоваться и такое обозначение:

$$A = (X, S, Y, (h_x)_{x\in X}, (f_x)_{x\in X}).$$

Напомним следующие основные понятия [16; 27; 33].

Определение 1. Состояние s и s' автомата A называется k-неотличимыми, если

$$A(s, P)) = A(s', P)$$

для любого входного слова P = x(1), x(2),…, x(k) длины k автомата A. В противном случае они называются k-различимыми.

Определение 2. Состояния s и s' автомата A называются неотличимыми, если они k-неотличимы для любого k. В противном случае они называются различными (отличными).

Известна следующая теорема.

Теорема 1 [16; 27]. Для неотличимости двух состояний автомата A = (X, S, Y, h, f) достаточна их ($|S| - 1$)-неотличимость.

Поскольку бинарное отношение k-неотличимости состояний автомата является отношением эквивалентности, все множество состояний S автомата A разбивается на непересекающиеся классы k-неотличимых состояний.

Будем обозначать это разбиение через:

$$N^k = (N_1^k, N_2^k, ..., N_{l_k}^k),$$

N_j^k, j ϵ [1, l_k] – классы k-неотличимых состояний автомата A, а l_k – число классов k-неотличимых состояний автомата A. Классы неотличимых состояний автомата A будем обозначать через N_j , j ϵ [1, l], а само разбиение множества S эти классы через

$$N = (N_1, N_2, ..., N_l),$$

l – число классов неотличимых состояний автомата A.

Определение 3. Число R называется степенью различимости автомата A, если

$$N^R = N;$$

$$N^k \neq N \text{ при } k<R.$$

Определение 4. Автомат A называется приведенным (или находится в приведенной форме), если $|N_j| = 1$ для любого $j\in[1, l]$.

Очевидно, что если A приведенный автомат, то $l = |S|$.

Определение 5. Два или более автоматов называется сравнимыми, если они имеют одинаковые входные и выходные алфавиты.

Если A и B сравнимые автоматы, s_A и s_B – состояния автоматов A и B, соответственно, то k-неотличимость и неотличимость этих состояний может быть определена аналогично определениям 1, 2 [16].

Определение 6. Говорят, что сравнимые автоматы A и B k-неотличимы, если каждому состоянию автомата A соответствует по крайней мере одно k-неотличимое от него состояние в автомате B и если каждому состоянию автомата B соответствует по крайней мере одно k-неотличимое от него состояние в автомате A. Если автоматы не являются неотличимыми, то они называются различными.

Очевидно, если автоматы k-неотличимы при любом k, то они неотличимы. Напомним еще одно понятие в теории конченых автоматов [40; 17].

Определение 7. Автомат $A = (X, S, Y, h, f)$ называется перестановочным автоматом, если его частичные функции переходов $(h_x)_{x \in X}$ осуществляют взаимно однозначные отображения множества S в себя.

В случае перестановочного автомата A полугруппа G_A автомата A есть группа. Граф переходов ([16]) перестановочного автомата A распадается на связанные компоненты, которые в силу перестановочности автомата A является сильно связанными [16].

Компонентами автомата A будут называться подавтоматы автомата A, отвечающие соответствующим компонентам его графа переходов.

Очевидно, что компоненты перестановочного автомата являются перестановочными автоматами.

8.2. Неотличимость состояний перестановочных автоматов

Исследование неотличимости состояний конечных автоматов проводились в целом ряде работ [16; 27; 33]. Полученные в них результаты основаны на табличном задании автомата, которые эффективны лишь при сравнительно малом числе состояний. В настоящем пункте рассматривается задача описания классов неотличимых состояний конечных перестановочных автоматов [33]. Полученные результаты могут быть использованы при исследовании эквивалентности ключей в ряде криптографических устройств, которые

могут трактоваться как конечные перестановочные автоматы с большим числом состояний.

Обозначим через B_i , $i \in [1,P]$ связанные компоненты перестановочного автомата A. Известно, что отношение неотличимости автоматов является отношением эквивалентности, поэтому множество всех связанных компонент B_i , $i \in [1, P]$ автомата A разбивается на некоторое число непересекающихся классов неотличимых связных компонент автомата A. Пусть t – число классов неотличимых связанных компонент автомата A. Если A_i , $i \in [1, t]$ – подавтомат A, состоящий из некоторого класса неотличимых связанных компонент автомата A, то перестановочный автомат A можно представлять себе как автомат, состоящий из перестановочных подавтоматов A_i , $i \in [1, t]$ автомата A, все связанные компоненты которых неотличимы. Для перестановочных автоматов приводимое ниже утверждение дает возможность свести задачу определения классов неотличимых состояний к двум задачам:

1) задача определения классов неотличимых состояний перестановочного автомата, связанные компоненты которого являются неотличимыми перестановочными автоматами;

2) задача определения неотличимости или различимости связанных перестановочных автоматов.

Теорема 2. Каждый класс неотличимых состояний перестановочного автомата A является классом неотличимых состояний некоторого подавтомата A_i , $i \in [1, t]$, состоящего из одного из классов неотличимых связанных компонент автомата A, где t – число классов неотличимых связных компонент автомата A.

Доказательство. Для доказательства теоремы 2 очевидно достаточно показать, что если два состояния автомата A, принадлежащие различным связным компонентам автомата A, неотличимы, то эти компоненты неотличимы. А это утверждение немедленно следует из [16], где показано, что если автоматы B и B’ сильно связаны и различимы, то любое состояние автомата B различимо с каждым состоянием автомата B’ и из того, что сильная связанность каждой связной компоненты следует из перестановочности автомата A.

Из этой теоремы непосредственно вытекает следствие.

Следствие 1. Перестановочный автомат A является приведенным тогда и только тогда, если каждая связная компонента автомата A приведена и нет ни одной пары неотличимых связных компонент автомата A.

Замечание 1. Как следует из доказательства теоремы 2, ее утверждение и утверждение следствия 1 справедливы для более широкого класса автоматов, а именно для автоматов, состоящих из изолированных сильно связанных компонент.

Перейдем теперь к решению первой из вышепоставленных двух задач. Рассмотрим сначала связный перестановочный автомат, состоящий из одной связной компоненты.

Теорема 3. Мощности классов неотличимых состояний связного перестановочного автомата A одинаковы и равны числу

$$\text{О.Н.Д.}\left(\left|N_1^1\right|, \left|N_2^1\right|, \ldots, \left|N_{l_1}^1\right|, \left|N_1^2\right|, \ldots, \left|N_{l_2}^2\right|, \ldots, \left|N_1^{|S|-1}\right|, \ldots, \left|N_{l_{|S|-1}}^{|S|-1}\right|\right)$$

Доказательство. Рассмотрим классы неотличимых состояний $N_1, N_2, \ldots, N_l$ автомата $A = (X, S, Y, h, f)$ и предположим, что при некоторых $i, j \in [1, l]$, $|N_j| > |N|_i$.

Пусть $s_j \in N_j$ и $s_i \in N_i$. Так как автомат A сильно связан, то существует входное слово $\mathfrak{Z}$ (конечной длины), для которого

$$h_{\mathfrak{Z}}(s_j) = s_i.$$

Вследствие того, что каждое состояние из множества $h_{\mathfrak{Z}}(N_j)$ неотличимо от состояния s_i (см. [16]) и $h_{\mathfrak{Z}}$ есть подстановка множества S, заключаем

$$\left|N_i\right| \geq \left|N_j\right|,$$

что противоречит предположению $\left|N_j\right| > \left|N_i\right|$. Таким образом, первое утверждение теоремы 3 доказано. Воспользуемся теперь тем обстоятельством, что каждый класс k-неотличимых состояний есть объединение некоторых классов (k+1)-неотличимых состояний [16; 27]). Если $d = \left|N_n^{|S|-1}\right|$, $n \in [1, l_{|S|-1}]$, то получаем, что мощность каждого класса k-неотличимых состояний при $k < \left|S\right|$ есть число кратное d, откуда и следует второе утверждение теоремы 3.

Следствие 2. Если $\left|S\right|$ – простое число, то связанный перестановочный автомат $A = (X, S, Y, h, f)$, у которого не все частичные функции выхода постоянны на множестве S, является приведенным автоматом.

Доказательство. Действительно

$$|S| = \sum_{i=1}^{l} |N_i| = l \cdot d,\ d = |N_i|,\ i \in [1, l].$$

Следовательно, либо $l = 1$, либо $d = 1$. Первый случай противоречит условию следствия 2 и значит $d = 1$, то есть A приведенный автомат.

Непосредственно из теоремы 3 получаем следствие 3.

Следствие 3. Если $(|N_i^1|, |N_j^1|) = 1$ для некоторых i, j∈[1; l_1], то связанный перестановочный автомат A = (X, S, Y, h, f) является приведенным автоматом.

Для произвольного автомата A = (X, S, Y, h, f) обозначим через Π = {Π_k, k∈{1, …, L(Π)} разбиение множества S на подмножества Π_k такие, что

$$\Pi_k \cap \Pi_j = \varnothing,\ k \neq j,\ \bigcup_k \Pi_k = S$$

и для любых g∈G_A и k существует j, при котором g (Π_k)⊆Π_j. Пусть Π* – множество всех таких разбиений. Будем говорить, что Π = {Π_k, k∈{1, …, L(Π)} не меньше Π' = {Π'$_j$, j∈{1, …, L(Π')}, если для любого j найдется k такое, что Π'$_j$ ⊆ Π_k. Множество Π* частично упорядочено и более того, как показано в [40], является структурой. Обозначим через Π^β = {$\Pi^\beta{}_k$, k∈{1, …, L(Π^β)} такое разбиение Π^β∈Π*, при котором частичные функции выхода $(f_x)_{x\in X}$ автомата A постоянны на каждом множестве $\Pi^\beta{}_k$∈Π^β. В [40] показано, что разбиение множества состояний S автомата A на классы неотличимых состояний является максимальным элементом в совокупности вида Π^β. Для связного перестановочного автомата A множество Π* состоит из разбиения Π_S = {S}, разбиения Π_0 = {s, s∈S} и разбиений множества S, определяемых всеми системами областей импримитивности группы G_A [41] автомата A. Если A – неприведенный связный, перестановочный автомат, у которого не все частные функции выхода постоянны на множестве состояний S, то очевидно, что разбиение множества S на классы неотличимых состояний автомата A представляет собой максимальный элемент в совокупности разбиений, определяемых всеми системами областей импримитивности группы G_A, на которых частичные функции выхода постоянны.

В частности, имеют место следующие утверждения.

Следствие 4. Связный перестановочный автомат A = (X, S, Y, h, f), у которого не все частичные функции выхода постоянны на множестве состояний S, не является приведенным автоматом тогда и только тогда, если его частичные функции выхода постоянны на блоках некоторой системы областей импримитивности группы G автомата A.

Следствие 5. Связанный перестановочный автомат с примитивной группой, не все частичные функции выхода которого посто-

янны на множестве его состояний, является приведенный автоматом.

Алгоритм поиска систем импримитивности для групп подстановок, заданных системой образующих приведен в [36].

Пример 1. Пусть X = {0}, Y = {0,1}, S = {1, 2, 3, 4, 5, 6}, $h_0 = \begin{pmatrix} 123456 \\ 234561 \end{pmatrix}$ – подстановка S, λ – отображение S в Y, определенное равенствами:

$$\lambda(1) = \lambda(2) = \lambda(3) = 0; \lambda(4) = \lambda(5) = \lambda(6) = 1.$$

Данный автомат A = (X, S, Y, h_0, λ) является автономным связанным перестановочным автоматом Мура. На основании следствий 2, 3 сказать что-либо о существовании различных неотличимых состояний данного автомата нельзя, так как $|S| = 6$ не является простым числом и разбиение на классы 1-неотличимых состояний имеет вид:

$$N^1 = (N_1^1, N_2^1) = (\{1, 2, 3\}, \{4, 5, 6\}),$$

то

$$(|N_1^1|, |N_2^1|) = 3.$$

Поэтому воспользуемся разбиением

$$N^2 = (N_1^2, N_2^2, N_3^2, N_4^2) = (\{1, 2\}, \{3\}, \{4, 5\}, \{6\})$$

Так как

$$(|N_1^2|, |N_2^2|) = (2, 1) = 1,$$

то на основании теоремы 3 заключаем, что данный автомат не имеет различных неотличимых состояний.

Пример 2. Пусть X = {0}, S = $V_n \backslash 0$ – векторное пространство размерности n над полем из двух элементов F_2 с исключенным нулевым вектором 0, Y = F_2, h_0 – полноцикловая подстановка множества S, λ – равновероятная двоичная функция, определена на V_n. Тогда, в силу утверждения следствия 3, A = (X, S, Y, h_0, λ) является приведенным автоматом.

Пусть теперь A – произвольный перестановочный автомат, связанные компоненты которого неотличимы. Будем считать, что A состоит из T > 1 неотличимых связанных компонент B_i , $i \in [1, T]$. Согласно теореме 3 классы неотличимых состояний каждого автомата B_i , $i \in [1, T]$ имеют одинаковую мощность d_i. Описание мощностей классов неотличимых состояний рассматриваемого автомата дается приводимым ниже утверждением.

Теорема 4. Мощности классов неотличимых состояний перестановочного автомата A, состоящего из неотличимых связанных компонент B_i, $i\in[1, T]$ одинаковы и равны

$$d = \sum_{i=1}^{T} d_i,$$

где d_i – мощность классов неотличимых состояний связной компоненты B_i, $i\in[1, T]$ автомата A.

Доказательство. Пусть s – некоторое состояние автомата A. Построим класс состояний автомата A, неотличимых от s. Без ограничения общности доказательства предположим, что s принадлежит некоторому классу неотличимых состояний компоненты B(1), $s = s(1)\in {}^{B(1)}N_{s(1)}$. Компонента B(1) неотличима от компоненты B(i), $i\in[2, T]$. Следовательно, существует состояние $s(i)\in {}^{B(i)}N_{s(i)}$ компоненты B(i), $i\in[2, P]$, неотличимое от s(1). В силу транзитивности отношения неотличимости множество состояний $\bigcup_{i\in[1,\ T]} {}^{B(i)}N_{s(i)}$ является множеством состояний автомата A, неотличимых от s(1), мощности $\sum_{i=1}^{T} d_i$, так как множества ${}^{B(i)}N_{s(i)}$ принадлежат различным компонентам, и поэтому попарно не пересекаются. Остается теперь заметить, что любое состояние s автомата A, неотличимое от s_1, должно принадлежать одному из классов ${}^{B(i)}N_{s(i)}$, $i\in[1, T]$. Таким образом, утверждение теоремы 4 полностью доказано.

Прежде чем перейти к решению задачи о неотличимости связных перестановочных автоматов, сделаем одно полезное замечание и докажем ряд вспомогательных утверждений.

Замечание 2. Если классы k-неотличимых состояний автомата A_1 имеют вид ${}^{A1}N^k_i$, $i\in[1, l^{A1}{}_k]$ классы k-неотличимых состояний автомата A_2 есть ${}^{A2}N^k_i$, $i\in[1, l^{A2}{}_k]$, а s^1_i – представители классов ${}^{A1}N^k_i$, s^2_i – представители классов ${}^{A2}N^k_i$, то очевидно, что k-неотличимость автоматов A_1, A_2 индуцирует взаимно однозначное соответствие μ_k между классами разбиений ${}^{A1}N^k$ и ${}^{A2}N^k$, а именно класс ${}^{A1}N^k_i$, $i\in[1, l^{A1}{}_k]$ автомата A_1 соответствует классу ${}^{A2}N^k_j$, $j\in[1, l^{A2}{}_k]$ при соответствии μ_k тогда и только тогда, если состояние s^1_i автомата A_1 k-неотличимо от состояния s^2_j автомата A_2. В этом случае, конечно, любое состояние из ${}^{A1}N^k_i$ автомата A_1 k-неотличимо от любого состояния из ${}^{A2}N^k_j$ автомата A_2.

В силу изложенных соображений имеем

$$l^{A1}{}_k = l^{A2}{}_k,$$

если автоматы A_1 и A_2 k-неотличимы.

Теорема 5. Для неотличимости двух автоматов $A_1 = (X, S, Y, h^1, f^1)$, $A_2 = (X, S, Y, h^2, f^2)$ достаточна их $(\min(R_1,R_2)+1)$-неотличимость, где R_1 , R_2 степени различимости автоматов соответственно A_1 , A_2.

Доказательство. Пусть автоматы A_1 и A_2 m-неотличимы, $m = \min(R_1,R_2)+1$. Рассмотрим автомат A, состоящий из подавтоматов A_1 и A_2 [16]. Согласно замечанию 2 классы m-неотличимых состояний автомата A имеют вид:

$$^{A}N_t^m = {}^{A1}N^m_i \cup {}^{A2}N^m_j,\ i, j\in[1, l_m],\ l_m = l^{A1}{}_m = l^{A2}{}_m,\ t\in [1, l^A{}_m],$$

где j определяется соотношением μ_m: $^{A1}N^m_i \rightarrow {}^{A2}N^m_j$.

Теперь осталось показать, что $R_A \le m$, что, в свою очередь, следует из того, что на самом деле $R_A \le m-1$, так как, очевидно,

$$^{A1}N^m_i = {}^{A1}N_i^{m-1},\ {}^{A2}N^m_j = {}^{A2}N^{m-1}_j,\ i, j\in[1, l_m].$$

Отметим, что примеры автономных регистров сдвига, а также примеры автоматов E_n, $Д_n$ [16] показывают невозможность понижения оценки $\min(R_1,R_2)+1$, данной в теореме 5.

Теорема 6. Степени различимости неотличимых автоматов равны.

Доказательство. Предположим, что для неотличимых автоматов A_1 и A_2 $R_1>R_2$. Тогда, вследствие замечания 2, имеем

$$l^{A_1}_{R_2} = l^{A_2}_{R_2} = l^{A_2}_{R_2+i} = l^{A_2},\ i\in[0, 1, 2, \ldots).$$

Поэтому

$$l^{A_1}_{R_2+i} = l^{A_2},\ i\in[0, 1, 2, \ldots),$$

следовательно,

$$R_1 \ge R_2,$$

что противоречит предположению.

Из приведенных двух теорем вытекает следствие.

Следствие 6. Степень различимости автомата A, состоящего из неотличимых подавтоматов A_1 и A_2 равна степеням различимости автоматов A_1 и A_2.

Сейчас мы имеем все необходимое для решения вопроса неотличимости связных перестановочных автоматов.

Теорема 7. Связные перестановочные автоматы B_1 и B_2 с множествами состояний S_1 и S_2 неотличимы тогда и только тогда, если общий наибольший делитель мощностей всех классов k-неотличимых состояний $k\in[1, \max(|S_1|, |S_2|)]$ автомата A, состоящего из подавтоматов B_1 и B_2, равен $d_1 + d_2$, где d_i – мощность класса неотличимых состояний автомата B_i , $i\in[1, 2]$.

Доказательство. Пусть автоматы B_1 и B_2 неотличимы, тогда согласно теореме 4 мощность каждого класса неотличимых состояний автомата A, состоящего из неотличимых связных компонент B_1, B_2, равна $d_1 + d_2$. Из следствия 6 вытекает

$$\left| {}^{A}N_i^R \right| = d_1 + d_2 \text{ , } i \in [1,\ l_R^A],\ R = R_A = R_{B1} = R_{B2}$$

и, так как (см. теорему 1) $R_{B1} < \left| S_1 \right|$, $R_{B2} < \left| S_2 \right|$,

то

$$R \le \min (\left| S_1 \right| - 1,\ \left| S_2 \right| - 1).$$

Теперь остается заметить, что каждый класс k-неотличимых состояний автомата A есть объединение некоторых непересекающихся классов k+1-неотличимых состояний [16], откуда и следует необходимость утверждения теоремы 7. Достаточность условий этой теоремы доказывается аналогично, при этом используется утверждение теоремы 5.

Замечание 3. Утверждение теоремы 7 позволяет судить о неотличимости или различимости двух перестановочных автоматов. Действительно, как нетрудно видеть, такие автоматы неотличимы тогда и только тогда, если для любой связной компоненты первого автомата существует неотличимая от нее связная компонента второго автомата и наоборот. Таким образом, считая этот перебор компонент автоматов выполнимым, утверждение теоремы 7 решает и эту более общую задачу.

Замечание 4. Методы применения при доказательствах сформулированных теорем, позволяют решить еще одну задачу, стоящую в стороне от рассматриваемой здесь темы перестановочных автоматов, – нетрудно проверить справедливость следующего утверждения.

Два приведенных автомата A_1 и A_2 с множествами состояний S_1, S_2 неотличимы тогда и только тогда, если общий наибольший делитель мощностей классов k-неотличимых состояний $k \in [1, \max(\left| S_1 \right|, \left| S_2 \right|)]$ автомата A, состоящего из подавтоматов A_1 и A_2, равен двум.

8.3. Оценки вероятности k-неотличимости двух случайно и равновероятно выбранных состояния автомата

Пусть автомат A с множеством состояний S имеет l_k классов k–неотличимых состояний мощностей $\left| N_i^k \right|$, $i \in [1, l_k]$, $\sum_{i=1}^{l_k} |N_i^k| = \left| S \right|$.

Тогда вероятность $P^{(k)}$ того, что два случайно, независимо и равновероятно выбранных состояний из S k-неотличимы равна

$$P^{(k)} = \frac{1}{|S|^2} \sum_{i=1}^{l_k} |N_i^k|^2 .$$

Из этой формулы нетрудно вывести оценки для $p^{(k)}$, а именно

$$\frac{1}{l_k} \le P^{(k)} \le \frac{(|S|-l_k)^2 + 2|S|-l_k}{|S|^2} .$$

Выведем, например, верхнюю оценку вероятности $P^{(k)}$.

Имеем $|N_i^k| > 0$, $i \in [1, l_k]$ и

$$\sum_{i=1}^{l_k} |N_i^k|^2 \le |S|^2 ;$$

$$\sum_{i=1}^{l_k} (|N_i^k| - 1) = |S| - l_k .$$

Тогда

$$\sum_{i=1}^{l_k} (|N_i^k| - 1)^2 = (|S| - l_k)^2 ;$$

$$\sum_{i=1}^{l_k} |N_i^k|^2 - 2|S| + l_k \le (|S| - l_k)^2 ;$$

$$\sum_{i=1}^{l_k} |N_i^k|^2 \le (|S| - l_k)^2 + 2|S| - l_k ,$$ откуда и следует верхняя оценка для $P^{(k)}$.

Верхняя оценка для вероятности $P^{(k)}$ достигается, если $l_k - 1$ классов k-неотличимых состояний имеют мощность, равную единице, а один класс k-неотличимых состояний имеет мощность, равную $|S| - l_k + 1$. Нижняя оценка для $P^{(k)}$ достигается, если данный автомат имеет l_k классов k-неотличимых состояний одинаковой мощности. Формула для нахождения вероятности P того, что два случайно, независимо и равновероятно выбранных состояния автомата A неотличимы, имеет вид

$$P = \frac{1}{|S|^2} \sum_{i=1}^{l} |N_i|^2 ,$$

где N_i, $i \in [1, l]$ – мощности классов неотличимых состояний, и оценивается:

$$\frac{1}{l} \le P \le \frac{(|S|-l)^2 + 2|S|-l}{|S|^2} .$$

Оценка для P достигается при условиях, аналогичных условиям достижения $P^{(k)}$ своих оценок. Если числа l, $|N_i|$, $i \in [1, l]$ или некоторые из них для рассматриваемого автомата A неизвестны, то, очевидно, мы не имеем возможности подсчета P по приведенным выше фор-

мулам. В случае получения верхних оценок для P и $P^{(t)}$ используются неравенства:

$$P^{(k)} \geq P,\ P^{(k)} \geq P^{(t)} \text{ при } k \leq t.$$

Другая возможность оценки сверху параметра P ($P^{(k)}$) представляется при знании оценок мощностей классов неотличимых (k-неотличимых) состояний автомата справедлива.

Теорема 8. Если мощности классов k-неотличимых состояния автомата удовлетворяют неравенству

$$a \leq \left| N_i^k \right| \leq b,\ i \in [1, l_k],$$

то

$$P^{(k)} \geq \frac{1}{|S|^2}\left(\frac{|S|-l_k a}{l_k}(b-a)+2|S|a-l_k a^2\right),$$

$$P^{(k)} \leq \frac{1}{|S|^2}\left(\left(\left[\frac{|S|-l_k a}{b-a}\right]+\left(\frac{|S|-l_k a}{b-a}-\left[\frac{|S|-l_k a}{b-a}\right]\right)^2\right)(b-a)^2+2a|S|-l_k a^2\right),$$

где через $\left[\frac{|S|-l_k a}{b-a}\right]$ обозначена целая часть числа $\frac{|S|-l_k a}{b-a}$. Доказательства этой теоремы основано на следующих вспомогательных утверждениях.

Лемма 1. Пусть $0 \leq x_i \leq 1$, $i \in [1, n]$, υ – числа, удовлетворяющие условию

$$\sum_{i=1}^{n} x_i = \upsilon.$$

Тогда

$$\max_{\substack{0 \leq x_i \leq 1 \\ \sum_{i=1}^{n} x_i = \upsilon}} \sum_{i=1}^{n} x_i^2 = [\upsilon] + (\upsilon - [\upsilon])^2,$$

$$\min_{\substack{0 \leq x_i \leq 1 \\ \sum_{i=1}^{n} x_i = \upsilon}} \sum_{i=1}^{n} x_i^2 = \frac{\upsilon}{n},$$

где $[\upsilon]$ обозначает целую часть числа υ.

Следствие 7. Пусть $a \leq \eta_i \leq b$, $i \in [1, n]$, $(a < b)$ и $\sum_{i=1}^{n} \eta_i = \eta$.

Тогда

$$\max \sum_{i=1}^{n} \eta_i^2 = \left(\left[\frac{\eta - na}{b-a}\right]+\left(\frac{\eta - na}{b-a}-\left[\frac{\eta - na}{b-a}\right]\right)^2\right)(b-a)^2 + 2a\eta - na^2,$$

$$\min \sum_{i=1}^{n} \eta_i^2 = \frac{(\eta - na)(b-a)}{n} + 2a\eta - na^2.$$

Заметим, что утверждение леммы 1 можно трактовать так. В n-мерном пространстве задан n-мерный куб $0 \leq x_i \leq 1$, $i \in [1, n]$.

Проводится гиперплоскость вида $\sum_{i=1}^{n} x_i = \nu$. Пересечение n-мерного куба с данной гиперплоскостью является выпуклым многогранником в пространстве размерности n–1. Очевидно $\sum_{i=1}^{n} x_i^2$ при наших ограничениях на x_i, $i \in [1, n]$ представляет собой расстояние от точки $(x_1, x_2, \ldots, x_n)$, лежащей на этом многограннике, до начала координат. Отсюда следует, что искомый максимум есть расстояние от начала координат до максимально удаленной вершины этого многогранника, а искомый минимум есть расстояние до его ближайшей грани, доказательство же следствия 7 состоит в рассмотрении нормированных величин $\frac{\eta_i - a}{b - a}$, $i \in [1, n]$ и применении к ним леммы 1.

(Доказательство теоремы 9 (см. раздел 8.4) состоит в замене величин η_i, $i \in [1, n]$, η величинами N_i^k, $i \in [1, l_k]$, $|S|$, применении введенной выше формулы для параметра $P^{(k)}$ и использовании утверждения следствия 7.) В дальнейшем нам потребуется утверждение теоремы 9 в частном случае (a = 0), и в связи с этим мы формулируем его при a = 0 в виде следствия 8.

Следствие 8. Пусть мощности $|N_i^k|$, $i \in [1, l_k]$ классов k-неотличимых состояний автомата ограничены сверху величиной b. Тогда

$$P^{(k)} \le \frac{b^2}{|S|^2}\left([\frac{|S|}{b}] + (\frac{|S|}{b} - [\frac{|S|}{b}])^2\right),$$

где $[\frac{|S|}{b}]$ – целая часть числа $\frac{|S|}{b}$.

Для подсчета вероятностей $P^{(k)}$, P и их оценок необходимо иметь информацию о мощностях классов k-неотличимых состояний рассматриваемого автомата. Эта информация, вообще говоря, может быть полезна при анализе статистик выходных последовательностей исследуемых автоматов, а также в целом ряде других исследований, например, при исследовании эффекта сокращения периодов выходных последовательностей перестановочных автоматов.

8.4. Неотличимость состояний n-й степени перестановочного автомата

Напомним, что n-й степенью автомата A = (X, S, Y, h, f) называется автомат $A^n = (X^n, S, Y, h^n, f^n)$ с входным алфавитом X^n, множеством состояний S, выходным алфавитом Y, частичными функ-

циями переходов ($h^n_{\bar{x}}$) $\bar{x} \in X^n$ и частичными функциями выхода ($f^n_{\bar{x}}$) $\bar{x} \in X^n$ определенными соотношениями:

$$h^n_{\bar{x}} s = h_{x(n)} h_{x(n-1)} \ldots h_{x(1)} s;$$

$$f^n_{\bar{x}} s = f_{x(n)} h_{x(n-1)} \ldots h_{x(1)} s,$$

где $s \in S$, $\bar{x} = x(1), x(2), \ldots, x(n) \in X^n$.

Для определения мощностей классов неотличимых состояний перестановочного автомата A^h методами пункта 2 необходимо знать его области связности. В связи с этим определение связных компонент степеней данного автомата приобретает первостепенное значение.

Определение I0. Элементарным контуром графа Γ_A переходов автомата A называется любой его контур, не содержащий одинаковых состояний.

Очевидно, что множество различных элементарных контуров графа переходов автомата A конечно. Обозначим через $d(\Gamma_A)$ наибольший общий делитель длин элементарных контуров. Формулируемые ниже утверждения, которые нам для единообразия удобно изложить на теоретико-автоматном языке, известны из теории конечных цепей Маркова [29].

Теорема 9. Автомат A^n, представляющий собой n-ю степень сильно связного автомата A, является сильно связным автоматом тогда и только тогда, если

$$(d(\Gamma_A), n) = 1$$

Следствие 9. Все степени сильно связного автомата A сильно связны тогда и только тогда, если $d(\Gamma_A) = 1$.

Предположим теперь, что $(d(\Gamma_A), n) = d \neq 1$. Сколько же областей связности имеет автомат A^n и каковы их мощности?

Ответ на этот вопрос для связных перестановочных автоматов дает теорема 10.

Теорема 10. Пусть $A = (X, S, Y, h, f)$ – связный перестановочный автомат и $(d(\Gamma_A), n) = d$. Тогда автомат A^n имеет d – областей связности, по $\frac{|S|}{d}$ состояний в каждой из них.

8.5. Неотличимость состояний аффинных автоматов

Одним из важных в криптографических приложениях классов векторных автоматов, в котором проблема неотличимости состояний может быть полностью решена, является класс векторных аф-

финных автоматов. Через A = (X, S, Y, h, f) обозначим конечный автомат с входным алфавитом X, множеством состояний S, выходным алфавитом Y, функцией переходов h: $S\times X \to S$, и функцией выходов f: $S\times X \to Y$. Напомним, что функциям h, f соответствуют так называемые частичные функции переходов $(h_x)_{x\in X}$ и выходов $(f_x)_{x\in X}$, где $h_x s = h(s, x)$, для $s\in S$, $x\in X$, аналогично $f_x s = f(s, x)$, $s\in S$, $x\in X$. Для слова Q(j) = x(1), …, x(j) положим $h_{Q(j)} = h_{x(j)}\ldots h_{x(1)}$, $f_{Q(j)} = f_{x(j)}h_{x(j-1)}\ldots h_{x(1)}$.

Пусть $A = (X, S, Y, h, f) = (X, V_n, V_m, (\alpha_x, a_x)_{x\in X}, (c_x, d_x)_{x\in X})$ – автомат вида: $S = V_n$, $Y = V_m$, где V_n, V_m – векторные пространства размерностей n, m, соответственно, над полем Fq из q элементов; частичные функции переходов $(h_x)_{x\in X}$ и выходов $(f_x)_{x\in X}$ определены соотношениями:

$$h_x s = \alpha_x s + a_x;$$

$$f_x s = c_x s + d_x;\ s\in S;\ x\in X,$$

где α_x: $V_n\to V_n$ c_x: $V_n\to V_m$, $x\in X$ – линейные отображения или соответствующие им матрицы в некоторых фиксированных базисах пространств V_n, V_m, а $a_x\in V_n$, $d_x\in V_m$, $x\in X$. Автоматы такого вида называются аффинными автоматами. Напомним, что аффинный автомат A называется линейным, если

$$a_x = 0,\ d_x = 0,\ x\in X$$

и вполне линейным, если дополнительно

$$a_x = a,\ c_x = c,\ x\in X$$

где a: $V_n\to V_n$, c: $V_n\to V_m$ – линейные отображения.

Напомним также, что линейным автоматом, ассоциированным с аффинным автоматом A, называется автомат A_{ac} с теми же внутренним, входным и выходным алфавитами, что и у автомата A, частичные функции переходов и выхода которого ассоциированы с соответствующими частичными функциями переходов и выхода аффинного автомата A. В частности, ассоциированный с A автомат A_{ac} – линейный автомат. Несложно показывается, что при входном слове Q(j) = x(1), …,x(j) аффинного автомата A

$$h_{Q(j)}(s) = \alpha_{x(j)}\alpha_{x(j-1)}\ldots\alpha_{x(1)}s + \sum_{k=2}^{j}\alpha_{x(j)}\alpha_{x(j-1)}\ldots\alpha_{x(k)}a_{x(k-1)} + a_{x(j)};$$

$$f_{Q(j)}(s) = c_{x(j)}\alpha_{x(j-1)}\ldots\alpha_{x(1)}s + \sum_{k=2}^{j-1}c_{x(j)}\alpha_{x(j-1)}\ldots\alpha_{x(k)}a_{x(k-1)} + c_{x(j)}a_{x(j-1)} + d_{x(j)},$$

откуда следует, что состояния s и s' k-неотличимы в автомате A тогда и только тогда, если они k-неотличимы в ассоциированном с A линейном автомате A_{ac}.

Опишем мощности классов k-неотличимых состояний аффинного автомата A. Обозначим через τ_k множество всех входных слов $Q(j) = x(1), \ldots, x(j)$, $1 \le j \le k$ автомата A, а через $L(\tau_k, y(\tau_k))$ систему $|X| + |X|^2 + \ldots + |X|^k$ линейных относительно $s \in S$ уравнений

$$L(\tau_k, y(\tau_k)): c_{x(j)}\alpha_{x(j-1)}\ldots\alpha_{x(1)} = y_{x(j), x(j-1), \ldots, x(1)};$$

$$Q(j) = x(1), \ldots, x(j) \in \tau_k, y_{x(j), x(j-1), \ldots, x(1)} \in V_m.$$

Если система $L(\tau_k, y(\tau_k))$ совместна, то множество ее решений, очевидно, составляет некоторый класс k-неотличимых состояний аффинного автомата A, поэтому мощности k-неотличимых состояний аффинного автомата A равны и зависят лишь от ранга системы $L(\tau_k, y(\tau_k))$. Здесь и далее под рангом линейной системы уравнений $L(\tau_k, y(\tau_k))$ понимается ранг соответствующей ей матрицы коэффициентов.

Если линейное отображение c_x, $x \in X$ задать матрицей

$$c_i = \begin{pmatrix} c_i^1 \\ c_i^2 \\ \vdots \\ c_i^m \end{pmatrix},$$

то ранг системы $L(\tau_k, y(\tau_k))$ равен рангу следующей системы $L(\tau_k)$ векторов пространства V_n^* (V_n^* – пространство, сопряженное к V_n):

$$L(\tau_k) = (c^t_{x(j)}\alpha_{x(j-1)}\ldots\alpha_{x(1)})_{t\in[1,\ m],\ \ x(1),\ x(2),\ \ldots,\ x(j)\in\tau_k}.$$

Обозначим через $V^*(L(\tau_k))$ подпространство пространства V_n^*, натянутое на систему векторов $L(\tau_k)$. Как известно из линейной алгебры, число решений системы $L(\tau_k, y(\tau_k))$ в случае ее совместности равно $q^{n-\dim V^*(L(\tau_k))}$. Поэтому, в силу сделанного выше замечания о классах k-неотличимых состояний аффинного автомата A, имеем

$$\left|{}^A N_j^k\right| = q^{n-\dim V^*(L(\tau_k))},\ j \in [1, l_k^A]$$

где ${}^A N_j^k$ – j-й класс k-неотличимых состояний, а l_k^A число классов k-неотличимых состояний аффинного автомата A.

Следовательно, можно заключить, что

$$l_K^A = q^{\dim V^*(L(\tau_k))}.$$

Отметим некоторые свойства системы $L(\tau_k)$ и векторного пространства $V^*(L(\tau_k))$. Прежде всего, из определения этого пространства вытекает

$$V^*(L(\tau_k)) \subseteq V^*(L(\tau_{k+1})),$$

$$\dim V^*(L(\tau_k)) \le \dim V^*(L(\tau_{k+1})).$$

Кроме того, из формулы для мощностей классов k-неотличимых состояний автомата A и того, что ${}^{A}N = {}^{A}N^{|s|+1}$, получаем

$$\dim V^{*}(L(\tau_{|s|-1}))= \dim V^{*}(L(\tau_k))$$

для любых $k \geq |S|-1$, $S = V_n$. Поэтому корректно следующее определение.

Определение 8. Уровнем стабилизации ранга системы векторов $L(\tau_k)$ аффинного автомата A (или более кратко – уровнем стабилизации ранга аффинного автомата A) называется минимальное число K^A, удовлетворяющее соотношениям

$$\dim V^{*}(L(\tau_{K^A}))\leq \dim V^{*}(L(\tau_k))$$

для всех $K \geq K^A$.

Без труда устанавливается связь между уровнем стабилизации ранга аффинного автомата A и его степенью различимости, а именно

$$K^A = R_A.$$

В теореме 1 отмечалось, что степень различимости любого автомата строго меньше числа его состояний. Эта оценка в классе всех автоматов не может быть понижена [16; 27]. Для аффинных автоматов имеет место лучшая оценка.

Теорема 11. Для аффинного автомата

$$A = (X, V_n, V_m, (\alpha_x, a_x)_{x\in X}, (c_x, d_x)_{x\in X});$$

$$R_A \leq n.$$

Доказательство. Из проведенных выше исследований вытекает, что для доказательства теоремы 10 достаточно показать, что из неравенства

$$\dim V^{*}(L(\tau_k))\leq \dim V^{*}(L(\tau_{k+1}))$$

для некоторого k следует

$$\dim V^{*}(L(\tau_{k+1}))\leq \dim V^{*}(L(\tau_{k+2})).$$

Это, в свою очередь, равносильно условию: из

$${}^{A}N^{K}={}^{A}N^{K+1}$$

вытекает

$${}^{A}N^{K+1}={}^{A}N^{K+2},$$

откуда и следует утверждение теоремы I0.

Очевидно, данная оценка сверху степени различимости аффинного автомата не может быть улучшена.

Определение 9. Рангом r_A аффинного автомата A называется размерность пространства $V^{*}(L(\tau_{K^A}))$.

Учитывая формулу, выражающую мощности классов k-неотличимых состояний аффинного автомата A и тот факт, что

$K^A = R_A$, легко получить формулы, выражающие мощности классов неотличимых состояний аффинного автомата A.

Теорема 12. Для аффинного автомата $A= (X, V_n, V_m, (\alpha_x, a_x)_{x\in X}, (c_x, d_x)_{x\in X})$ мощности $|^A N_i|$ классов неотличимых состояний и их число l^A могут быть подсчитаны по формулам $|^A N_i| = q^{n-r_A}$, $l^A = q^{r_A}$.

Теорема 13. Пространство $V^*(L(\tau_{K^A}))$ есть минимальное подпространство пространства V_n^*, содержащее вектора (c_x^t) $x\in X$, $t\in[1,m]$ и инвариантное относительно линейных преобразований α_i, $x\in X$ ($c_x^t \xrightarrow{\alpha_i} c_x^t\alpha_j$).

Доказательство. Утверждение теоремы 12 непосредственно вытекает из определения системы $L(\tau_{K^A})$ и пространства $V^*(L(\tau_{K^A}))$.

Обозначим через V_0^K множество состояний $s\in V_n$, при которых выполняются равенства

$$c_{x(j)}\alpha_{x(j-1)}\ldots\alpha_{x(1)}s = 0$$

для любых слов $Q(j) = x(1), \ldots, x(j)$ из τ_k. Непосредственно проверяется, что множество V_0^K является подпространством пространства V_n и представляет собой некоторый класс k-неотличимых состояний аффинного автомата A, а $V_c^{K^A}$ является подпространством инвариантным относительно линейных преобразований $(\alpha_x)_{x\in X}$ и представляет собой некоторый класс неотличимых состояний аффинного автомата A.

Теорема 14. Классы k-неотличимых состояний аффинного автомата A есть смежные классы пространства V_n по его подпространству V_0^k.

Доказательство. Из определения пространства V_0^k непосредственно следует, что все вектора любого класса из факторпространства V_n/V_0^k неотличимы. Мощности классов k-неотличимых состояний равны $q^{n-\dim V^*(L(\tau_k))}$, в то же время любой смежный класс пространства V_n по подпространству V_0^k состоит из $q^{n-\dim V^*(L(\tau_k))}$ неотличимых состояний. Таким образом, теорема 14 полностью доказана.

Из теоремы 14 непосредственно вытекает следствие.

Следствие 10. Классы неотличимых состояний аффинного автомата A есть элементы фактор-пространства $V_n/V_0^{K^A}$.

Отметим, что для линейных автоматов $A = (X, V_n, V_m, (\alpha_x)_{x\in X}, (c_x)_{x\in X})$ с параметрами $q = 2$, $X = F_2$, $m = 1$ аналог теоремы 14 был

доказан ранее И. И. Зуевым. Кроме того, исследование классов неотличимых состояний аффинного автомата A вида: $X = V_t$ – векторное пространство размерности t над полем F_p (p – простое число), $\alpha_x = \alpha$, $c_x = C$ для всех $x \in X$, $a_x = B(x)$, $d_x = D(x)$, где $x \in V_t$, а α: $V_n \to V_n$, C: $V_n \to V_m$, B: $V_t \to V_n$, D: $V_t \to V_m$ – линейные отображения, проводилось ранее в работе [38].

Построим приведенную форму $\tilde{A} = (X, \tilde{S}, Y, \tilde{h}, \tilde{f})$ аффинного автомата $A = (X, V_n, V_m, (\alpha_x)_{x\in X}, (c_x)_{x\in X})$. Для этого необходимо определить множество состояний $\tilde{S}$ частичные функции переходов $(\tilde{h}_x)_{x\in X}$ и частичные функции выхода $(\tilde{f}_x)_{x\in X}$ автомата A. Пусть

$$\tilde{S} = V_{\tilde{n}} = V_n / V_0^{K^A};\ \tilde{n} = n - r_A;$$

$$\tilde{h}_x\ \tilde{s} = \tilde{\alpha}_x \tilde{s} + \tilde{a}_x;$$

$$\tilde{f}_x\ \tilde{s} = \tilde{c}_x \tilde{s} + \tilde{d}_x;\ x \in X;\ \tilde{s} \in \tilde{S},$$

где отображение $\tilde{\alpha}_x$: $V_{\tilde{n}} \to V_{\tilde{n}}$, $x \in X$ определено как линейное отображение $V_n / V_0^{K^A} \to V_n / V_0^{K^A}$, индуцированное линейным отображением α_x: $V_n \to V_n$ (напомним, что $V_0^{K^A}$ инвариантно относительно линейных отображений $(\alpha_x)_{x\in X}$; вектор $\tilde{a}_x$, $x \in X$ определен образом вектора a_x при естественном гомоморфизме σ: $V_n \to V_n / V_0^{K^A}$, $\tilde{\alpha}_x = \sigma(a_x)$; отображение $\tilde{c}_x$: $V_{\tilde{n}} \to V_m$, $x \in X$ определено как линейное отображение, индуцированное гомоморфизмом c_i: $V_n \to V_m$ при вложении $V_n \supset \mathrm{Ker}(c_x) \supset V_0^{K^A}$; $\tilde{d}_x = d_x$, $x \in X$.

По построению автомата $\tilde{A}$ усматривается, что он неотличим от автомата A и является приведенным аффинным автоматом. Таким образом, доказана.

Теорема 15. Приведенная форма аффинного автомата является аффинным автоматом.

8.6. Неотличимость аффинных автоматов

Согласно теореме 15 вопросы неотличимости аффинных автоматов сводятся к вопросу о неотличимости (или изоморфизму) приведенных аффинных автоматов. Пусть $A = (X, V_n, V_m, (\alpha_x, a_x)_{x\in X}, (c_x, d_x)_{x\in X})$ и $A' = (X, V'_n, V_m, (\alpha'_x, a'_x)_{x\in X}, (c'_x, d'_x)_{x\in X})$ – приведенные аффинные автоматы. Напомним, что автоматы $A = (X, S, Y, h, f)$, $A' = (X, S', Y, h', f')$ называются изоморфными, если существует взаимно однозначное отображение ψ: $S \to S'$, для которого

$$\psi h_x = h'_x \psi;$$
$$f_x = f'_x \psi;\ x \in X.$$

Будем называть изоморфизм $\psi: V_n \to V'_n$ аффинных автоматов A, A' аффинным (линейным) изоморфизмом, если отображение ψ: V_n в V_n' аффинно (линейно). Следующая теорема для аффинных автоматов уточняет известное утверждение об изоморфизме неотличимых приведенных автоматов [16].

Теорема 16. Неотличимые приведенные аффинные автоматы аффинно изоморфны.

Доказательство. Пусть приведенные аффинные автоматы $A = (X, V_n, V_m, (\alpha_x, a_x)_{x\in X}, (c_x, d_x)_{x\in X})$ и $A' = (X, V`_n, V_m, (\alpha'_x, a'_x)_{x\in X}, (c'_x, d'_x)_{x\in X})$ неотличимы, то есть для любого состояния $s \in V_n$ автомата A существует состояние $s' \in V'_n$ автомата A', для которого

$$c_{x(j)}\alpha_{i(j-1)}\ldots\alpha_{i(1)}s + \sum_{k=2}^{j-1} c_{x(j)}\alpha_{x(j-1)}\ldots\alpha_{x(k)}a_{x(k-1)} + c_{x(j)}a_{x(j-1)} + d_{x(j)} =$$
$$= c'_{x(j)}\alpha'_{x(j-1)}\ldots\alpha'_{x(1)}\,s' + \sum_{k=2}^{j-1} c'_{x(j)}\alpha'_{x(j-1)}\ldots\alpha'_{x(k)}\,a'_{x(k-1)} + c'_{x(j)}a'_{x(j-1)} + d'_{x(j)}$$

при любом входном слове $Q(j) = x(1), \ldots, x(j)$, $j \in \{1, 2, \ldots\}$ и обратно, для любого состояния $s' \in V`_n$ существует состояние $s \in V_n$, при котором выполняются предыдущие равенства. Очевидно, в наших обозначениях можно записать

$$s' = \mu(s),$$

где $\mu: V_n \to V`_n$ взаимно однозначное соответствие между $V_n$ и $V`_n$, устанавливающее изоморфизм аффинных автоматов A и A'. Обозначим сумму всех членов, начиная со второго, в левой части приведенного выше равенства через доб(Q(j)), а сумму всех членов, начиная со второго, в правой части этого равенства через доб`(Q(j)). Тогда система указанных равенств запишется в форме

$$c_{x(j)}\alpha_{x(j-1)}\ldots\alpha_{x(1)}s + \text{доб}(Q(j)) = c'_{x(j)}\alpha'_{x(j-1)}\ldots\alpha'_{x(1)}s' + \text{доб}`(Q(j)),$$
$$s' = \mu(s),\ s \in V_n,\ s' \in V`_n$$

для любых слов Q(j). Нам необходимо показать, что $\mu(s) = \psi s + a`$, где $\psi: V_n \to V`_n$ – некоторое линейное отображение, $a` \in V`_n$.

Для этого, очевидно, достаточно показать, что из условий $s'_1 = \mu(s_1)$, $s'_2 = \mu(s_2)$, $s_1, s_2 \in V_n$, $s'_1, s'_2 \in V`_n$ следует

$$\mu(s_1 + s_2) = s'_1 + s'_2 - a`$$

или, что состояние $(s_1 + s_2) \in V_n$ автомата A неотличимо от состояния $(s'_1 + s'_2 - a`) \in V`_n$ автомата A`, то есть для всех слов $Q(j) = x(1), \ldots, x(j)$:

$c_{x(j)}\alpha_{x(j-1)}\ldots\alpha_{x(1)}(s_1+s_2)+\text{доб}(Q(j)) = c'_{x(j)}\alpha'_{x(j-1)}\ldots\alpha'_{x(1)}(s'_1+s'_2-a`)+\text{доб}`(Q(j)).$

Эти равенства равносильны соотношениям

$$c_{x(j)}\alpha_{x(j-1)}\ldots\alpha_{x(1)}s_1+ c_{x(j)}\alpha_{x(j-1)}\ldots\alpha_{x(1)}s_2+ \text{доб}(Q(j)) =$$
$$= c'_{x(j)}\alpha'_{x(j-1)}\ldots \alpha'_{x(1)}s'_1+ c'_{x(j)}\alpha'_{x(j-1)}\ldots \alpha'_{x(1)}s'_2-c'_{x(j)}\alpha'_{x(j-1)}\ldots \alpha'_{x(1)}a`+$$
$$+ \text{доб}`(Q(j))$$

для всех слов Q(j) = x(1), …, x(j) или

$$c_{x(j)}\alpha_{x(j-1)}\ldots\alpha_{x(1)}s_1+c_{x(j)}\alpha_{x(j-1)}\ldots\alpha_{x(1)}s_2+\text{доб}(Q(j))+\text{доб}(Q(j))-\text{доб}(Q(j)) =$$
$$= c'_{x(j)}\alpha'_{x(j-1)}\ldots \alpha'_{x(1)}s'_1+c'_{x(j)}\alpha'_{x(j-1)}\ldots\alpha'_{x(1)}s'_2-c'_{x(j)}\alpha'_{x(j-1)}\ldots \alpha'_{x(1)}a`+$$
$$+\text{доб}`(Q(j))+\text{доб}`(Q(j))-\text{доб}`(Q(j)).$$

Эти равенства при $s'_1 = \mu(s_1)$ и $s'_2 = \mu(s_2)$ равносильны соотношению

$$\text{доб}(Q(j)) = c'_{x(j)}\alpha'_{x(j-1)}\ldots\alpha'_{x(1)}a`+\text{доб}`(Q(j)),$$

которое должно выполняться при любом слове Q(j) = x(1), …, x(j). Положив $a`=\mu(0)$, мы убеждаемся в справедливости этого соотношения при любом слове Q(j). Утверждение теоремы полностью доказано.

Следствие 11. Приведенные неотличимые линейные (вполне линейные) автоматы линейно изоморфны.

Доказательство этого утверждения аналогично доказательству теоремы 16.

8.7. Неотличимость состояний автономных векторных нелинейных автоматов

Ниже используется понятие разветвления [25] нелинейного преобразования абелевой группы, в частном случае, когда в качестве группы берется векторное пространство.

Рассмотрим векторный автономный автомат

$$A = (X, Y, h, \lambda) = (V_n, F_q, [(\alpha_{\varepsilon_1,\ \ldots,\ \varepsilon_m})_{\varepsilon_i\in F_q, i\in[1,\ m]}, (f_i)_{i\in[1,\ m]}], \lambda),$$

где $S = V_n$ – векторное пространство размерности n над полем Fq, $Y = Fq$, $\lambda = g$ – линейная функция, определенная на Vn, а функция переходов h определена равенством

$$hs = \alpha_{f_1(s),f_2(s),\ldots,f_m(s)}s,$$

где $s\in V_n$, $\alpha_{\varepsilon_1,\varepsilon_2,\ldots,\varepsilon_m}$, $\varepsilon_i \in F_q$, $i\in[1, m]$ – линейные преобразования векторного пространства V_n, $(f_i)_{i\in[1,m]}$ линейно независимые линейные функции на V_n.

Для подсчета мощностей классов k-неотличимых состояний автомата A обозначим через $d(y_1, \ldots, y_k)$ мощность(возможно и нулевую) множества состояний автомата A, дающих выход $y_1, \ldots, y_k$ за k

тактов работы автомата A. Если $d(y_1, \ldots, y_k) \neq 0$, то очевидно, что мощность класса k-неотличимых состояний автомата A, дающих выход $y_1, \ldots, y_k$, равна $d(y_1, \ldots, y_k)$.

Рассмотрим следующую систему $L(\varepsilon, y)$ линейных уравнений

$$L_1(\varepsilon)\begin{cases} f_1(s) = \varepsilon_1^1 \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots f_m(s) = \varepsilon_1^m \\ f_1(\alpha_{\varepsilon_1^1, \varepsilon_1^2, \ldots, \varepsilon_1^m} s) = \varepsilon_2^1 \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots f_m(\alpha_{\varepsilon_1^1, \varepsilon_1^2, \ldots, \varepsilon_1^m} s) = \varepsilon_2^m \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ f_1(\alpha_{\varepsilon_{k-2}^1, \varepsilon_{k-2}^2, \ldots, \varepsilon_{k-2}^m} \ldots \alpha_{\varepsilon_1^1, \ldots, \varepsilon_1^m} s) = \varepsilon_{k-1}^1 \ldots\ldots f_m(\alpha_{\varepsilon_{k-2}^1, \ldots, \varepsilon_{k-2}^m} \ldots \alpha_{\varepsilon_1^1, \ldots, \varepsilon_1^m} s) = \varepsilon_{k-1}^m \end{cases}$$

$$L_2(\varepsilon, y)\begin{cases} g(s) = y_1 \\ g(\alpha_{\varepsilon_1^1, \ldots, \varepsilon_1^m} s) = y_2 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ g(\alpha_{\varepsilon_{k-1}^1, \ldots, \varepsilon_{k-1}^m} \ldots \alpha_{\varepsilon_1^1, \ldots, \varepsilon_1^m} s) = y_k \end{cases}$$

где $\varepsilon_i^j \in F_q, i \in [1, k-1], j \in [1, m]$.

Система $L(\varepsilon, y)$ состоит из двух подсистем, которые мы обозначили через $L_1(\varepsilon)$ и $L_2(\varepsilon, y)$. Очевидно решение s системы $L(\varepsilon, y)$ принадлежит классу k-неотличимых состояний автомата A, дающих выход $y_1, \ldots, y_k$. Обратно, любое состояние автомата A, принадлежащее классу k-неотличимых состояний, дающих выход $y_1, \ldots, y_k$ есть решение системы $L(\varepsilon, y)$ при некоторых $\varepsilon_i^j \in F_q, i \in [1, k-1], j \in [1, m]$. Поэтому, обозначив через E множество всех наборов

$$\varepsilon = \begin{pmatrix} \varepsilon_1^1 & \varepsilon_1^2 & \ldots & \varepsilon_1^m \\ \varepsilon_2^1 & \varepsilon_2^2 & \ldots & \varepsilon_2^m \\ \ldots & \ldots & \ldots & \ldots \\ \varepsilon_{k-1}^1 & \varepsilon_{k-1}^2 & \ldots & \varepsilon_{k-1}^m \end{pmatrix}$$

получаем следующую формулу, выражающую число $d(y_1, \ldots, y_k)$

$$d(y_1, \ldots, y_k) = \sum_{\varepsilon \in E} \Delta(L(\varepsilon, y)) \cdot q^{n - r(L(\varepsilon, y))}$$

где $r(L(\varepsilon, y))$ – ранг системы $L(\varepsilon, y)$, а $\Delta(L(\varepsilon, y)) = 1$, если система $L(\varepsilon, y)$ совместна и $\Delta(L(\varepsilon, y)) = 0$ – в противном случае.

Воспользовавшись теперь формулой вероятности $P^{(k)}$ (см. раздел 8.3), для векторного автомата A получаем

$$P^{(k)} = \frac{1}{q^{2n}} \sum d^2(y_1, \ldots, y_k),$$

где сумма берется по всем наборам $y_1, \ldots, y_k$, $y_j \in F_q$.

Мы рассмотрим сейчас ряд условий, наложенных на системы $L_1(\varepsilon)$ и $L_2(\varepsilon, y)$, при которых все мощности $d(y_1, \ldots, y_k)$ классов k-

неотличимых состояний, дающих выход $y_1, \ldots, y_k$, одинаковы и равны числу q^{n-k}.

Условие 1. При любых наборах $\varepsilon \in E$ имеют место равенства

$$g = \eta_1, g\alpha_{\varepsilon_1^1, \ldots, \varepsilon_1^m} = \eta_2, \ldots, g\alpha_{\varepsilon_{k-1}^1, \ldots, \varepsilon_{k-1}^m} \ldots \alpha_{\varepsilon_1^1, \ldots, \varepsilon_1^m} = \eta_k,$$

где $\eta_1, \eta_2, \ldots, \eta_k$ – линейно независимые линейные функции, определенные на V_n.

Действительно, при выполнении этого условия число k-неотличимых состояний, дающих выход $y_1, \ldots, y_k$, равно числу решений системы $L_2(\varepsilon, y)$, а оно в силу линейной независимости функций $\eta_1, \eta_2, \ldots, \eta_k$ равно q^{n-k}.

Условие 2. При любом $\varepsilon \in E$ ранг системы $L(\varepsilon, y)$ линейных уравнений равен $m(k-1) + k$.

В этом случае ясно, что $\Delta(L(\varepsilon, y)) = 1$ и $r(L(\varepsilon, y)) = m(k-1) + k$ для любых наборов $\varepsilon \in E$ и $y_1, \ldots, y_k$ так, что

$$d(y_1, \ldots, y_k) = \sum_{\varepsilon \in E} q^{n-m(k-1)-k} = q^{n-k}.$$

Обозначим через $V(L_1(\varepsilon))$ векторное пространство линейных функций, натянутое на функции

$$(f_i)_{i \in [1,m]};$$

$$(f_i \alpha_{\varepsilon_1^1, \ldots, \varepsilon_1^m})_{i \in [1,m]};$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$(f_i \alpha_{\varepsilon_{k-2}^1, \ldots, \varepsilon_{k-2}^m} \ldots \alpha_{\varepsilon_1^1, \ldots, \varepsilon_1^m})_{i \in [1,m]},$$

а через $V(L_2(\varepsilon))$ – векторное пространство линейных функций, натянутое на функции

$$g, g\alpha_{\varepsilon_1^1, \ldots, \varepsilon_1^m}, \ldots, g\alpha_{\varepsilon_{k-1}^1, \ldots, \varepsilon_{k-1}^m} \ldots \alpha_{\varepsilon_1^1, \ldots, \varepsilon_1^m}.$$

Условие 3. Для любых наборов $\varepsilon \in E$

$$V(L_1(\varepsilon)) \cap V(L_2(\varepsilon)) = 0, \quad \dim V(L_2(\varepsilon)) = k.$$

Действительно, при выполнении условия 3 $\Delta(L(\varepsilon, y))$ и $r(L(\varepsilon, y))$ не зависят от значений набора $y_1, \ldots, y_k$, поэтому $d(y_1, \ldots, y_k) = d$ для любого набора $y_1, \ldots, y_k$, что возможно лишь тогда, когда

$$d = q^{n-k}.$$

При выполнении одного из условий 1, 2, 3 формула вероятности $P^{(k)}$ для автономного векторного автомата A принимает вид $P^{(k)} = \frac{1}{q^k}$ и, следовательно, в этих случаях

$$P \le \frac{1}{q^k}.$$

Глава 9. НЕОТЛИЧИМОСТЬ СОСТОЯНИЙ АВТОНОМНОГО ПОСЛЕДОВАТЕЛЬНОГО СОЕДИНЕНИЯ ПЕРЕСТАНОВОЧНЫХ АВТОМАТОВ

Дается оценка снизу числа классов неотличимых состояний и верхняя оценка их мощности автономного последовательного соединения перестановочных автоматов.

9.1. Оценки числа классов неотличимых состояний автономных последовательных соединений перестановочных автоматов

В настоящем пункте исследуется возможность использования знания общих делителей мощностей областей связности перестановочного автомата для получения оценок снизу его числа различимых состояний, то есть числа классов неотличимых состояний автомата. Пусть A – перестановочный автомат с множеством состояний S_A, а $B_i, i \in [1,t]$ – его связные компоненты с множествами состояний $S_{B_i}, i \in [1,t]$ соответственно.

В [6] показано, что мощности классов неотличимых состояний связного перестановочного автомата одинаковы. В связи с этим мощности классов неотличимых состояний каждого автомата $B_i, i \in [1,t]$ равны.

Пусть

$\left|N_{B_i}\right|$ – мощность класса неотличимых состояний автомата B_i,

$\ell_{B_i} = \dfrac{\left|S_{B_i}\right|}{\left|N_{B_i}\right|}, i \in [1,t]$ – число этих классов, при этом

$$d_A = \underset{1 \le i \le t}{НОД}\left(\left|S_{B_i}\right|\right),\ m_A = \underset{1 \le i \le t}{НОК}\left(\ell_{B_i}\right),$$

где НОД означает наибольший общий делитель, а НОК – наименьшее общее кратное соответствующих целых чисел.

Обозначим через $A_j = (B_i^j)_{i \in [1,t_j]}, j \in [1,\gamma]$ подавтомат автомата A, состоящий из j-го класса $B_1^j, \ldots, B_{t_j}^j$ неотличимых автоматов $B_i, i \in [1,t]$. Очевидно, что

$$\left|N_{A_j}\right| = \sum_{i=1}^{t_j} \left|N_{B_i^j}\right|, \quad l_{A_j} = l_{B_i^j},\ i \in [1, t_j],$$

где $\left|N_{A_j}\right|$ – мощность классов неотличимых состояний автомата A_j;

l_{A_j} – число этих классов. Имеют место следующие утверждения.

Лемма 1. Пусть $d|d_A$. Тогда $\frac{d}{(d,l_{A_j})}\Big|\left|N_{A_j}\right|$ и $\frac{d}{(\left|N_{A_j}\right|,d)}\Big|l_{A_j}$ при любом $j\in[1,\gamma]$.

Доказательство. Положим

$$\left|S_{B_i^j}\right| = d\cdot k_i^{(j)},\ i\in[1,t_j],\ j\in[1,\gamma].$$

Так как мощности классов неотличимых состояний произвольного связного перестановочного автомата одинаковы, то одинаковы эти мощности для любого связного подавтомата B автомата A. Следовательно, нетрудно доказать, что одинаковы и мощности $\left|N_{A_j}\right|$ классов неотличимых состояний произвольного автомата A_j. Поэтому имеем

$$\left|N_{A_j}\right|\cdot l_{A_j} = \sum_{i=1}^{t_j}\left|S_{B_i^j}\right| = d\cdot\sum_{i=1}^{t_j}k_i^{(j)},$$

откуда и следует утверждение леммы 1.

Лемма 2. Пусть p – простое число, $\alpha\geq 1$ – целое число, $p^{\alpha}|d_A$, $(p^{\alpha},m_A)=p^{\beta}$, $0\leq\beta<\alpha$. Тогда мощность любого класса k-неотличимых состояний (k = 1, 2, 3…) перестановочного автомата A кратна $p^{\alpha-\beta}$.

Доказательство. Так каждый класс k-неотличимых состояний автомата A представляет собой объединение некоторых классов (k+1)-неотличимых его состояний, то для доказательства леммы 2 достаточно показать, что $p^{\alpha-\beta}\Big|\left|N_{A_j}\right|$ при любом $j\in[1,\gamma]$. По лемме 1

$$\frac{p^{\alpha}}{(p^{\alpha},\ell_{A_j})}\Big|\left|N_{A_j}\right|,\ j\in[1,\gamma].$$

Заметим, что из условия $(p^{\alpha},m_A)=p^{\beta},\quad 0\leq\beta<\alpha$ вытекает

$$(p^{\alpha},\ell_{A_j})=p^{\beta_j},\ j\in[1,\gamma]$$

при некоторых $\beta_j\leq\beta$, и следовательно,

$$\frac{p^{\alpha}}{(p^{\alpha},\ell_{A_j})}=p^{\alpha-\beta_j}\Big|\left|N_{A_j}\right|,\quad j\in[1,\gamma].$$

Но тогда и тем более $p^{\alpha-\beta_j}\Big|\left|N_{A_j}\right|,\quad j\in[1,\gamma]$, что и требовалось показать.

Из леммы 2 непосредственно вытекают такие утверждения.

Следствие 1. Пусть $(p_i)_{i\in[1,n]}$ – простые числа, $(\alpha_i)_{i\in[1,n]}$ – целые положительные числа, $p_1^{\alpha_1}p_2^{\alpha_2}...p_n^{\alpha_n} \mid d_A$ и $(p_1^{\alpha_1}\dots p_n^{\alpha_n}, m_A) = p_1^{\beta_1}\dots p_1^{\beta_n}, \beta_i \geq 0, i \in [1,n].$

Тогда мощность любого класса k-неотличимых состояний (k = 1, 2, …) перестановочного автомата A кратна числу $p_1^{\alpha_1-\beta_1}...p_n^{\alpha_n-\beta_n}$.

Следствие 2. Пусть наибольший общий делитель мощностей некоторых классов k-неотличимых состояний перестановочного автомата A равен единице и $d|d_A$. Тогда $d|m_A$.

Лемма 3. Пусть p – простое число, α > 0 – целое число и $p^{\alpha} \mid d_A, p^{\alpha+1} > |S_A|$. Тогда при любом $j \in [1,\gamma]$

$$(p^{\alpha}, \ell_{A_j}) = \frac{p^{\alpha}}{\left(p^{\alpha}, \left|N_{A_j}\right|\right)}.$$

Доказательство. Как при доказательстве леммы 1 имеем

$$\left|N_{A_j}\right| \cdot \ell_{A_j} = p^{\alpha}\sum_{i=1}^{t_j} k_i^{(j)},$$

причем $p > \sum_{i=1}^{t_j} k_i^{(j)}$, так как $p > \frac{|S_A|}{p^{\alpha}} = \sum_{\substack{i\in[1,t_j]\\ j\in[1,\gamma]}} k_i^{(j)}.$

Следовательно,

$$\left(\left(p^{\alpha}, \left|N_{A_j}\right|\right) = p^{\beta_j}\right)$$

тогда и только тогда, когда

$$\left(\left(p^{\alpha}, \ell_{A_j}\right) = p^{\alpha-\beta_j}\right).$$

Лемма 4. Пусть p – простое число, α > 0 – целое число, а $p^{\alpha} \mid d_A$, $p^{\alpha+1} > |S_A|$. Тогда

$$\left(D_A, p^{\alpha}\right) = \frac{p^{\alpha}}{(m_A, p^{\alpha})},$$

где D_A – общий наибольший делитель мощностей классов k-неотличимых состояний перестановочного автомата A, $k \in [1, |S_A| - 1]$.

Доказательство. Легко заметить, что

$$D_A = \underset{j\in[1,\gamma]}{Н.О.Д}\left(\left|N_{A_j}\right|\right), \text{ а}$$

$$\left(m_A, p^{\alpha}\right) = p^{\alpha - \min\limits_{j\in[1,\gamma]}(\beta_j)} \text{ и } \left(d_A, p^{\alpha}\right) = p^{\min\limits_{j\in[1,\gamma]}(\beta_j)},$$

где $p^{\beta_j} = \left(p^{\alpha}, \left|N_{A_j}\right|\right), j \in [1,\gamma]$. Требуемое утверждение теперь непосредственно следует из леммы 3.

Проведенные исследования позволяют находить некоторые делители параметра m_A перестановочного автомата A. Приводимое ниже утверждение позволяет с их помощью оценивать снизу число классов l_A неотличимых состояний перестановочного автомата A.

Лемма 5. Пусть $d | m_A$. Тогда

$$\ell_A \geq \sum_{i=1}^{n} p_i^{\alpha_i},$$

где $d = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_n^{\alpha_n}$ – каноническое разложение числа d на простые множители.

В качестве примеров приложения сформулированных утверждений ниже рассматриваются два типа последовательного соединения перестановочных автоматов.

Пусть A` = (S`, Y`, h`, λ`) приведенный, связный, перестановочный, автономный автомат (иногда говорят полноцикловый автомат) с множеством состояний S′, |S′| > 1, выходным алфавитом Y′, |Y′| > 1, функцией перехода h′ и функцией выхода λ′, а A`` = (X``, S``, Y``, $(h_x)_{x \in X``}$, $(f_x)_{x \in X``}$), Y` = X`` – перестановочный автомат с частичными функциями переходов $(h_x)_{x \in X``}$ и частичными функциями выхода $(f_x)_{x \in X``}$.

Напомним, что последовательным соединением автоматов A′, A″ называется автономный автомат $A` \to A`` = \left(S' \times S'', Y``, h^{A' \to A''}, \lambda^{A' \to A''}\right)$ с множеством состояний $S' \times S''$, выходным алфавитом Y″, функциями переходов $h^{A' \to A''}$ и выхода $\lambda^{A' \to A''}$, определенными соотношениями:

$$h^{A' \to A''}(s', s'') = \left(h`(s'), h``_{\lambda'(s')}(s'')\right),$$

$$\lambda^{A' \to A''}(s', s'') = f``_{\lambda'(s')}(s''), \quad s' \in S', s'' \in S''.$$

Такое последовательное соединение автономного автомата A′ с автоматом A″ мы будем называть в дальнейшем *автономным последовательным соединением автоматов* A′, A″. Обозначим через $A`[\to]A``$ и назовем *обобщенным автономным последовательным соединением автоматов* A′ и A″ автономный автомат, отличающийся от автомата $A` \to A``$ функцией выхода, которая может быть задана любым отображением

$$S' \times S'' \to Y,$$

где Y – некоторый алфавит. В такой терминологии, очевидно, последовательное соединение является и обобщенным последовательным соединением, но не наоборот. Очевидно, построенный автомат $A = A'[\to]A''$ является перестановочным автономным автоматом, мощности областей связности (длины циклов) которого кратны чис-

лу |S′|. Обозначим через $W_A(s',s'')$ период выходной последовательности A(s`, s``), соответствующей начальному состоянию $(s',s'')\in S'\times S''$ автомата A. Положим $W_A = \underset{(s',s'')\in S'\times S''}{H.O.K.}\left(W_A(s',s'')\right)$. Последняя величина называется *периодом внешнего функционирования автомата* A. Заметим, что период $W_A$(s`, s``) последовательности A(s`, s``) совпадает с числом классов неотличимых состояний связной компоненты автомата A, содержащей состояние (s',s''), в связи с чем можно заключить

$$W_A = m_A.$$

Таким образом, при формулировке приведенных в этом пункте утверждений для класса обобщенных автономных последовательных соединений автоматов рассматриваемого вида $A = A'[\rightarrow]A''$ достаточно положить $d = |S'|$ и $W_A = m_A$.

Рассмотрим теперь несколько детальнее последовательное соединение A = A`→A`` автоматов A′ и A″. Обозначим через A(s`) выходную последовательность автомата A` = (S`, Y`, h`, λ`), соответствующую его начальному состоянию $s'\in S'$, а через $W_{A`}(s')$ – ее период. Очевидно, что

$$W_{A`}(s') = |S`|$$

при любом $s'\in S'$, так как A′ – связный, перестановочный, приведенный, автономный автомат. Кроме того, выходная последовательность (A`→A``)(s`, s``) совпадает с выходной последовательностью A``(s``, A`(s`)) автомата A″, соответствующей входной последовательности A`(s`) и начальному состоянию *s″* автомата A″. Отсюда легко вывести, что период $W_{A'\rightarrow A''}$ внешнего функционирования автомата A=A`→A`` совпадает с *периодом внешнего функционирования* $W_{A``}(J)$ *неавтономного автомата A″ при входной периодической последовательности* $J = A`(s')$, то есть

$$W_{A'\rightarrow A''} = W_{A``}\left(A`(s`)\right)$$

при любом $s'\in S'$. Это замечание для автономных последовательных соединений A`→A`` автоматов A′, A″ открывает новый путь нахождения оценок их числа классов неотличимых состояний, заключающийся в предварительном нахождении делителей периода внешнего функционирования $W_{A``}(J)$ перестановочного автомата A`` = (X``, S``, Y``, $(h_x)_{x\in X``}$, $(f_x)_{x\in X``}$) при его входной последовательности $J = A`(s')$, s`∈S` и использования затем утверждения леммы 5.

Исследованию этого подхода и посвящается оставшаяся часть настоящего пункта.

Пусть J = x(1), x(2), …, x(m+1), – входная последовательность периода ω(J) некоторого перестановочного автомата A = (X, S, Y, $(h_x)_{x\in X}$, $(f_x)_{x\in X}$). Будем называть ее мультиграммы $J^{(k)}$ = x(k), x(k+1), … и $J^{(k`)}$ = x(k`), x(k`+1), … сравнимыми мультиграммами, если они имеют одинаковую длину (как конечную, так и бесконечную). Обозначим через ${}^{A}N_{y}^{J^{(k)}}$ множество решений системы уравнений A(s, $J^{(k)}$) = $y_1, y_2, \ldots, y_{m+1}, \ldots$

$$f_{x(k)}(s) = y_1$$
$$f_{x(k+1)}h_{x(k)}(s) = y_2$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$
$$f_{x(k+j)}h_{x(k+j-1)}\ldots h_{x(k)}(s) = y_{m+1}$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

относительно неизвестного $s\in S$.

Теорема 1. Пусть J = x(1), x(2), …, x(m+1), … – входная последовательность периода ω(J) некоторого перестановочного автомата A = (X, S, Y, $(h_x)_{x\in X}$, $(f_x)_{x\in X}$), содержащая сравнимые мультиграммы $J^{(k)}, J^{(k')}$. Тогда при каждом наборе $y = y_1, y_2, \ldots, y_{m+1}, \ldots, y_m \in Y^m$

$$\left|{}^{A}N_{y}^{J^{(k)}}\right| = \left|{}^{A}N_{y}^{J^{(k')}}\right|$$

при $k \equiv k' \bmod(\omega(j), W_A(J))$.

Доказательство. Покажем, что при выполнении условий теоремы 1 для k и k' существует взаимно однозначное соответствие между решениями системы уравнений

1) A(s, $J^{(k)}$) = $y_1, y_2, \ldots, y_{m+1}, \ldots$

и решениями системы уравнений

2) A(s, $J^{(k`)}$) = $y_1, y_2, \ldots, y_{m+1}, \ldots$.

В силу симметрии достаточно найти взаимно однозначное отображение $\psi : S \to S$ такое, что если $s_0 \in S$ является решением системы 1), то $\psi(s_0)$ будет решением системы 2). Итак, пусть, например, $k > k'$ и $s_0 \in S$ является решением системы 1), то есть

$$y = y_1, y_2, \ldots, y_{m+1}, \ldots = A(s_0, J^{(k)}) = A(s_0, J^{(k`+(k-k`))}).$$

Из условия $k \equiv k' \bmod(\omega(J), W_A(J))$ вытекает существование натуральных чисел n_1, n_2, при которых

$$n_1\omega(J) + (k - k') = n_2 W_A(J).$$

Следовательно,

$$y = A(s_0, J^{(k'+(k-k'))}) = A(s_0, J^{(k'+(k-k')+n_1\omega(J))}) =$$
$$= A(s_0, J^{(k'+n_2 W_A(J))}) = A((h_{x(k'-1+n_2 W_A(J))} \ldots h_{x(k')})^{-1} s_0, J^{(k')})\text{,}$$

так как период последовательности $A(s_0, J^{(k'+n_2 W_A(J))})$ является делителем периода $W_A(J)$. Положим $\psi \equiv (h_{x(k'-1+n_2 W_A(J))} \ldots h_{x(k')})^{-1}$. Очевидно ψ, в силу перестановочности автомата A, является взаимно однозначным отображением S в S, причем $A(\psi(s_0), J^{(k')}) = y$. Таким образом, теорема полностью доказана.

Назовем входные слова J, J`$\in X^k$ автомата A вероятностно неотличимыми относительно A, если для любого y$\in Y^k$ при случайном и равновероятном выборе начального состояния s$\in$S вероятности P(A(s, J) = y), P(A(s, J`) = y) событий A(s, J) = y и A(s, J`) = y совпадают.

Из утверждения теоремы 1 вытекает равносильное ему следующее важное

Следствие 3. Пусть J = x(1), x(2), …, x(m+1), … – входная последовательность периода ω(J) некоторого перестановочного автомата A = (X, S, Y, $(h_x)_{x\in X}$, $(f_x)_{x\in X}$). Тогда любые ее сравнимые мультиграммы $J^{(k)}, J^{(k')}$; $k \equiv k' \bmod(\omega(J), W_A(J))$ вероятностно неотличимы относительно автомата *A*.

Следует отметить, что приведенное выше утверждение представляет собой лишь обобщение аналогичного утверждения, доказанного В. А. Башевым другим способом для перестановочных автоматов Мура в случае $(\omega(J), \omega_A^{ext}(J)) = 1$. Для неперестановочных автоматов имеет место более слабое утверждение.

Назовем входные слова автомата A J, J`$\in X^k$ *A-неотличимыми*, если для любого y$\in Y^k$ при случайном и равновероятном выборе начального состояния s$\in$S

P(A(s, J) = y) · P(A(s, J`) = y) ≠ 0 либо P(A(s, J) = y) = P(A(s, J`) = y) = 0.

Теорема 2. Пусть J = x(1), x(2), …, x(m+1), … – входная последовательность периода ω(J) автомата A = (X, S, Y, $(h_x)_{x\in X}$, $(f_x)_{x\in X}$), при которой все последовательности $\{A(s,J),\ s \in S\}$ являются периодическими (чисто периодическими). Тогда любые ее сравнимые мультиграммы $J^{(k)}, J^{(k')}$; $k \equiv k' \bmod(\omega(J), W_A(J))$ последовательности *J* являются *A*-неотличимыми.

Доказательство этого утверждения во многом подобно доказательству теоремы 1.

Существенным же отличием является лишь момент рассмотрения равенства

$$y = A(s_0, J^{(k)}) = A(s_0, J^{(k'+n_2 W_A(J))}).$$

Оно может быть продолжено так:

$$A(s_0, J^{(k)}) = A(s', J^{(k'+n_2 W_A(J)+n_3 W_A(J))}),$$

где s' – некоторое состояние из S. Заметим, что n_3 может быть выбрано так, что $\omega(J) \mid n_2 + n_3$. При таком n_3 последнее равенство, которое можно записать в виде

$$A\left(s_0, J^{(k)}\right) = A\left(s', J^{(k')}\right),$$

которое, в силу естественной симметрии выбора $J^{(k)}, J^{(k')}$, и доказывает теорему 2.

Обозначим через θ(J) и назовем полнотой последовательности J элементов алфавита X максимальное k, если оно существует, при котором все возможные k-граммы алфавита X встречаются в последовательности J. Без ограничения общности будем считать, что рассматриваемые нами входные периодические последовательности J автомата A имеют полноту θ(J)≥1.

Обозначим через Q_A и назовем степенью вероятностной неотличимости автомата A максимальное k, если оно существует, при котором любая пара слов из X^k вероятностно неотличима относительно A, в противном случае полагаем $Q_A = \infty$.

Используя теорему 2, получаем следствие 4.

Следствие 4. Пусть J = x(1), x(2), …, x(m+1), … – входная последовательность перестановочного автомата $A = (X, S, Y, (h_x)_{x\in X}, (f_x)_{x\in X})$ периода ω(J) и полноты θ(J) > Q_A. Тогда $(\omega(j), \omega_A^{ext}(j)) \neq 1$.

Легко видеть, что в случае k-автономного автомата A условие θ(J) > Q_A приведенного выше следствия можно заменить на более слабое θ(J) > Q_A–k.

Очевидно, утверждения теоремы 1 и следствий 3, 4 наиболее эффективно могут быть использованы, если ω(J) – простое число. Тем самым и их приложения к рассматриваемому нами автономному соединению $A' \to A''$ приведенного связного перестановочного автономного автомата $A' = (S', Y, h`, \lambda')$ с перестановочным автоматом $A'' = (X``, S``, Y``, (h``_i)_{i\in I''}, (f``_i)_{i\in I''})$, $Y` = X``$ наиболее эффективно, если $|S'|$ – простое число. Этим случаем мы и ограничиваемся в проводимом ниже исследовании автомата $A = A' \to A''$.

Ранее для перестановочного автомата A с множеством состояний S и известным общим делителем $p^{\alpha}, p^{\alpha+1} > |S|$ мощностей областей его связности, были даны необходимые и достаточные условия, при которых $\left(p^{\alpha}, m_A\right) = p^{\alpha-\beta}, \beta \geq 0$. Основываясь на этих условиях, мы приводим их уточнения для рассматриваемого нами здесь автомата $A' \to A''$.

Следствие 5. Пусть $|S'|$ – простое число и $|S'| > |S''|$. Тогда следующие условия эквивалентны:

1) $\left(W_{A' \to A''}, |S'|\right) = 1$;

2) для каждого y $\left|{}^{A''}N_y^{J^{(k)}}\right| = \left|{}^{A''}N_y^{J^{(k')}}\right|$

при любых сравнимых мультиграммах $J^{(k)}, J^{(k')}$ выходной последовательности $J = A`(s'),\ s' \in S'$ автомата A'.

Доказательство. Так как $W_{A' \to A''} = W_{A'}(J)$, то, пользуясь теоремой 1, заключаем, что условие 1) влечет выполнение условия 2). Предположим теперь, что для автомата A'' выполнено условие 2). Очевидно, мощность класса k-неотличимых состояний автомата $A' \to A''$, дающих выход $y_1, y_2, \ldots, y_k$, может быть подсчитана по формуле:

$$\left|{}^{A' \to A''}N_{y_1 \ldots y_k}\right| = \sum \left|{}^{A'}N_{x(1)\ldots x(k)}\right| \cdot \left|{}^{A''}N_{y_1 \ldots y_k}^{x(1)\ldots x(k)}\right|,$$

где сумма взята по всем различным k-граммам выходной последовательности $J = A`(s'),\ s' \in S'$ автомата A', а $\left|{}^{A'}N_{x(1)\ldots x(k)}\right|$ – мощность класса k-неотличимых состояний автомата A', дающих выход $x(1), \ldots, x(k)$; $\left|{}^{A''}N_{y_1 \ldots y_k}^{x(1)\ldots x(k)}\right|$ – как обычно, мощность множества состояний $N_y^{J(k)}$ при $J(k) = x(1), \ldots, x(k),\ y = y_1, \ldots, y_k$. Учитывая независимость чисел $\left|{}^{A''}N_{y_1 \ldots y_k}^{x(1)\ldots x(k)}\right|$ от k-грамм $x(1), \ldots, x(k)$ выходной последовательности $J = A`(s')$ автомата A' и то, что

$$\sum \left|{}^{A'}N_{x(1)\ldots x(k)}\right| = |S'|,$$

последнее равенство можно переписать в виде

$$\left|{}^{A' \to A''}N_{y_1 \ldots y_k}\right| = |S'| \cdot \left|N_{y_1 \ldots y_k}\right|,$$

где $\left|N_{y_1 \ldots y_k}\right| = \left|{}^{A''}N_{y_1 \ldots y_k}^{x(1)\ldots x(k)}\right|$. Таким образом, мощность любого класса k-неотличимых состояний автомата $A' \to A''$ кратна $|S'|$. Следовательно, по лемме 4 можно заключить, что $\left(W_{A' \to A''}, |S'|\right) = 1$.

В ряде случаев можно указать еще более простые условия, гарантирующие справедливость оценки снизу $|S'|$ числа классов неотличимых состояний автомата $A' \to A''$. Приведем эти случаи.

Для удобства предположим, что $|Y``|>1$. Обозначим через θ(A`(s`)) полноту выходной последовательности $A`(s'),\ s'\in S'$ автомата A`. Так как A` – полноцикловый автомат, то параметр θ(A`(s`)) не зависит от выбора s`∈ S`.

Используя следствие 4, легко доказываются следующие теоремы.

Теорема 3. Пусть $|S'|$ – простое число, θ(A`(s`)) > $Q_{A``}$. Тогда число классов неотличимых состояний автономного последовательного соединения $A'\to A''$ ограничено снизу величиной $|S'|$, период $W_{A`\to A``}$ внешнего функционирования автомата $A'\to A''$ кратен $|S'|$.

Теорема 4. Пусть $|S'|$ – простое число, $A''=\left(X``,V_n,F_q,(h_x)_{x\in X``},(f_x)_{x\in X``}\right)$ – векторный перестановочный неавтономный автомат и q^n < θ(A`(s`)). Тогда число классов неотличимых состояний автомата $A'\to A''$ ограничено снизу величиной $|S'|$, а его период внешнего функционирования кратен $|S'|$.

Теорема 5. Пусть $|S'|$ – простое число, $A''=\left(X``,V_n,F_q,(\alpha_x)_{x\in X``},(c_x)_{x\in X``}\right)$ – векторный линейный перестановочный неавтономный автомат и n < θ(A`(s`)). Тогда число классов неотличимых состояний автомата $A'\to A''$ ограничено снизу величиной $|S'|$, а его период внешнего функционирования кратен $|S'|$.

Для произвольного векторного автомата

$$A=\left(X,V_n,F_q,(h_x)_{x\in X},(f_x)_{x\in X}\right)$$

обозначим через H_A минимальное k, при котором найдется входное слово x(1), x(2), …, x(k) автомата A и некоторая функция Φ $F_q^{k-1}\to F_q$, для которых

$$f_{x(k)}h_{x(k-1)}\ldots h_{x(1)}=\Phi(f_{x(1)},\ f_{x(2)}h_{x(1)},\ \ldots,\ f_{x(k-1)}h_{x(k-1)}\ldots h_{x(1)}).$$

Для векторного автомата $A=\left(X,V_n,F_q,(h_x)_{x\in X},(f_x)_{x\in X}\right)$, исходя из определений параметров H_A, Q_A несложно доказывается неравенство

$$Q_A < H_A.$$

Напомним, что автомат A называется k-автономным, если при любом его начальном состоянии выходная последовательность длины k не зависит от входного слова длины k. В этом смысле любой автомат Мура является 1-автономным автоматом. Автомат называют автономным, если он k-автономен при любом k.

Заметим, что для k-автономных автоматов A из условий $\left(\omega(J), W_A(J)\right)=1,\ \theta(J)\geq H_A-k$ вытекает автономность векторного автомата A. Это утверждение является обобщением доказанного ранее В. А. Башевым утверждения, состоящего в том, что для входной последовательности J периода $\omega(J)$ и полноты θ(J) векторного линейного перестановочного автомата Мура $A''=\left(X``, V_n, F_q, (\alpha_x)_{x\in X``}, \lambda\right)$ из условий $\left(\omega(J), W_{A''}(J)\right)=1,\ \theta(J)\geq H_{A''}-1$ вытекает автономность автомата A''.

9.2. Оценки мощностей классов неотличимых состояний автономных последовательных соединений перестановочных автоматов

В предыдущем пункте мы нашли оценки снизу числа классов неотличимых состояний автономных последовательных соединений перестановочных автоматов типов A′[→]A″ и A′→A″, причем для последнего типа автономного последовательного соединения были использованы два подхода к нахождению этих оценок. Первый заключался в подсчете и сравнении мощностей классов – неотличимых состояний, второй – в подсчете и сравнении условных вероятностей появления выходных слов или же в проверке неавтономности заданного автомата. Обсуждаемая в данном пункте задача оценки мощностей классов неотличимых состояний автономного последовательного соединения A′→A″ оказывается по своей природе несколько сложней. Это может быть частично объяснено тем, что вопросы оценок мощностей классов неотличимых состояний автомата A′→A″ оказываются тесно связанными с вопросами оценок периодов индивидуальных выходных последовательностей автомата A′→A″, в то время как исследованные ранее оценки числа классов неотличимых состояний автомата A′→A″ были связаны с задачей оценки его периода внешнего функционирования.

Пусть, как и ранее, A′ = (S′, Y′, h′, λ′), |S′| > 1, |Y′| > 1 – некоторый приведенный связный перестановочный автономный автомат, а A″ = (X″, S″, Y″, $(h''_x)_{x\in X''}$, $(f_x)_{x\in X''}$), X″ = Y′. Рассмотрим последовательное соединение A′→A″ автоматов A′, A″.

Как было показано при доказательстве следствия 5, мощность $|^{A'\to A''}N_{y_1,\ \ldots,\ y_k}|$ класса k-неотличимых состояний автомата A′→A″, дающих выход $y_1, \ldots, y_k$, выражается формулой

$$|^{A'\to A''}N_{y_1,\ldots,y_k}| = \sum |^{A'}N_{x(1),\ldots,x(k)}| \cdot |^{A``}N^{x(1),\ldots,x(k)}_{y_1,\ldots,y_k}|,$$

где сумма берется по всем различным k-граммам (x(1), …, x(k))-выходной последовательности A`(s′), s′∈S′ автомата A′, а $|^{A'}N_{x(1),\ldots,x(k)}|$ – мощность класса k-неотличимых состояний автомата A`, дающих выход x(1), …, x(k); $|^{A``}N^{x(1),\ldots,x(k)}_{y_1,\ldots,y_k}|$ – число состояний автомата A″, дающих выход y_1, …, y_k при входной последовательности x(1), …, x(k). Очевидно, что при достаточно больших k (например, k > |S′| · |S″| – 1) приведенная формула выражает мощность некоторого класса неотличимых состояний автомата A′→A″. Естественно, на наш взгляд, подходить к исследованию верхних оценок числа $|^{A'\to A''}N_{y_1,\ldots,y_k}|$ посредством предварительных оценок величин $|^{A'}N_{i(1),\ldots,i(k)}|$, $|^{A``}N^{x(1),\ldots,x(k)}_{y_1,\ldots,y_k}|$ и числа ненулевых слагаемых в приведенной выше сумме.

Теорема 6. Если выходная последовательность A`(s′) автомата A′ содержит диагностическую (относительно автомата A″) мультиграмму, то мощности классов неотличимых состояний автомата A′→A″ ограничены сверху величиной |S′|.

Доказательство. Имеем

$$|^{A'\to A''}N_{y_1,\ldots,y_k}| = \sum |^{A'}N_{x(1),\ldots,x(k)}| \cdot |^{A``}N^{x(1),\ldots,x(k)}_{y_1,\ldots,y_k}|.$$

При достаточно большом k

$$|^{A``}N^{x(1),\ldots,x(k)}_{y_1,\ldots,y_k}| \le 1,$$

так как автомат A″ – перестановочный, а его входная последовательность A`(s′) содержит диагностическую мультиграмму. Поэтому

$$|^{A'(\to)A''}N_{y_1,\ldots,y_k}| \le \sum |^{A'}N_{x(1),\ldots,x(k)}| = |S'|$$

при достаточно большом k. Теорема 6 полностью доказана.

Аналогичным образом доказываются приводимые ниже теорема 7 и следствие 6.

Теорема 7. Если выходная последовательность автомата A′ содержит диагностическую мультиграмму для A″ и θ = θ(A`(s`) > $\sigma_{A''}$, то мощности классов неотличимых состояний автомата A′→A″ ограничены сверху величиной

$$|S'| - \min_{x(1),\ldots,x(\theta)} |^{A'}N_{x(1),\ldots,x(\theta)}|.$$

Будем говорить, что множество входных слов $\mathfrak{I}_1$, …, $\mathfrak{I}_t$ одинаковой длины автомата A *сильно различимо (относительно A),* если при любой правой части **y** система уравнений A(s, $\mathfrak{I}_j$) = **y**, j∈{1, …, t} не имеет решения в множестве начальных состояний автомата A. В противном случае данное множество входных слов автомата A

называется *слабо неотличимым* множеством (относительно A). Максимальное k, если таковое существует, при котором все k-граммы входного алфавита автомата A слабо неотличимы, обозначим через σ_A и назовем степенью слабой автономности автомата A. В противном случае полагаем $\sigma_A = \infty$.

Обозначим через [ν] целую часть числа ν.

Лемма 6. Пусть J = x(1), x(2), … – входная последовательность автомата A периода ω(J), содержащая пару сильно различимых мультиграмм. Тогда любое множество из $t > [\frac{\omega(J)}{2}]$ различных мультиграмм $\{J^{k_j} = x(k_j), x(k_j+1), \ldots, j \in [1, t]\}$ – сильно различимо.

Доказательство. Пусть $J^{(k)} = x(k), x(k+1), \ldots$; $J^{(k')} = x(k'), x(k'+1), \ldots$ – пара сильно различимых мультиграмм последовательности J = x(1), x(2), … . Тогда при любом j пары $J^{(k+j)}$, $J^{(k'+j)}$ также сильно различимы. Отсюда, в силу элементарных соображений, и вытекает утверждение леммы 6.

Следствие 6. Если выходная последовательность автомата A′ содержит диагностическую пару мультиграмм и пару сильно различимых мультиграмм относительно автомата A″, то мощности классов неотличимых состояний автомата A′→A″ ограничены сверху величиной $[\frac{|S'|}{2}]$.

Под периодом W(A(s, J)) выходной последовательности произвольного автомата A будем понимать период смешанно периодической последовательности A(s, J). Справедлива теорема 8.

Теорема 8. Пусть J = x(0), x(1), x(2), … – входная последовательность периода ω(J) автомата $A = (X, S, Y, (h_x)_{x \in X}, (f_x)_{x \in X})$. Тогда множество сравнимых мультиграмм вида

$$J^{(kd)} = x(kd), x(kd+1), \ldots, k \in \{0, 1, 2, \ldots\}, J^{(0)} = J,$$

$$d = (\omega(J), W(A(s, J))$$

слабо неотличимо относительно связной компоненты A_s автомата A, содержащей состояние $s \in S$.

Доказательство. Для произвольного состояния s_0 автомата A рассмотрим выходную (вообще говоря, смешанно периодическую) последовательность $A(s_0, J) = y_0, y_1, \ldots$ и последовательность состояний $A_M(s_0, J) = s_0, s_1, \ldots$, отвечающую входной последовательности J = x(0), x(1), x(2), … периода ω(J) и начальному состоянию s_0. Легко видеть, что существует t, при котором последовательность $A(s_t, J) = y_t, y_{t+1}, \ldots$ – чисто периодическая.

При этом, очевидно, связная компонента A_{s_0} содержит в качестве подавтомата связную компоненту A_{s_t}. Положим для краткости $s_t = s$, $\omega(J) = \omega$, $W(A(s_t, J)) = W$. При $(\omega, W^t) = \omega$ утверждение теоремы 8 очевидно. Предположим, что $(\omega, W) = d \neq \omega$. Существуют натуральные числа n_1, n_2, при которых $n_1\omega - n_2W = kd$, где k – некоторое фиксированное число, $k \in [1, \frac{\omega}{d}]$. Имеем

$$A(s, J) = A(s, J^{(\omega)}) = A(s, J^{(kd-kd)}) = \mathrm{Ext}_A(s, J^{(kd-n_1\omega+n_2W)}) = A(s, J^{(kd+n_2W)}).$$

Выберем натуральное число n_3 так, чтобы $\omega | n_2+n_3$, и продолжим равенства следующим образом:

$$A(s, J^{(kd+n_2W)}) = A(h_{x(kd+n_2W+n_3W-1)}\ldots h_{x(kd+n_2W)}s, J^{(kd+n_2W+n_3W)}) =$$
$$= A(h_{x(kd+n_2W+n_3W-1)}\ldots h_{x(kd+n_2W)}s, J^{(kd)}),$$

так как $\omega(J^{(kd+(n_2+n_3)W)}) = \omega$. Очевидно, что состояние

$$s(kd) = h_{x(kd+(n_2+n_3)W-1)}\ldots h_{x(kd+n_2W)}s$$

принадлежит связной компоненте A_s автомата A. Таким образом, показано существование состояний s, s(d), …, $s(\frac{\omega}{d}-1)$ связной компоненты A_s автомата A, при которых

$$A(s, J) = A(s(d), J^{(d)}) = \ldots = A(s(\frac{\omega}{d}-1), J^{((\frac{\omega}{d}-1)d)}),$$

что и доказывает утверждение теоремы 8.

Непосредственно из теоремы 8 легко получить следствие.

Следствие 7. Пусть J – входная последовательность периода $\omega(J)$ и полноты $\theta(J) > \sigma_A$ автомата $A = (X, S, Y, (h_x)_{x\in X}, (f_x)_{x\in X})$. Тогда при любом $s \in S$

$$(\omega(J), W(A(s, J))) \neq 1.$$

Отметим, что для k-автономного автомата A условие $\theta(J) > \sigma_A$ следствия 7 можно заменить на более слабое: $\theta(J) > \sigma_A - k$.

Это утверждение совместно с утверждением следствия 9 дает следствие 8.

Следствие 8. Пусть J – входная последовательность периода $\omega(J)$ и полноты $\theta(J) > \sigma_A$ автомата A. Тогда периоды выходных последовательностей автомата A строго больше единицы. Если $\omega(J)$ – простое число, то эти периоды кратны $\omega(J)$.

Мы можем теперь дать уточнения оценок мощностей классов неотличимых состояний автомата $A = A' \to A''$.

Теорема 9. Пусть $\theta(A`(s`))>\sigma_{A''}$. Тогда периоды выходных последовательностей автомата $A'\to A''$ больше единицы. Если $|S'|$ – простое число, то

1) периоды выходных последовательностей автомата $A'\to A''$ кратны $|S'|$,

2) мощности классов неотличимых состояний автомата $A'\to A''$ ограничены сверху величиной $|S''|$.

Доказательство. Утверждения о периодах выходных последовательностей автомата $A'\to A''$ непосредственно вытекают из следствия 8. Докажем утверждение пункта 2 теоремы 9. Обозначим через B_i , $i\in[1, t]$ связные компоненты автомата $A'\to A''$. Очевидно, что множество состояний S_{B_i} каждого автомата B_i имеет мощность, кратную $|S'|$, $|S_{B_i}| = k_i|S'|$. Кроме того, число классов неотличимых состояний $l_i = l_{B_i}$ и их мощности $N_i = N_{B_i}$ связаны соотношением $\frac{k_i|S'|}{l_i} = N_i$, при этом $(l_i)_{i\in[1, t]}$ являются периодами выходных последовательностей автомата A'' при входной последовательности $A`(s')$, $s'\in S'$. Так как l_i кратны $|S'|$, то N_i делит k_i и, следовательно, мощности классов неотличимых состояний ограничены величиной $|S''|$, потому что $\sum_{i=1}^{t} k_i = |S''|$. Аналогичным образом доказывается и следствие 9.

Следствие 9. Пусть выходная последовательность автомата A' содержит пару сильно различимых относительно автомата A'', мультиграмм. Тогда периоды выходных последовательностей автомата $A'\to A''$ больше единицы. Если $|S'|$ – простое число, то

1) периоды выходных последовательностей автомата $A'\to A''$ кратны $|S'|$;

2) мощности классов неотличимых состояний автомата $A'\to A''$ ограничены сверху величиной $|S''|$.

Резюмируя приведенный в настоящем пункте подход к изучению оценок сверху мощностей классов неотличимых состояний автономного последовательного соединения перестановочных автоматов, а также связанные с ним исследования оценок периодов выходных последовательностей автоматов, можно заключить, что эффективность проведенных исследований для практики почти полностью определяется умением рассчитывать введенные параметр $\sigma_{A``}$ автомата $A``$ и параметр $\theta(A`(s`))$ выходной последовательности $A`(s`)$ автомата $A`$.

Глава 10. АЛГОРИТМЫ НАХОЖДЕНИЯ МИНИМАЛЬНЫХ СИСТЕМ ОБЛАСТЕЙ ИМПРИМИТИВНОСТИ ГРУППЫ ПОДСТАНОВОК

В данной главе рассмотрим новый алгоритм решения задачи нахождения минимальных систем областей импримитивности группы подстановок.

Пусть $S = \{1, 2, \ldots, n\}$, $(h_x)_{x \in \{1, \ldots, m\}}$ – подстановки на S, $\langle h_1, \ldots, h_m \rangle$ – группа, порожденная подстановками $(h_x)_{x \in \{1,\ldots,m\}}$. Будем предполагать, что $\langle h_1, \ldots, h_m \rangle$ – транзитивная группа.

Один из известных методов построения всех областей импримитивности группы $G = \langle h_1, \ldots, h_m \rangle$ состоит в следующем. Все области импримитивности получаются из систем минимальных областей импримитивности. Под минимальной системой областей импримитивности понимают такую область импримитивности, которую нельзя разбить на собственные подмножества, вновь составляющие области импримитивности. В работе [36] М. Аткинсоном описан и обоснован алгоритм поиска минимальных систем областей импримитивности группы G. Однако сложность этого алгоритма не оценена. Одним из параметров сложности этого алгоритма служит максимальная длина R слова в положительных образующих данной группы, используемого в алгоритме. Из анализа алгоритма вытекает, что данная величина ограничена сверху величиной $|S|-2$. Ниже приводится алгоритм Аткинсона нахождения минимальных областей импримитивности группы подстановок.

10.1. Алгоритм нахождения минимальных систем импримитивности групп подстановок (M. D. Atkinson)

Пусть $\Omega = \{1, 2, \ldots, n\}$ – конечное множество; $g_1, g_2, \ldots, g_m$ – система образующих транзитивной группы подстановок G. Алгоритм заключается в выполнении процедуры P_ω, которая позволяет находить наименьший блок, содержащий $\{1, \omega\}$ и систему блоков, содержащую этот блок. Действие подстановки g_i на элемент β ниже обозначается как βg_i.

Процедура P_ω

Вводится вспомогательное множество C и функция $f: \Omega \to \Omega$.

Шаг 1: $C = \varnothing$ – пустое множество, для любых $\alpha \in \Omega$: $f(\alpha) := \alpha$.

Шаг 2: добавляем ω к C: $C := C \cup \{\omega\}$, $f(\omega) := 1$.

Шаг 3: удаляем β из C: $C := C \setminus \{\beta\}$ и $\alpha := f(\beta)$.

Шаг 4: счетчик $j := 0$.

Шаг 5: $j := j+1$; вычисляем $\gamma = \alpha g_j$ и $\delta = \beta g_j$.

Шаг 6: проверяем, если $f(\gamma) ? = f(\delta)$, то переходим на шаг 9.

Шаг 7: убеждаемся, что $f(\delta) < f(\gamma)$, при необходимости переобозначим δ и γ.

Шаг 8: если для некоторого $\varepsilon \in \Omega$: $f(\varepsilon) ? = f(\gamma)$, то $f(\varepsilon) := f(\delta)$; добавляем $f(\gamma)$ к C: $C := C \cup \{f(\gamma)\}$.

Шаг 9: если $j < m$ – переходим на шаг 5.

Шаг 10: если C – не пусто, то переходим на шаг 3.

Шаг 11: Стоп.

Покажем, что процедура P_ω выполняет поставленную выше задачу. Пусть f_0 – исходная функция f: $f_0(\omega) = 1$ и $f_0(\alpha) = \alpha$ для любого $\alpha \neq \omega$, а $f_1, \ldots, f_r$ – варианты функции f, полученные на шаге 8. Каждой функции f_i соответствует разбиение Π_i множества Ω. Каждый элемент разбиения Π_i множества Ω состоит из символов множества Ω, на которых f_i принимает фиксированное значение. Вследствие шага 8 Π_{i+1} получаем из Π_i объединением двух его элементов.

Для любого разбиения Π множества Ω: обозначим $\Pi(\alpha)$ – элемент разбиения Π, содержащий α. Нетрудно заметить, что $f_0(\alpha) \in \Pi_0(\alpha)$ для любого $\alpha \in \Omega$, а $f_i(\alpha) \in \Pi_i(\alpha)$ для любого α из Ω, $i \in \{1, \ldots, r\}$ (можно показать методом математической индукции по параметру i).

Лемма 1.

a) Если $f_i(\alpha) = f_i(\beta)$ для некоторых $\alpha \in \Omega$, $\beta \in \Omega$, то $f_j(\alpha) = f_j(\beta)$, $j \in \{1, \ldots, r\}$;

b) $f_i^2 = f_i$, $i \in \{0, 1, \ldots, r\}$.

Доказательство.

a) $f_i(\alpha) = f_i(\beta)$. Следовательно, $\alpha \in \prod_i(\alpha)$, $\beta \in \prod_i(\alpha)$, а $\prod_j(\alpha) \supseteq \prod_i(\alpha)$, $j \in \{1, \ldots, r\}$. Значит, $\alpha \in \prod_j(\alpha)$, $\beta \in \prod_j(\alpha)$, $j \in \{1, \ldots, r\}$, то есть $f_j(\alpha) = f_j(\beta)$;

b) для любого $\alpha \in \Omega$: $f_i(\alpha) \in \prod_i(\alpha)$. Следовательно, $f_i(f_i(\alpha)) = f_i(\alpha)$.

Лемма 2.

a) $\alpha \geq f_0(\alpha) \geq f_1(\alpha) \geq \ldots \geq \bar{f}(\alpha) = f_r(\alpha)$;

b) если $\beta \in C$, тогда и только тогда $\beta \neq f(\beta)$;

c) если $\beta \in C$, то существует $\alpha < \beta$: $\bar{f}(\alpha) = \bar{f}(\beta)$ и $\bar{f}(\alpha g_j) = \bar{f}(\beta g_j)$, $j \in \{1, \ldots, m\}$.

Доказательство.

a) Доказательство вытекает из шагов 1, 7, 8;

b) символ β добавляется к C на шагах 2 и 8. На шаге 2: $\beta = \omega$, а $\omega > f_0(\omega) = 1 = \bar{f}(\omega)$. На шаге 8: $\beta = f_i(\gamma)$, для некоторого i и γ. Тогда $f_i(\beta) = \beta = f_i(\gamma)$ и $f_{i+1}(\beta) < f_i(\beta)$. Обратно: если $\beta > \bar{f}(\beta)$, тогда либо $\beta = \omega$ принадлежало C, либо существует i с условием: $\beta = f_i(\beta) > f_{i+1}(\beta)$, тогда очевидно, что $f_i(\beta) = \beta$ принадлежало C;

c) пусть α – символ, определенный на шаге 3. Тогда $\alpha = f_i(\beta) < \beta$ для некоторого i. Более того, $f_i(\alpha) = f_i^2(\beta) = f_i(\beta)$, а значит, $f(\alpha) = \bar{f}(\beta)$. В итоге после шага 8 для заданного j: $f_k(\alpha g_j) = f_k(\beta g_j)$ для некоторого k, а значит $f(\alpha g_j) = \bar{f}(\beta g_j)$.

Лемма 3. $\bar{\Pi} = \Pi_r$ – инвариантно относительно группы G.

Доказательство. Достаточно доказать, что для любая подстановка g_j сохраняет $\bar{\Pi}$. Предположим, что существуют $\theta,\varphi \in \Omega$, $\theta<\varphi$, $\bar{f}(\theta) = \bar{f}(\varphi)$, но $\bar{f}(\theta g_j) \neq \bar{f}(\varphi g_j)$. Выберем φ минимальным, удовлетворяющим этому условию. Тогда $f(\theta) = \bar{f}(\varphi) \leq \theta < \varphi$, следовательно (лемма 2) φ принадлежало C на некотором шаге, а тогда (лемма 2) существует $\alpha \in \Omega$: $\alpha<\varphi$ и $f(\alpha) = \bar{f}(\varphi) = \bar{f}(\theta)$, $\bar{f}(\alpha g_j) = \bar{f}(\varphi g_j)$, но так как φ выбиралось минимальным (то есть $\alpha \leq \theta$), то $\bar{f}(\alpha g_j) = \bar{f}(\theta g_j)$. Тогда $\bar{f}(\theta g_j) = \bar{f}(\alpha g_j) = \bar{f}(\varphi g_j)$ – противоречие.

Обозначим $\Delta = \Pi(1)$ – блок группы G, содержащий $\{1, \omega\}$. Так как G – транзитивна, а $\bar{\Pi}$ – инвариантна относительно G, то $\bar{\Pi}$ – система блоков, содержащая блок Δ.

Лемма 4. Δ – наименьший блок, содержащий $\{1, \omega\}$.

Доказательство. Пусть Δ_1 – минимальный блок, содержащий 1 и ω так что $\Delta_1 \subseteq \Delta$. Пусть $P = \{\Delta_1^g \mid g \in G\}$ – разбиение Ω. Ниже будет доказано, что каждое Π_i – есть продолжение разбиения P(а именно: для любого элемента $B \in \Pi_i$: существует $B' \in P$, что $B \subseteq B'$). Это очевидно, если i = 0. Предположим, что i > 0. Докажем утверждение в этом случае при помощи метода математической индукции.

Пусть Π_i – продолжение разбиения P, тогда Π_{i+1} отличается от Π_i тем, что один из элементов Π_{i+1} получен путем объединения двух элементов Π_i вида $\Pi_i(f_i(\gamma)) \cup \Pi_i(f_i(\delta)) = \Pi_i(\gamma) \cup \Pi_i(\delta)$ {см. шаг 8 и утверждения перед леммой 1}, где $\gamma = \alpha g_j$, $\delta = \beta g_j$ и $\Pi_i(\alpha) = \Pi_i(\beta)$. По предположению индукции, $P(\alpha) = P(\beta)$.

Тогда $P(\gamma) = P(\alpha)g_j = P(\beta)g_j = P(\delta) \supseteq (\Pi_i(f_i(\gamma)) \cup \Pi_i(f_i(\delta)))$. Таким образом, завершен шаг индукции и в итоге у нас есть $\Delta = \bar{\Pi}(1) = \Pi_r(1) \subseteq P(1) = \Delta_1$. Значит, $\Delta = \Delta_1$.

Вывод: для проверки, является ли транзитивная группа подстановок G примитивной, необходимо выполнить процедуру P_ω, $\omega = 1, 2, \ldots, m$.

10.2. Новый алгоритм получения минимальных систем областей импримитивности группы подстановок

В разделе строится новый алгоритм решения указанной задачи. Его особенностью является укрупнение операций алгоритма Аткинсона. Основная идея алгоритма исходит из техники доказательства основных утверждений работы [18]. Доказывается верхняя оценка параметра R, выраженная через диаметр графа, построенного на множестве точек S с дугами, определенными подстановками ($h_1, \ldots, h_m$).

Для нахождения минимальных систем поступаем таким образом. Фиксируем произвольную пару элементов $a, b \in S$, $a \neq b$, вводим следующие обозначения:

$\tau_k = \{x_j, x_{j-1}, \ldots, x_1;\ j \le k\}$ – множество всех слов длины, не большей k, алфавита $X = \{1, 2, \ldots, m\}$, $\varnothing$ – пустое слово, полагаем $\varnothing \in \tau_k$:

$$\Pi_k^{ab} = \{(h_{x_j} h_{x_{j-1}} \ldots h_{x_1} a,\ h_{x_j} h_{x_{j-1}} \ldots h_{x_1} b):\ x_j, x_{j-1}, \ldots, x_1 \in \tau_k\}.$$

Отметим, что $(a, b) \in \Pi_k^{ab}$.

Будем рассматривать Π_k^{ab} как множество неупорядоченных пар элементов. Положим $\hat{\Pi}_k^{ab} = \Pi_k^{ab} \cup \{(c, c), c \in S\}$. Множество пар $\hat{\Pi}_k^{ab}$ будем трактовать и как бинарное отношение на S. Два элемента $(c, d) \in S \times S$ находятся в отношении $\hat{\Pi}_k^{ab}$: $c\ \hat{\Pi}_k^{ab}\ d$ тогда и только тогда, когда $(c, d) \in \hat{\Pi}_k^{ab}$.

Определим бинарное отношение ${}^*\Pi_k^{ab}$ как транзитивное замыкание отношения $\hat{\Pi}_k^{ab}$. Два элемента $(s_1, s_N) \in S \times S$ находятся в отношении ${}^*\Pi_k^{ab}$: $s_1\ {}^*\Pi_k^{ab}\ s_N$ тогда и только тогда, когда найдется цепочка элементов $s_2, \ldots, s_{N-1}$, для которой $(s_i, s_{i+1}) \in \hat{\Pi}_k^{ab}$, $i \in \{1, \ldots, N-1\}$.

Очевидно, ${}^*\Pi_k^{ab}$ – бинарное отношение эквивалентности на S. Пусть $K_k^{ab} = \{\chi_1^k, \ldots, \chi_{p_k}^k\}$ – множество всех классов эквивалентности отношения ${}^*\Pi_k^{ab}$ и $R = R(a, b)$ – минимальное k, при котором $K_k^{ab} = K_{k+1}^{ab}$. Ниже будет доказано, что $K_R^{ab} = K_{R+i}^{ab}$ при любом $i \ge 0$.

Алгоритм построения минимальной системы областей импримитивности группы $\langle h_1, \ldots, h_m \rangle$, один из блоков которой содержит элементы (a, b), состоит в последовательном построении множеств K_k^{ab}, $k \in \{1, \ldots, R\}$. Возможны два случая:

1. $K_R^{ab} = S$, $p_k = 1$.
2. $K_R^{ab} \neq S$, $K_R^{ab} = (\chi_1^R, \ldots, \chi_{p_R}^R)$.

Первый случай характеризуется тем, что (a, b) не могут одновременно принадлежать одному и тому же блоку системы областей импримитивности. Во втором случае K_R^{ab} – минимальная система областей импримитивности группы $\langle h_1, \ldots, h_m \rangle$, один из блоков которой содержит пару (a, b).

Очевидно, сложность нахождения областей импримитивности характеризуется величиной R = R(a, b), максимальной длиной входных слов $x_j, x_{j-1}, \ldots, x_1$, которые участвуют в образовании пар Π_k^{ab}.

Теорема. Справедлива следующая оценка

$$R(a, b) \leq (L_0 + 1)(D + 1) + K_{L_0+1} - 2.$$

Здесь D – диаметр графа переходов автомата Медведева $A = (X, S, (h_x)_{x \in X})$ с входным алфавитом X, множеством состояний S, частичными функциями переходов $(h_x)_{x \in X}$. L_0 – максимальное $L \in \{0, 1, \ldots\}$, если оно существует, при котором $K_L - K_{L+1} > D + 1$, где K_L – частное от деления |S| на 2^L. Если такого L не существует, то полагаем $L_0 = -1$.

Доказательство. Очевидно, для любого k: K_k^{ab} является подразбиением K_{k+1}^{ab}, то есть каждый блок χ_i^{k+1} разбиения K_{k+1}^{ab} является объединением некоторых блоков χ_i^k отношения ${}^*\Pi_k^{ab}$.

Покажем теперь, что если при некотором k_0: ${}^*\Pi_{k_0}^{ab} = {}^*\Pi_{k_0+1}^{ab}$, то ${}^*\Pi_{k_0}^{ab} = {}^*\Pi_{k_0+i}^{ab}$ при любом i. Для этого докажем, что из ${}^*\Pi_k^{ab} = {}^*\Pi_{k+1}^{ab}$ и $c_1 \, {}^*\Pi_{k+2}^{ab} \, c_N$, $c_1, c_N \in S$ следует $c_1 \, {}^*\Pi_k^{ab} \, c_N$.

Пусть для некоторого k: ${}^*\Pi_k^{ab} = {}^*\Pi_{k+1}^{ab}$ и $c_1 \, {}^*\Pi_{k+2}^{ab} \, c_N$. Последнее соотношение равносильно существованию элементов $c_2, \ldots, c_{N-1}$, при которых

$$c_1 \hat{\Pi}_{k+2}^{ab} c_2 \hat{\Pi}_{k+2}^{ab} \ldots c_{N-1} \hat{\Pi}_{k+2}^{ab} c_N.$$

При этом мы можем считать, что среди $c_1, \ldots, c_N$ нет одинаковых элементов, то есть $(c_i, c_{i+1}) \in \Pi_{k+2}^{ab}$, $i \in \{1, 2, \ldots, N-1\}$.

Пусть

$$c_i = h_{x_{k+2}} h_{x_{k+1}} \ldots h_{x_1} a, \quad c_{i+1} = h_{x_{k+2}} h_{x_{k+1}} \ldots h_{x_1} b.$$

Так как ${}^*\Pi_k^{ab} = {}^*\Pi_{k+1}^{ab}$, то

$$h_{x_{k+1}}\ h_{x_k}\ \ldots\ h_{x_1}\ \mathrm{a}\ {}^*\Pi_k^{ab}\ h_{x_{k+1}}\ h_{x_k}\ \ldots\ h_{x_1}\ \mathrm{b}.$$

Тогда

$$h_{x_{k+2}}\ h_{x_{k+1}}\ \ldots\ h_{x_1}\ \mathrm{a}\ {}^*\Pi_{k+1}^{ab}\ h_{x_{k+2}}\ h_{x_{k+1}}\ \ldots\ h_{x_1}\ \mathrm{b}$$

и опять в силу ${}^*\Pi_k^{ab} = {}^*\Pi_{k+1}^{ab}$:

$$h_{x_{k+2}}\ h_{x_{k+1}}\ \ldots\ h_{x_1}\ \mathrm{a}\ {}^*\Pi_k^{ab}\ h_{x_{k+2}}\ h_{x_{k+1}}\ \ldots\ h_{x_1}\ \mathrm{b}.$$

Таким образом, $c_i\ {}^*\Pi_k^{ab}\ c_{i+1}$. Так как i было выбрано произвольно, то получаем $c_1\ {}^*\Pi_k^{ab}\ c_N$. Из доказанного вытекает, что $R(a,b) \le |S| - 2$. В частности, наше утверждение доказано при $L_0 = -1$, так как в этом случае $K_{L_0+1} = K_0 = |S|$.

Предположим теперь, что $L_0 \ne -1$. Имеем $K_0^{ab} = (\chi_1^0, \ldots, \chi_{p_0}^0)$, $\chi_1^0 = (a, b)$, $|\chi_1^0| = 1$, $p_0 = |S| - 1$. По условию $|S| - K_1 > D+1$. Поэтому для $K_D^{ab} = (\chi_1^D, \ldots, \chi_{p_0}^D)$ справедливы неравенства $|\chi_i^D| \ge 2$, $i \in \{1, 2, \ldots, p_D\}$. Здесь использовано то, что в любое состояние можно перейти из (a, b) за D или менее шагов. При $L_0 = 0$ имеем $p_D \le K_1$, а для $D+i+1 \le R(a, b)$ имеем

$$p_{D+i+1} < p_{D+i}.$$

Следовательно, $R(a, b) \le D + P_D - 1 \le D + K_1 - 1$.

Для доказательства теоремы в случае $L_0 > 0$ нам потребуется вспомогательная лемма. Обозначения леммы. Пусть $\{M_i\}$ – некоторая совокупность подмножеств множества $\{1, \ldots, n\}$. Будем говорить, что множества M_i, M_j находятся в бинарном отношении σ и писать $M_i \sigma M_j$ тогда и только тогда, если $M_i \cap M_j \ne \varnothing$. Будем говорить, что M_1 и M_N из $\{M_i\}$ эквивалентны: $M_1 \sim M_N$, если существуют $M_2, \ldots, M_{N-1}$ из $\{M_i\}$, для которых

$$M_1 \sigma M_2 \sigma \ldots \sigma M_{N-1} \sigma M_N.$$

Утверждение леммы. Класс эквивалентности χ_j^{k+m}, $j \in \{1, 2, \ldots, p_{k+m}\}$ бинарного отношения эквивалентности ${}^*\Pi_{k+m}^{ab}$ является объединением всех множеств из класса отношения эквивалентности $\sim$, определенного на совокупности множеств

$$\{h_{x_j}\ h_{x_{j-1}}\ \ldots\ h_{x_1}\ \chi_\alpha^k : \alpha \in \{1, \ldots, p_k\}, x_j, \ldots, x_1 \in \tau_m, 0 \le j \le m\}.$$

Доказательство леммы.

Пусть U – объединение всех множеств из некоторого класса эквивалентности отношения $\sim$, определенного на совокупности множеств

$\{h_{x_L} h_{x_{L-1}} \dots h_{x_L} \chi_\alpha^k : \alpha \in [1, p_k], x_L, \dots, x_1 \in \tau_m, 0 \le L \le m\}$ и $s_1 \in U$.

Нам необходимо доказать, что $s_1 {}^* \Pi_{k+m}^{ab} s_N$ тогда и только тогда, если $s_N \in U$.

Пусть существуют $s_2, \dots, s_{N-1}$, для которых $s_1 \hat{\Pi}_{k+m}^{ab} s_2 \hat{\Pi}_{k+m}^{ab} \dots s_{N-1} \hat{\Pi}_{k+m}^{ab} s_N$, и предположим, что $s_i \in U$. Покажем, что тогда и $s_{i+1} \in U$. Действительно, имеем для некоторого $\mathfrak{I}^j = x_j, x_{j-1}, \dots, x_1$, $j \le k+m$ и $\varepsilon \in \{0, 1\}$: $s_i = h_{x_j} h_{x_{j-1}} \dots h_{x_1} a_\varepsilon$, $s_{i+1} = h_{x_j} h_{x_{j-1}} \dots h_{x_1} a_{\varepsilon+1}$, где $a_0 = a$, $a_1 = b$, сумма $\varepsilon+1$ берется по модулю 2. При $j \le k$, очевидно, что $(s_i, s_{i+1}) \in \Pi_k^{ab}$, то есть $s_i, s_{i+1} \in \chi_\alpha^k$ при некотором α. Следовательно, $s_{i+1} \in U$.

При $j > k$

$$s_i = h_{x_j} h_{x_{j-1}} \dots h_{x_{k+1}} h_{x_k} \dots h_{x_1} a_\varepsilon, \quad s_{i+1} = h_{x_j} h_{x_{j-1}} \dots h_{x_{k+1}} h_{x_k} \dots h_{x_1} a_{\varepsilon+1}.$$

При этом $h_{x_k} \dots h_{x_1} a_\varepsilon \in \chi_\alpha^k$, $h_{x_k} \dots h_{x_1} a_{\varepsilon+1} \in \chi_\alpha^k$ при некотором α. Следовательно, $(s_i, s_{i+1}) \in h_{x_j} h_{x_{j-1}} \dots h_{x_{k+1}} \chi_\alpha^k$. Поэтому $s_{i+1} \in U$.

Используя принцип математической индукции, заключаем, что $s_N \in U$.

Пусть теперь $s_1, s_N \in U$ и, не ограничивая общности, пусть $s_1 \in M_1$, $s_N \in M_N$ и $M_1 \sigma M_2 \sigma \dots \sigma M_{N-1} \sigma M_N$, где M_i – множество вида $h_{x_j} h_{x_{j-1}} \dots h_{x_1} \chi_\alpha^k$, здесь $\alpha \in \{1, \dots, p_k\}$, $x_l, \dots, x_1 \in \tau_m$, $0 \le j \le m$. Докажем, что для любых $s_i \in M_i$, $s_{i+1} \in M_{i+1}$: $s_i {}^* \Pi_{k+m}^{ab} s_{i+1}$.

Пусть $s \in M_i \cap M_{i+1}$. Покажем, что $s_i {}^* \Pi_{k+m}^{ab} s$, $s_{i+1} {}^* \Pi_{k+m}^{ab} s$. Отсюда в силу произвольности выбора i и будет следовать нужное бинарное отношение $s_1 {}^* \Pi_{k+m}^{ab} s_N$.

Положим

$$s = h_{x_j} h_{x_{j-1}} \dots h_{x_1} c_1 = h_{x_j} h_{x_{j-1}} \dots h_{x_1} h_{x'_{t'}} \dots h_{x'_1} a_{\varepsilon'}, \ t' \le k,$$

$$s_i = h_{x_j} h_{x_{j-1}} \dots h_{x_1} c_T = h_{x_j} h_{x_{j-1}} \dots h_{x_1} \delta_{i''_{t''}} \dots \delta_{i''_1} a_{\varepsilon''}, \ t'' \le k, \ \varepsilon', \varepsilon'' \in \{0, 1\}.$$

Здесь $(c_1, c_T) \in \chi_\alpha^k$. По определению χ_α^k, найдутся $(c_2, \dots, c_{T-1}) \in S$, при которых $c_1 \hat{\Pi}_k^{ab} c_2 \hat{\Pi}_k^{ab} \dots c_{T-1} \hat{\Pi}_k^{ab} c_T$. Если $c_i = h_{x_p^{(1)}} \dots h_{x_1^{(1)}} a_\varepsilon$, $c_{i+1} = h_{x_p^{(1)}} \dots h_{x_1^{(1)}} a_{\varepsilon+1}$, где $x_p^{(1)}, \dots, x_1^{(1)} \in \tau_k$, то

$$h_{x_j} h_{x_{j-1}} \dots h_{x_1} c_i \hat{\Pi}_{k+m}^{ab} h_{x_j} h_{x_{j-1}} \dots h_{x_1} c_{i+1}.$$

Следовательно, $h_{x_j} h_{x_{j-1}} \dots h_{x_1} c_1 \hat{\Pi}_{k+m}^{ab} h_{x_j} h_{x_{j-1}} \dots h_{x_1} c_T$.

Аналогичным образом показывается, что $s_{i+1} {}^{*}\Pi^{ab}_{k+m}$ s.

Лемма полностью доказана.

Проведем доказательство утверждения теоремы в случае $L_0 > 0$.

Ранее было показано, что при любом j

$$|\chi_j^D| \geq 2.$$

Если ${}^{*}\Pi^{ab}_{D} \neq {}^{*}\Pi^{ab}_{D+1}$, то, очевидно, существует j_0, при котором $|\chi_{j_0}^{D+1}| \geq 4$. Тогда использование леммы дает $|\chi_j^{2D+1}| \geq 4$ при любом $j \in \{1, \ldots, p_{2D+1}\}$.

Аналогично получим: для любого $L \leq L_0$ либо $|\chi_j^{L(D+1)+D}| \geq 2^{L+1}$, $j \in \{1, \ldots, p_{L(D+1)+D}\}$, либо при некотором $L \leq L_0$

$${}^{*}\Pi^{ab}_{L(D+1)+D} = {}^{*}\Pi^{ab}_{L(D+1)+D+1}.$$

В первом случае, в частности, имеем

$$p_{L_0(D+1)+D} \leq K_{L_0+1},\ P_{L_0(D+1)+D+i} \geq P_{L_0(D+1)+D+i+1} \qquad (12)$$

при любом i. При этом минимальное i_0, при котором будет иметь место равенство, определяет $R(a, b) = L_0(D+1)+D+i_0$.

Из (12) получаем $i_0 \leq R(a, b) \leq K_{L_0+1} - 1$. Следовательно, $R(a, b) \leq L_0(D+1)+D+K_{L_0+1} - 1$, что и требовалось доказать.

Из данной оценки несложно получить

$$R(a, b) \leq (D+1)[\log_2 |S|+1] - 2,$$

где $[\nu]$ – целая часть числа ν.

Глава 11. ОДНОСТОРОННЯЯ НЕОТЛИЧИМОСТЬ СОСТОЯНИЙ КОНЕЧНЫХ АВТОМАТОВ

В разделе вводится и изучается понятие (Ψ, η)-неотличимости состояний конечного автомата. Предлагается метод определения начального состояния автомата по его входному и соответствующему ему выходному слову.

11.1. Понятие (Ψ, η)-неотличимости состояний автомата

Известная работа Э. Мура [27], приведшая к созданию экспериментов с автоматами, опиралась на явление неотличимости состояний автомата, состоящее в том, что неотличимые состояния одинаково реагируют на одни и те же входные слова. Данное понятие допускает обобщение, которое здесь и рассматривается. Неотличимость одного состояния от другого в таком обобщенном смысле трактуется как функциональная зависимость выходных слов автомата полученных со второго состояния от выходных слов, полученных с первого состояния. Ряд приводимых ниже определений и утверждений сформулированы ранее в [4].

Пусть $A = (X, S, Y, (h_x)_{x\in X}, (f_x)_{x\in X})$ – конечный автомат. Рассмотрим отображение $\Psi: X\to X$ и семейство отображений $\eta = (\eta_x)_{x\in X}$, $\eta_x: S\to Y$, $x\in X$. Для $\mathfrak{I} = x(1), x(2), .., x(k)$ положим $\Psi(\mathfrak{I}) = \Psi(x(1)), \Psi(x(2)), .., \Psi(x(k))$.

Определение 1. Состояние $s\in S$ автомата A называется (Ψ, η, k)-неотличимым от $s'\in S$, если при любом входном слове $\mathfrak{I} = x_1, x_2, .., x_k$ из X^k выходные последовательности

$$A(s, \mathfrak{I}) = y_1, y_2, .., y_k, A(s', \Psi(\mathfrak{I})) = y'_1, y'_2, .., y'_k$$

автомата A, соответствующие его начальным состояниям s, s’ и, соответственно, входным словам $\mathfrak{I}$, $\Psi(\mathfrak{I}) = \Psi(x_1), \Psi(x_2), .., \Psi(x_k)$, связаны соотношением

$$y'_j = \eta_{x(j)}y_j\ ,\ j \in [1, k].$$

Определение 2. Состояние $s\in S$ автомата A называется (Ψ,η)-неотличимым от состояния $s'\in S$, если оно (Ψ, η, k) неотличимо от s' при любом $k\in[1, 2, ...)$.

Следующий простейший пример показывает существование автоматов с (Ψ,η)-неотличимыми состояниями.

Пример 1. Положим X = {0}, то есть автомат A = (X, S, Y, $(h_x)_{x\in X}$, $(f_x)_{x\in X}$) – автономный, S = {1, 2, 3, 4, 5, 6}, Y = {0, 1} и

$$h_0(j) = j+1,\ j\in[1, 5],\ h_0(6) = 1;$$

$$f_0(1)= f_0(2) = f_0(3) = 0;\ f_0(4) = f_0(5) = f_0(6) = 1.$$

Таким образом, данный автономный автомат является полноцикловым, приведенным, и непосредственная проверка для отображений

$$\Psi: 0\to0\quad \eta_0: 0\to1,\ 1\to0$$

показывает, что состояние j (Ψ, η)-неотличимо от состояния j+3 mod(6), j∈[1,6].

11.2. Определение начального состояния автомата по его входному и выходному слову

Для автомата A, имеющего (Ψ, η)-неотличимые состояния, можно предложить следующий подход к определению его начального состояния по заданному входному слову $\mathfrak{I}$ = x(1), x(2), ..., x(k) и выходной последовательности $A(s_o, \mathfrak{I}) = Q = y_1, y_2, ..., y_k$. Именно по заданным $\mathfrak{I}$ и Q строим пары $\Psi^j\mathfrak{I}$, η^jQ , j∈[0, m], $\psi^o\mathfrak{I} = \mathfrak{I}$, $\eta^oQ = Q$. Если $\Psi^j\mathfrak{I} = x'(1), x'(2), \ldots, x'(k)$, $\eta^jQ = y'_1, y'_2, ..., y'_k$, то

$$\Psi^{j+1}\mathfrak{I} = \Psi x'(1), \Psi x'(2), \ldots, \Psi x'(k);$$

$$\eta^{j+1}Q = \eta_{x(1)}y`_1, \eta_{x(2)}y`_2, \ldots, \eta_{x(k)}y`_k.$$

Здесь m – параметр метода. Далее методом опробования с использованием памяти [2] находим решение хотя бы одного из уравнений: $A(s, \Psi^j\mathfrak{I}) = \eta^jQ$, j∈[0, m]. Затем решаем задачу определения искомого состояния s_o по известному состоянию s^*, найденному ранее как решение уравнения $A(s,\Psi^{j_o}\mathfrak{I}) = \eta^{j_o}Q$, при некотором $j_o\in[0, m]$, используя отношение (Ψ,η)-неотличимости состояний автомата A.

Ниже будет показано, что отношение (Ψ, η)-неотличимости состояний автомата индуцирует в ряде случаев взаимно однозначное соответствие φ на множестве состояний S автомата A такое, что состояние s (Ψ, η)-неотличимо от состояния φs. В связи с этим для применения метода опробования с использованием памяти m выбираем так, чтобы оно не превосходило длины минимального цикла подстановки φ; решение s_o на последнем этапе метода можно найти, опробуя состояния s^*, φs^*, ..., $\varphi^{t(s^*)-1}s^*$, где t(s*) – длина цикла подстановки φ, содержащего s^*.

11.3. Свойства (Ψ, η)-неотличимых состояний автомата

Следующее утверждение непосредственно вытекает из определений 1, 2.

Лемма 1. Если состояние $s \in S$ автомата A (Ψ, η, k)-неотличимо ((Ψ, η)-неотличимо) от состояния $s' \in S$, то для любого входного слова x(1), x(2), ..., $x(j) \in X^j$, $j < k$ состояние $h_{x(j)}$, $h_{x(j-1)}$, ..., $h_{x(1)}s$ (Ψ, η, k–j)-неотличимо ((Ψ, η)-неотличимо) от состояния $h_{\Psi x(j)}$, $h_{\Psi x(j-1)}$, ..., $h_{\Psi x(1)}s`$.

Для автомата A и отображения $\Psi: X \to X$ определим вспомогательный автомат $A_{M,\psi} = (X`, S \times S, Y \times Y, (\Delta_{x`})_{x` \in X`}, (\beta_{x`})_{x` \in X`})$, где $X` = \{(x, \Psi x), x \in X`\}$, $\Delta_{(x,\Psi x)}(s, s') = (h_x s, h_{\Psi x} s')$, $\beta_{x,\Psi x}(s, s') = (f_x s, f_{\Psi x} s')$.

Фиксируя начальное состояние (s, s′) автомата $A_{M,\psi}$, получаем инициальный автомат $A_{M,\psi}(s, s')$ и автомат $A_{M,\psi}\langle(s, s')\rangle$, порожденный начальным состоянием (s, s′).

Определим диаметр D(s, s`) инициального автомата $A_{M,\psi}\langle(s, s')\rangle$ как минимальное число D, такое, что для любой вершины (s″, s‴) графа перехода автомата $A_{M,\psi}\langle(s, s')\rangle$, если состояние (s″, s‴) достижимо из (s, s′) , то оно достижимо с помощью некоторого входного слова, длина которого не больше D.

Лемма 2. Если состояние s автомата A (Ψ, η, k)-неотличимо от состояния $s' \in S$ при $k > D(s, s')$, то состояние s (ψ, η)-неотличимо от s′.

Доказательство. Пусть выполнены условия леммы 2. Покажем, что s (Ψ, η)-неотличимо от s’. Рассмотрим произвольное входное слово $\mathfrak{I} = x(1), x(2), \ldots, x(k+1) \in X^{k+1}$. Имеем

$$A(s, x(1), x(2), \ldots, x(k+1)) = y_1, y_2, \ldots, y_k, y_{k+1},$$

$$A(s', \Psi(x(1)), \Psi(x(2)), \ldots, \Psi(x(k+1))) = y_1', y_2', \ldots, y_k', y_{k+1}',$$

где $y_1', y_2', \ldots, y_k' = \eta_{x(1)}y_1, \eta_{x(2)}y_2, \ldots \eta_{x(k)}y_k$, и остается показать, что

$$y'_{k+1} = \eta_{x(k+1)}y_{k+1},$$

то есть

$$\eta_{x(k+1)}f_{x(k+1)}h_{x(k)}\ldots h_{x(1)}s = f_{\Psi(x(k+1))}h_{\Psi(x(k))}\ldots h_{\Psi(x(1))}s'.$$

Заметим, что состояние $(h_{x(k)}\ldots h_{x(1)}s, h_{\Psi(x(k))}\ldots h_{\Psi(x(1))}s')$ достижимо в автомате $A_{M,\psi}\langle(s, s')\rangle$ при некотором входном слове x’(1), x’(2), …, x’(L) длины $L \le D(s, s')$ и по условию леммы для входного слова

$$x''(1), x''(2), \ldots, x''(L), x''(L+1) = x'(1), x'(2), \ldots, x'(L), x(k+1)$$

имеем

$$A(s, x''(1), x''(2), \ldots, x''(L), x''(L+1)) = y_1'', y_2'', \ldots, y_L'', y_{L+1}'',$$

$$A(s', \psi(x''(1)), \psi(x''(2)), \ldots, \psi(x''(L)), \psi(x''(L+1))) =$$

$$= \eta_{x''(1)}y_1'', \ldots, \eta_{x''(L)}y_L'', \eta_{x''(L+1)}y_{L+1}'',$$

в частности,

$$\eta_{x(k+1)}f_{x(k+1)}h_{x(k)}\ldots h_{x(1)}s = \eta_{x''(L+1)}y_{L+1}'' = f_{\psi(x(k+1))}h_{\psi(x(k))}\ldots h_{\psi(x(1))}s',$$

что и требовалось доказать.

Понятие (ψ, η)-неотличимость состояний автомата A естественным образом определяет бинарное отношение $\varphi = \varphi(\Psi, \eta)$ на его множестве состояний S.

Лемма 3. Если для сильно связного автомата A и отображений Ψ, $\eta = (\eta_x)_{x\in X}$ справедливо: $\varphi \neq \varnothing$, и автомат A сильно связан, то $Пр_1\varphi = S$, то есть, если в сильно связном автомате A найдется некоторое состояние s (Ψ, η)-неотличимое от некоторого s', то для любого состояния автомата A найдется (Ψ, η)-неотличимое от него состояние.

Утверждение леммы непосредственно следует из сильной связности автомата A и леммы 1.

Обозначим через φ^{-1} обратное отношение к бинарному отношению φ. Очевидно $Пр_1\varphi^{-1} = Пр_2\varphi$. Легко доказывается следующий аналог леммы 3.

Лемма 4. Если для сильно связного автомата A и отображений ψ, $\eta = (\eta_x)_{x\in X}$ справедливо: $\varphi \neq \varnothing$ и ψ – подстановка на X, то $Пр_1\varphi^{-1} = Пр_2\varphi = S$.

Лемма 5. Если для приведенного автомата A и отображений ψ, $\eta = (\eta_x)_{x\in X}$ справедливо: $\varphi \neq \varnothing$ и ψ – подстановка на X, то бинарное отношение φ является отображением S в S.

Доказательство. Предположим, что при выполнении условий леммы 5 найдутся состояния s, s_1, s_2 из S, при которых

$$(s, s_1)\in\varphi, (s_1, s_2)\in\varphi, s_1 \neq s_2,$$

то есть состояние s (Ψ,η)-неотличимо от s_1 и s_2 одновременно. Тогда при любом входном слове $\mathfrak{I} = x(1), x(2), \ldots, x(L), L\in[1, 2, \ldots)$ автомата A имеем

$$A(s, \mathfrak{I}) = y_1, y_2, \ldots, y_L;$$

$$A(s_1,\psi(\mathfrak{I}))=\eta_{x(1)}y_1,\eta_{x(2)}y_2,\ldots,\eta_{x(L)}y_L=A(s_2,\psi(\mathfrak{I})).$$

Так как ψ – подстановка на X, а x(1), x(2), …, x(L) – произвольное входное слово автомата A, то состояния s_1, s_2 неотличимы, что противоречит приведенности автомата A.

Следующее утверждение доказывается аналогично лемме 5.

Лемма 6. Если для приведенного автомата A и отображений ψ, $\eta = (\eta_x)_{x\in X}$ справедливо, что $\varphi \neq \varnothing$ и $\eta = (\eta_x)_{x\in X}$ – подстановки на Y, то бинарное отношение φ^{-1} является отображением S в S.

Теорема 1. Если для биекций ψ и $\eta = (\eta_x)_{x\in X}$ на X и Y, соответственно, и приведенного сильно связного автомата A справедливо, что $\varphi \neq \varnothing$, то φ – подстановка на S и $\underset{s\in S}{НОК}\ t(s)$ делит НОК(degφ, $\underset{s\in S}{НОД}\, t(s)$), где t(s) – длина цикла подстановки φ, которому принадлежит $s\in S$, degφ = $\underset{x\in X}{НОК}\ t(x)$, t(x) – длина цикла подстановки Ψ, содержащего элемент $x\in X$.

Доказательство. Из лемм 3, 4, 5, 6 непосредственно вытекает, что при выполнении условий теоремы φ является подстановкой на S. Фиксируем произвольное состояние $s\in S$ и рассмотрим цикл подстановки φ: s, φs, …, $\varphi^t s = s$, t = t(s). Выберем произвольное состояние $s^*\in S$. Так как автомат A сильно связный, то найдется его входное слово $\Im = x(1), x(2), ..., x(k)$, при котором

$$h_{x(k)}h_{x(k-1)}\ldots h_{x(1)}s = s^*.$$

По лемме 1 состояние $h_{\psi^j(x(k))}\ldots h_{\psi^j(x(1))}\varphi^j s$, (Ψ,η)-неотличимо от состояния $h_{\psi^{j+1}(x(k))}\ldots h_{\psi^{j+1}(x(1))}\varphi^{j+1}s$, $j\in[0, 1, ...)$, то есть

$$\varphi\, h_{\psi^j(x(k))}\ldots h_{\psi^j(x(1))}\varphi^j s = h_{\psi^{j+1}(x(k))}\ldots h_{\psi^{j+1}(x(1))}\varphi^{j+1}s\ .$$

Таким образом,

$$\varphi^j s^* = h_{\psi^j(x(k))}\ldots\ h_{\psi^j(x(1))}\varphi^j s\ ,\ j\in[0, 1, ...).$$

Из последнего равенства непосредственно вытекает, что

$$t(s^*)\ |\ НОК(t(s), deg\Psi)$$

при любом выборе состояний s, s^* из S, следовательно

$$t(s^*)\ |\ НОК(deg\Psi,\ \underset{s\in S}{НОД}\, t(s)).$$

Откуда вытекает

$$\underset{s\in S}{НОК}\, t(s)\ |\ НОК(deg\Psi,\ \underset{s\in S}{НОД}\, t(s)\ ).$$

Утверждение теоремы доказано.

Как следует из доказательства данной теоремы, при выполнении ее условий справедливы равенства

$$\eta_x f_x = f_{\Psi(x)}\varphi;$$
$$\varphi h_x \varphi^{-1} = h_{\Psi(x)};$$
$$x\in X,$$

которые можно использовать для явного описания отображения φ, в связи с чем несложно доказывается следующее утверждение.

Теорема 2. Пусть Ψ и $\eta = (\eta_x)_{x\in X}$ – биекции на X и Y соответственно. Сильно связный приведенный автомат $A = (X, S, Y, (h_x)_{x\in X}, (f_x)_{x\in X})$ имеет (Ψ, η)-неотличимые состояния ($\varphi \neq \varnothing$) тогда и только тогда, когда при любом $x\in X$ выполняются равенства

$$\eta_x f_x = f_{\Psi(x)}\varphi,\ \varphi h_x \varphi^{-1} = h_{\Psi(x)},\ x\in X,$$

где φ – некоторая подстановка на S.

Через $G = \langle (h_x)_{x\in X}\rangle$ обозначим полугруппу отображений S в S, порожденную частичными функциями перехода $(h_x)_{x\in X}$ автомата A. Напомним, что полугруппа G называется импримитивной, если существует разбиение $R(S) = (S_1, S_2, \ldots, S_m)$ множества S, при котором $2 \le m \le |S|-1$ и для любых $j\in\{1, \ldots, m\}$, $x\in X$ найдется $j`\in\{1, \ldots, m\}$ со свойством $h_x(S_j) \subseteq S_{j`}$. Система множеств $(S_1, S_2, \ldots, S_m)$ называется системой блоков импримитивности полугруппы G. Из теорем 1, 2 легко получить следствие 1.

Следствие 1. Пусть выполнены условия теоремы 1, причем ψ – тождественное отображение X на X . Тогда φ – подстановка на S с циклами одинаковой длины t; если $t \neq 1$, то циклы φ являются блоками импримитивности полугруппы $G = \langle (h_x)_{x\in X}\rangle$ автомата A и для любого $x\in X$ ограничение отображения h_x на каждом цикле инъективно.

Обозначим через $\deg\Phi$ порядок отображения $\Phi: X\times Y \to X\times Y$

$$\Phi(x, y) = (\Psi x, \eta_x y)$$

для заданных биекций Ψ, $\eta = (\eta_x)_{x\in X}$ на X и Y соответственно.

Теорема 3. Если для сильно связного приведенного автомата A и биекций Ψ, $\eta = (\eta_x)_{x\in X}$ справедливо $\varphi \neq \varnothing$, то φ – подстановка на S и $t(s)|\deg\Phi$, где t(s) – длина цикла подстановки φ, содержащего состояние $s\in S$, а $\deg\Phi$ – порядок отображения $\Phi: X\times Y\to X\times Y$

$$\Phi(x, y) = (\psi(x), \eta_x(y)).$$

Доказательство. По теореме 1 φ – подстановка на S. Пусть

$$A(s, x(1), \ldots, x(k)) = y_1, \ldots, y_k.$$

Используя условия теоремы, легко получить

$$A(\varphi^{\deg\Phi}s, x(1) \ldots, x(k)) = y_1, \ldots, y_k.$$

Так как автомат A приведен, то

$$\varphi^{\deg\Phi}s = s$$

Следовательно, $t(s) \mid \deg\Phi$.

Пример 2. Пусть $A=(X, S, Y, (h_x)_{x\in X}, (f_x)_{x\in X})$ – приведенный, сильно связный автомат, $X = Y= \{0, 1\}$, $\Psi = E$ – тождественное отображение X в X, а $\eta_x = \eta$ для всех $x\in X$, при этом $\eta(0) = 1$, $\eta(1) = 0$.

Если для автомата A и указанных отображений Ψ, η выполнено $\varphi \neq \varnothing$, то, используя утверждения теорем 1, 3, заключаем, что длины циклов подстановки φ равны 2, в частности, число $|S|$ должно быть четным числом.

Пример 3. Пусть $A = (X, S, Y, (h_x)_{x\in X}, (f_x)_{x\in X})$ – приведенный, сильно связный автомат, $Y = G$ – конечная группа, $\Psi = E$, а $\eta_x = \eta$ для всех $x \in X$, причем $\eta: g \to gg_0$, $g \in G$, где g_0 – некоторый фиксированный, отличный от единицы элемент группы G. Если для автомата A и отображений Ψ, η выполнено $\varphi \neq \varnothing$, то по теореме 3 и следствию 1 заключаем, что φ – подстановка с циклами одинаковой длины и эта длина делит порядок элемента g_0, в частности, при этом $(|G|, |S|) \neq 1$.

Пример 4. Рассмотрим автономный автомат $A = (S, Y, \delta, \lambda)$, $\delta: S \to S$, $\lambda: S \to Y$.

Тогда (Ψ, η)-неотличимость состояний s, s′ автомата A означает, что для отображения $\eta: Y \to Y$ из равенства $A(s) = y_1, y_2, \ldots$ вытекает равенство $A(s`) = \eta(y_1), \eta(y_2), \ldots$. Поэтому для автономного автомата A данное понятие удобно трактовать как η-неотличимость состояний s, s′.

11.4. (η, d)-периодические выходные последовательности автономного автомата

Пусть η не является тождественным отображением Y в Y, а d – некоторое натуральное число. Будем говорить, что последовательность $y_1, y_2, \ldots$ элементов алфавита Y $\varphi \neq \varnothing$ (имеет (η, d)-период), если $y_{j+d} = y_j$, $j \in \{1, 2, \ldots\}$. Легко доказывается следующее утверждение: полноцикловый автомат A имеет η-неотличимые состояния тогда и только тогда, если для его выходной последовательности существует (η, d)-период для некоторого $d < S$.

Теорема 4. Пусть $Q = y_1, y_2, \ldots$ – периодическая (иногда говорят, что чисто периодическая) последовательность элементов алфавита Y периода ω и пусть каждый элемент y из Y содержится в последовательности Q. Если последовательность Q имеет (η, d)-период при некотором $\eta: O \to O$, то

а) η-подстановка на O;

б) $\omega = D\deg(\eta)$, где $D = (d, \omega)$;

в) $D \geq \frac{\omega}{C}$, где C = max(degσ) и максимум берется по всем подстановкам σ из симметрической группы степени |Y|, таким, что длины циклов ее являются делителями ω.

Доказательство. Пусть M = НОК(d, ω). Тогда

$$y_{j+M} = \eta^{\frac{M}{d}}(y_j) = y_j,\ j \in [1, 2 \ldots)$$

и, так как по условию каждый элемент из Y содержится в последовательности Q, заключаем, что η-подстановка на Y.

Обозначим период последовательности $y_j, y_{j+D}, \ldots, y_{j+kD}, \ldots$ через ω_j. Очевидно,

$$\omega \mid D \cdot НОК(\omega_1, \omega_2, \ldots, \omega_D)$$

и

$$y_{j+kD} = y_{j+(k+\frac{\omega}{D})D},\ j \in [1, 2, \ldots),$$

то есть $НОК(\omega_1, \ldots, \omega_D) \mid \frac{\omega}{D}$. Следовательно,

$$\omega = D \cdot НОК(\omega_1, \ldots, \omega_D).$$

Легко показывается, что ω_j является периодом также и последовательности

$$y_j, y_{j+d}, \ldots, y_{j+kd}, \ldots .$$

Следовательно,

$$\omega_j = t(y_j),$$

где $t(y_j)$ – длина цикла подстановки η, содержащего элемент y_j. Заметим также, что число циклов η не превосходит D. Из указанного выше вытекает

$$\deg\eta = НОК(\omega_1, \ldots, \omega_D).$$

Таким образом,

$$\omega = D \cdot \deg\eta,$$

откуда

$$D \geq \frac{\omega}{C}.$$

Следствие 2. Пусть выполнены условия теоремы 4. Тогда

$$d \geq \frac{P}{\max\deg\sigma},$$

где p – некоторый произвольный делитель ω, а максимум берется по всем подстановкам σ из симметрической группы подстановок на Y.

Утверждение данного следствия непосредственно вытекает из теоремы 4. Оно может быть использовано при исследовании (η, d)-

периодичности последовательностей, периоды которых кратны известному числу P.

Непосредственно из теоремы 4 вытекает следствие 3.

Следствие 3.

1. Если для полноциклового, приведенного автомата $A = (S, Y, \delta, \lambda)$ и нетождественной подстановки η на Y имеет место $НОД(deg\eta, |S|) = 1$, то в автомате A отсутствуют η-неотличимые состояния, выходная последовательность A(s) при любом $s \in S$ не является (η, d)-периодической при любом d.

2. Если выходная последовательность A(s) приведенного полноциклового автомата $A = (S, Y, \delta, \lambda)$ (η, d)-периодична и содержит все элементы из Y, то

$$(|S|, d) \geq \frac{|S|}{C},\ d \geq R_A,$$

где $C = \max(deg\sigma)$, максимум берется по всем подстановкам σ из симметрической группы подстановок на множестве Y, длины циклов которых являются делителями числа |S|, R_A – степень различимости автомата A.

Замечание. Пусть $A = (S, Y, \delta, \lambda)$ – приведенный, полноцикловый автомат со степенью различимости R. Рассмотрим автономный автомат $A^R = (S, Y^{(1)}, \delta^{(1)}, \lambda^{(1)})$, где $Y^{(1)}$ – множество различных выходных R-грамм автомата A, а

$$\delta^{(1)} = \delta^R \text{ и } \lambda^{(1)}(s) = (\lambda(s), \lambda(\delta s), \ldots, \lambda(\delta^{R-1}s)).$$

Легко показывается, что для автомата A^R существует отображение η: $Y^{(1)} \to Y^{(1)}$, при котором его выходная последовательность $A^R(s)$ при любом $s \in S$ (x, 1)-периодична.

Пример 6. Пусть $A = (S, Y, \delta, \lambda)$ – автономный автомат, выходным алфавитом Y которого является некоторая конечная группа G. Состояния $s, s' \in S$ назовем G-неотличимыми, если найдется неединичный элемент $g \in G$, при котором

$$A(s) = y_1, y_2, \ldots, A(s') = y'_1, y'_2, \ldots, y`_j = gy_j, \quad j \in [1, 2, ...).$$

Будем говорить, что автомат A G-приведен, если для любых состояний $s, s' \in S$ из предыдущих равенств вытекает $s = s'$, $g = e$ (e – единица группы G). Из следствия 3 вытекает следующее утверждение. Если для полноциклового приведенного автомата $A = (S, Y, \delta, \lambda)$, где $Y = G$ – некоторая конечная группа,

$$(|G, |S) = 1,$$

то A является G-приведенным автоматом.

Пусть $A_1 = (S_1, Y, h^{(1)}, \lambda^{(1)})$ – полноцикловый автомат, $A_2 = (X, S_2, (h_x^2)_{x\in X})$ – перестановочный, коммутирующий (то есть $h_x^2 h_{x`}^2 = h_{x`}^2 h_x^2$, при любых $x, x` \in X$) автомат без выхода, $Y = X$, а G – некоторая конечная группа и $\lambda: S_1 \times S_2 \to G$ отображение вида

$$\lambda(s_1,s_2) = f(s_1)\cdot\nu(s_2),$$

где $f: S_1 \to G$, $\nu: S_2 \to G$.

11.5. G-приведенность автономного последовательного соединения автоматов

Рассмотрим последовательное соединение $A = A_1 \to A_2$ автоматов A_1, A_2 с выходной функцией λ, $A = A_1 \to A_2 = (S_1 \times S_2, G, \delta, \lambda)$, $\delta(s_1, s_2) = (h^{(1)}(s_1), h^{(2)}_{\lambda^{(1)}_{s_1}} s_2)$, $\lambda(s_1, s_2) = f(s_1)\cdot\nu(s_2)$, умножение $(\cdot)$ – операция в группе G. Автомат A имеет вид, показанный на рис. 11.

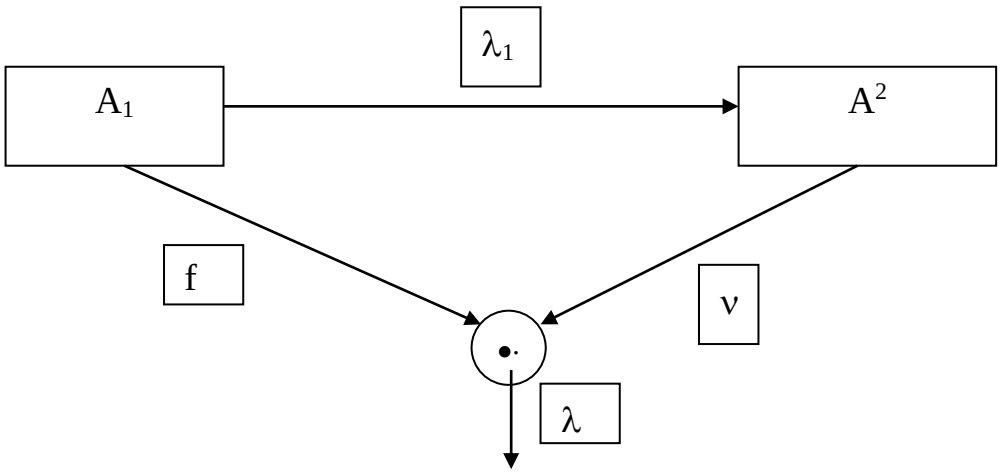

Рис. 11

Обозначим через A_f автономный автомат, отличающийся от A_1 лишь функцией выхода $A_f = (S_1, Y, \delta, f)$, а через $A_\Pi = (S_2, Y, \Pi, \nu)$ – автономный автомат с множеством состояний S_2, функцией перехода

$$\Pi = h^2_{x(|S_1|)} h^2_{x(|S_1|-1)} \ldots h^2_{x(1)},$$

где $A_1(s_1) = x(1), x(2), \ldots, x(|S_1|), \ldots$ – выходная последовательность автомата A_1 от некоторого состояния $s_1 \in S_1$.

Теорема 5. Пусть $A_1 = (S_1, Y, \delta^{(1)}, \lambda^{(1)})$ и $A_2 = (X, S_2, (h_x^2)_{x\in X})$ – перестановочный коммутирующий автомат, Y = X, G – некоторая конечная группа $\lambda: S_1\times S_2 \to G$ отображение вида

$$\lambda(s_1, s_2) = f(s_1)\cdot \nu(s_2),$$

где $f: S_1\to G$, $\nu: S_2\to G$. Пусть также автоматы $A_f = (S_1, Y, \delta, f)$, $A_П = (S_2, Y, П, \nu)$ G-приведенные. Тогда если автомат $A = A_1\to A_2$ полноцикловый, то он G-приведен.

Доказательство. Предположим, что при выполнении условий теоремы автомат A не является G-приведенным. Если рассматривать умножение элементов группы G на элемент $g\in G$ как подстановку на G, то данное предположение эквивалентно существованию g-неотличимых состояний автомата A при некотором $g\in G$. По теореме 2 для автомата A имеем

$$\varphi\delta = \delta\varphi,\ g\lambda = \lambda\varphi,$$

где φ – подстановка на $S_1\times S_2$, индуцируемая отношением g-неотличимости состояний автомата A. Так как A – полноцикловый автомат, то $\varphi = \delta^m$ при некотором натуральном числе m и последние равенства равносильны равенству

$$g\lambda = \lambda\delta^m$$

или

$$g\cdot f(s_1)\cdot \nu(s_2) = f(s_1')\cdot \nu(s_2')$$

где $(s_1, s_2)\in S_1xS_2$, $(s_1', s_2') = \delta^m(s_1, s_2)$.

Используя условия теоремы (в частности, коммутируемость автомата A_2), получаем

$$g\cdot f(s_1)\cdot \nu(П^j s_2) = f(s_1')\cdot \nu(П^j s_2')$$

или

$$f^{-1}(s_1')\cdot g\cdot f(s_1)\cdot \nu(П^j s_2) = \nu(П^j s_2').$$

Из G-приведенности автомата A_2 имеем

$$s_2' = s_2,\ f^{-1}(s_1')\cdot g\cdot f(s_1) = e,\ s_1\in S_1,$$

где e – единица G. Использование теперь G-приведенности автомата A_f дает

$$s_1 = s_1',\ g = e.$$

Таким образом, g = e, $(s_1, s_2) = (s_1', s_2')$, то есть автомат A G-приведен.

Аналогичным образом доказывается теорема 6.

Теорема 6. Пусть $A_1 = (S_1, Y, \delta^{(1)}, \lambda^{(1)})$ – полноцикловый автомат, $A_2 = (X, S_2, (h_x^2)_{x\in X})$ – перестановочный коммутирующий автомат, Y = X, G – некоторая конечная группа $\lambda: S_1\times S_2 \to G$ – отображение вида

$$\lambda(s_1, s_2) = \nu(s_2),$$

где ν: $S_2 \to G$.

Пусть также автомат $A = A_1 \to A_2$ – полноцикловый, автомат $A_П = (S_2, Y, П, \nu)$ – G-приведенный и автомат $A' = (S_1 \times S_2, S_2, \delta, \lambda')$, отличающийся от A лишь функцией выхода λ', $\lambda'(s_1, s_2) = s_2$, $(s_1, s_2) \in S_1 \times S_2$), – приведенный. Тогда автомат A G-приведен.

Глава 12. СИЛЬНО ПРИВЕДЕННЫЕ АВТОМАТЫ

В разделе вводится понятие сильной приведенности автомата, качественно отражающее факт получения различных выходных последовательностей автомата с его начальных состояний при любой входной периодической последовательности. Дается описание перестановочных сильно приведенных автоматов.

Рассмотрим последовательное соединение $B \to A$ автономного перестановочного автомата B с неавтономным перестановочным автоматом $A=(X,S,Y,(h_x)_{x\in X},(f_x)_{x\in X})$.

Состояния $s,s` \in S$ автомата A назовем *неотличимыми относительно автомата B*, если существует состояние t автомата B, при котором выходные последовательности $(B \to A)(t,s)$ и $(B \to A)(t,s`)$ автомата $B \to A$ с начальных состояний (t,s) и (t,s`) совпадают. В противном случае состояния $s, s` \in S$ автомата A назовем *различимыми относительно автомата B*. Рассматриваемая задача состоит в описании автоматов $(B \to A)$, для которых каждая пара различных состояний s, s` автомата A различима относительно B.

Автомат A назовем *ω-приведенным*, если при каждой входной периодической последовательности $\mathfrak{I}$ периода $\omega(\mathfrak{I}) \le \omega$ из равенства $A(s, \mathfrak{I}) = A(s` \mathfrak{I})$ следует, что s = s`. Такие ω-приведенные автоматы A обеспечивают отсутствие различных неотличимых состояний относительно автомата B при любом перестановочном автономном автомате B с множеством состояний S^B, $|S^B| \le \omega$.

Ниже дается описание ω-приведенных перестановочных автоматов и так называемых *сильно приведенных перестановочных автоматов, то есть ω-приведенных перестановочных автоматов при любом ω.*

Предварительно напомним необходимое нам понятие теории автоматов. Автоматом (системой) с конечной памятью [16] называется автомат $A = (X, S, Y, (h_x)_{x\in X}, (f_x)_{x\in X})$, для которого существует функция φ вида φ: $X^{N_1} \times Y^{N_2-1} \to Y$, для которой при любой входной последовательности $\mathfrak{I} = x_1, x_2, \ldots, x_j, \ldots$ и любого начального состояния $s \in S$ для $A (s, \mathfrak{I}) = y_1, y_2, \ldots, y_j, \ldots$ выполняются равенства

$$y_j = \varphi(x_j,...,x_{j-N_1}, y_{j-1},...,y_{j-N_2}).$$

Теорема. Приведенный перестановочный автомат является сильно приведенным автоматом тогда и только тогда, если он с конечной памятью.

Доказательство теоремы проведем с помощью приводимых ниже утверждений.

Лемма 1. Пусть $\omega \geq \frac{1}{2}|S|(|S|-1)$. Тогда ω-приведенный перестановочный автомат A = (X, S, Y, $(h_x)_{x\in X}$, $(f_x)_{x\in X}$) является автоматом с конечной памятью.

Доказательство. Предположим, что некоторый перестановочный ω-приведенный автомат A не является автоматом с конечной памятью. Тогда для любого $c>1$ существуют входная последовательность $\mathfrak{I} = x_1, \ldots, x_C$ и s, s` ∈ S, для которых

$$A(s, x_1, x_2, ..., x_{C-1}, s) = A(s', x_1, x_2, ..., x_{C-1}),$$

$$A(s, \mathfrak{I}) \neq A(s`, \mathfrak{I}).$$

Из этого условия, в частности, следует, что s≠s`. Положим $C-1 \geq \frac{1}{2}|S|(|S|-1)+1$, и рассмотрим последовательности состояний, отвечающие начальным состояниям s, s` и входному слову $\mathfrak{I}]_{C-1} = x_1, ..., x_{C-1}$ автомата A

$$A_M(s, \mathfrak{I}_{C-1})] = s_1, s_2, ..., s_C, \ s_1 = s,$$

$$A_M(s', \mathfrak{I}_{C-1})] = s'_1, s'_2, ..., s'_C, \ s'_1 = s'.$$

Из условий перестановочности автомата A, а так же $s \neq s'$, и выбора C следует существование $j, r \in \left\{\{1, ..., \frac{1}{2}|S|(|S|-1)+1\right\}$, j < r, при которых $s_j = s_r$, $s'_j = s'_r$ либо $s_j = s'_r$, $s'_j = s_r$. Тогда для последовательности $\tilde{\mathfrak{I}} = x_j, x_{j+1}, ..., x_{r-1}, x_j, ..., x_{r-1}, ...$ периода, не превосходящего ω, имеем

$$A(s_j, \tilde{\mathfrak{I}}) = A(s'_j, \tilde{\mathfrak{I}}),$$

при этом $s_j \neq s'_j$, так как, во-первых, $s \neq s'$ и, во-вторых, A – перестановочный автомат. Полученное противоречие опровергает начальное предположение.

Используя последнюю часть доказательства данной леммы, несложно получить утверждение.

Утверждение. Если перестановочный автомат A является ω-приведенный при $\omega \geq \frac{1}{2}|S|(|S|-1)$, то он является ω`-приведенным при любом ω`.

Лемма 2. Если перестановочный приведенный автомат A не является ω-приведенным для некоторого ω, то A не является автоматом с конечной памятью.

Доказательство. Предположим, что для автомата A = (X, S, Y, $(h_x)_{x\in X}$, $(f_x)_{x\in X}$) выполнены условия леммы, и A – автомат с конечной памятью N.

Пусть $\Im = x_1, x_2, \ldots$ – входная последовательность периода ω, а $s \neq s'$ – состояния автомата A, при которых

$$A(s, \Im) = A(s', \Im).$$

Тогда, как нетрудно видеть, различные состояния $h_{x_N} h_{x_{N-1}} \ldots h_{x_1} s$, $h_{x_N} \ldots h_{x_1} s'$ неотличимы, что противоречит приведенности A.

Из приведенных утверждений непосредственно вытекает справедливость сформулированной теоремы.

Таким образом, задача описания автоматов B→A, для которых каждая пара различных состояний s, s` автомата A различима относительно B, частично свелась к описанию приведенных перестановочных автоматов с конечной памятью.

Как известно, автомат A = (X, S, Y, $(h_x)_{x\in X}$, $(f_x)_{x\in X}$) с конечной памятью имеет соотношение вход-выход [16. – С. 212–215] вида $y_j = \varphi(x_j, \ldots, x_{j-N_1}, y_{j-1}, \ldots, y_{j-N_2})$, где φ – функция, а N_1 и N_2 – памяти X и Y автомата A.

Обычное (стандартное) задание системы с данным соотношением вход-выход дается следующим образом. Это автомат $A'' = (X, S'', Y, (h''_x)_{x\in X}, (f''_x)_{x\in X})$, у которого $S'' = X^{N_1} \times Y^{N_2}$,

$$h''_{x_j}(x_{j-1}, \ldots, x_{j-N_1}, y_{j-1}, \ldots, y_{j-N_2}) = (x_j, x_{j-1}, \ldots, x_{j-N_1+1}, y_j, y_{j-1}, \ldots, y_{j-N_2+1}),$$

где

$$y_j = \varphi(x_j, x_{j-1}, \ldots, x_{j-N_1}, y_{j-1}, \ldots, y_{j-N_2}),$$

а

$$f''_{x_j}(x_{j-1}, \ldots, x_{j-N_1}, y_{j-1}, \ldots, y_{j-N_2}) = \varphi(x_j, \ldots, x_{j-N_1}, y_{j-1}, \ldots, y_{j-N_2}).$$

Простейший анализ биективности отображений $(h''_x)_{x\in X}$ (перестановочности автомата A'',$(|X| \geq 2)$ показывает, что автомат A'' является перестановочным лишь при выполнении следующих условий: 1) $N_1 = 0$; 2) функция φ: $X \times Y^{N_2} \to Y$ $(\varphi(x, y_{N_2}, \ldots, y_1))$ биективна по последней переменной y_1.

Схематично они могут быть представлены в следующем виде (рис. 12).

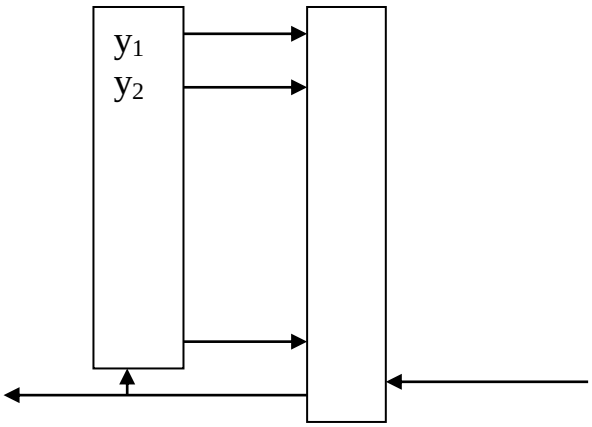

Рис. 12

Следовательно, искомые нами автоматы, заданные в форме A'', исчерпывается регистрами сдвига, являющимися перестановочными автоматами.

Глава 13. ОБ ОДНОМ ПОДХОДЕ К ЛИНЕАРИЗАЦИИ УРАВНЕНИЙ ПОЛУЧЕНИЯ ВЫХОДНОЙ ПОСЛЕДОВАТЕЛЬНОСТИ ВЕКТОРНОГО АВТОМАТА

Проводится линеаризация системы уравнений, описывающих выходное слово векторного автомата при известном входном слове. Эта процедура осуществляется с помощью построения изоморфизма заданного автомата в другой автомат, в котором образ исследуемой системы уравнений становится линейным. Показано, что трудоемкость построения такого изоморфизма совпадает с трудоемкостью решения исследуемой начальной системы уравнений с точностью до трудоемкости решения системы линейных уравнений. Ниже используются результаты работы [9].

13.1. $\mathfrak{I}$-размерность векторного автомата, $\mathfrak{I}$-линейная размерность

Пусть $A = (X, S, Y, h, f)$ – векторный автомат с входным алфавитом X, множеством состояний $S = V_n$, являющимся векторным пространством размерности n над полем $GF(q)$ из q элементов, выходным алфавитом Y, частичными функциями перехода h_x $S \to S$, $x \in X$ и частичными функциями выходов f_x: $S \to Y$, $x \in X$.

Будем говорить, что, семейство отображений β_j: $V_n \to V_n$, $j \in \{1, \ldots, k\}$ независимо, а отображения β_j, $j \in \{1, \ldots, k\}$ – *независимы*, если для любого $c \in \{1, \ldots, k\}$ число решений системы уравнений

$\beta_1(s) = y_1$,

$\beta_2(s) = y_2$,

……

$\beta_c(s) = y_c$, $s \in V_n$, $y_i \in GF(q)$, $i \in \{1, \ldots, c\}$.

не зависит от набора $y_1, y_2, \ldots, y_c$ правой части системы.

Пусть $A = (X, S, Y, (h_x)_{x \in X}, (f_x)_{x \in X})$ – конечный автомат с входным алфавитом X, множеством состояний $S = V_n$, являющимся векторным пространством размерности n над полем $GF(q)$ из q элементов, выходным алфавитом $Y = GF(q)$, частичными функциями переходов $(h_x)_{x \in X}$ и выходов $(f_x)_{x \in X}$, h_x: $S \to S$, f_x: $S \to Y$. Обозначим через $\mathfrak{I} = x_1, x_2, \ldots$ входную последовательность автомата A.

Определение 1. Максимальное число r, при котором функции

$$f_{x_1}, f_{x_2} h_{x_1}, \ldots, f_{x_r} h_{x_{r-1}} \ldots h_{x_1}$$

независимы, называется $\mathfrak{I}$-размерностью $r^A(\mathfrak{I})$-векторного автомата A.

Заметим, что $r^A(\mathfrak{I}) = 0$ тогда и только тогда, когда f_{x_1} – неравновероятная функция на V_n.

Очевидны следующие утверждения:

1) $r^A(\mathfrak{I}) \le n$;

2) $r^A(\mathfrak{I}) = n$ тогда и только тогда, когда семейство функций

$$f_{x_1}, f_{x_2}h_{x_1}, \ldots, f_{x_n}h_{x_{n-1}}\ldots h_{x_1}$$

алгебраически независимо;

3) если φ изоморфизм (по состояниям) векторных автоматов A и φ(A), то $r^A(\mathfrak{I}) = r^{\varphi(A)}(\mathfrak{I})$;

4) любое семейство $k < n$ независимых функций $\beta_1, \beta_2, \ldots, \beta_k$: $V_n \to GF(q)$ можно дополнить до алгебраически независимых функций.

Определение 2. $\mathfrak{I}$-линейной размерностью $L^A(\mathfrak{I})$ векторного автомата A называется число, равное 0, если f_{x_1} является нелинейной функцией, и равное максимальному числу L, при котором функции f_{x_1}, $f_{x_2}h_{x_1}, \ldots,$ $f_{x_L}h_{x_{L-1}}\ldots h_{x_1}$ линейны и линейно независимы.

13.2. Определение начального состояния векторного автомата A по его входной и выходной последовательностям

Теорема. Пусть A – векторный автомат $\mathfrak{I}$-размерности $r^A(\bar{x})$. Тогда существует изоморфный ему автомат φ(A) такой, что

$$r^A(\mathfrak{I}) = L^{\varphi(A)}(\mathfrak{I}).$$

Доказательство. Очевидно, можно считать, что $r^A(\mathfrak{I}) > 0$. Если $r = r^A(\mathfrak{I}) < n$, то семейство функций $f_{x_1}, f_{x_2}h_{x_1}, \ldots, f_{x_r}h_{x_{r-1}}\ldots h_{x_1}$ дополним (см. утверждение 4) до семейства n алгебраически независимых функций $f_{x_1}, f_{x_2}h_{x_1}, \ldots, f_{x_r}h_{x_{r-1}}\ldots h_{x_1}, \beta_{r+1}, \ldots, \beta_n$. Обозначим через Φ отображение $V_n \to V_n$ вида

$$\Phi(s) = (f_{x_1}(s), f_{x_2}h_{x_1}(s), \ldots, f_{x_r}h_{x_{r-1}}\ldots h_{x_1}(s), \beta_{r+1}(s), \ldots, \beta_n(s)),\ s \in V_n,$$

а через Q – линейное невырожденное отображение $V_n \to V_n$: $Q(s) = (g_1(s), g_2(s), \ldots, g_n(s))$. Рассмотрим автомат

$$A' = (X, S, Y, (Q^{-1}\Phi h_x \Phi^{-1}Q)_{x\in X}, (f_x\Phi^{-1}Q)_{x\in X}).$$

Здесь $S = V_n$, $Y = GF(q)$, $(Q^{-1}\Phi h_x\Phi^{-1}Q)_{x\in X}$ – частичные функции переходов автомата A', а $(f_x\Phi^{-1}Q)_{x\in X}$ – его частичные функции выходов.

Непосредственная проверка показывает, что отображение $Q^{-1}\Phi$: $V_n \rightarrow V_n$ осуществляет изоморфизм по состояниям автомата A в A', при этом

$$L^{A'}(\bar{x}) = r^{A}(\bar{x}).$$

Исходя из утверждения данной теоремы, можно предложить следующий метод определения начального состояния векторного автомата A с $r^{A}(\bar{x}) > 0$ по его входной последовательности $\mathfrak{I} = x_1, x_2, \ldots$ и выходной последовательности $y = y_1, y_2, \ldots$.

1. Находится отображение ψ, осуществляющее изоморфизм A в A' автомат с

$$L = L^{A'}(\mathfrak{I}) = r^{A}(\mathfrak{I}).$$

2. С помощью решения системы линейных уравнений определяются все состояния s' автомата A', дающие выходное слово $y = y_1, y_2, \ldots, y_L$ при входном слове $\mathfrak{I} = x_1, x_2, \ldots, x_L$.

3. Проводится опробование состояний из прообразов ψ^{-1}s'состояний s' в автомате A до получения искомого состояния.

Пункт 3 требует нахождения отображения ψ^{-1}, которое, согласно теореме, является обратным к $Q^{-1}\Phi$: $V_n \rightarrow V_n$, осуществляющим изоморфизм ψ. Для его нахождения $\psi^{-1}=\Phi^{-1}Q$, очевидно, необходимо найти Φ^{-1}, то есть уметь решать системы уравнений вида:

$$f_{x_1}(s) = y(1)$$
$$f_{x_2}h_{x_1}(s) = y(2)$$
$$\ldots\ldots\ldots\ldots\ldots$$
$$f_{x_r}h_{x_{r-1}}\ldots h_{x_1}(s) = y(r)$$
$$\beta_{r+1}(s) = y(r+1)$$
$$\ldots\ldots\ldots\ldots\ldots$$
$$\beta_n(s) = y(n)$$

где $y(1), \ldots, y(n) \in Y^n$.

Таким образом, трудоемкость указанного способа определения состояния автомата A, не меньше трудоемкости нахождения решений последней системы уравнений. С другой стороны, доказанная теорема дает возможность из достаточно «простых» автоматов, то есть автоматов A, у которых функции

$$f_{x_1}, f_{x_2}h_{x_1}, \ldots, f_{x_n}h_{x_{n-1}}\ldots h_{x_1}$$

линейны строить изоморфные им автоматы с нелинейными аналогичными функциями, то есть строить «сложные» автоматы с заданными качествами из «простых» автоматов.

Глава 14. ЗАПРЕТЫ АВТОМАТОВ И ДВОИЧНЫХ ФУНКЦИЙ

В этой главе оценивается сверху минимальная длина выходных слов, которые не могут быть получены на выходе заданного автомата. Улучшается известная оценка сверху запрета двоичной функции. (Используются результаты работы [3].)

14.1. Криптографические приложения

Известно (например, [14]), что в науке и технике и, в частности, в различных системах обеспечения безопасности широко применяются генераторы псевдослучайных последовательностей. Так, например, эти генераторы используются в синхронных поточных криптосхемах в качестве управляющих блоков поточных криптосхем.

Основные требования к таким генераторам сформулированы в [1. – С. 247]. Одно из этих требований состоит в том, что последовательность, вырабатываемая генератором, должна иметь большой период. Другое, не менее важное, требование состоит в том, что статистические свойства управляющей гаммы шифрующего блока должны приближаться к свойствам случайной равновероятной последовательности. В частности, последовательности таких генераторов должны содержать любые возможные k-граммы при небольших значениях k. Имеет определенный криптографический смысл решение вопроса о принципиальной возможности получения заданных мультиграмм в выходных последовательностях анализируемых узлов шифраторов или решение обратной задачи о том, какие мультиграммы в принципе не могут быть получены на выходе заданного блока криптосхемы, какова минимальная длина таких мулътиграмм. Так, например, может оказаться, что число различных мультиграмм, снимаемых с управляющих блоков шифратора, которые участвуют в образовании шифра шифрующего блока, мало [1]. Очевидно, это отразится в худшую сторону на криптографической стойкости рассматриваемого шифратора. Исследование поставленных вопросов стимулируется и другими соображениями. Например, зная мультиграммы, которые не могут быть получены с некоторого блока шифратора, можно, при применении ряда методов определения ключей отбраковывать эти мультиграммы, что может повысить эффективность этих методов.

Если моделировать функционирование генераторов автоматами, то, естественно, возникает задача описания автоматов, позволяющих выработать любую конечную последовательность элементов выходного алфавита. Кроме того, представляет интерес задача описания выходных слов автомата, которые невозможно получить с заданного автомата. Прототипом указанных задач является задача изучения запретов кодирующих устройств с конечной памятью без обратной связи (регистров сдвига) или адекватная задача изучения запретов двоичных функций [44, 31].

14.2. Запреты автоматов

В данном пункте исследуются следующие вопросы.

1) Существует ли алгоритм, проверяющий для каждого автомата A, все ли мультиграммы могут быть получены на его выходе?

2) Какова минимальная длина мультиграмм, которые не могут быть получены на выходе заданного автомата A?

Заметим, что ранее в работе [31] поставленные выше вопросы исследовались для весьма узкого класса автоматов, именно для автоматов, представимых проходными линиями задержки. Результаты [31] послужили толчком в решении этих задач в общей постановке для класса конечных автоматов. Следуя определениям работы [31], условимся говорить, что некоторая *мультиграмма является запретной* для автомата A, если она не может быть получена на выходе автомата A. Минимальную длину запретной для автомата A мультиграммы будем называть *длиной запрета автомата A* и обозначать через L(A). Сам автомат A будет называться *автоматом с запретом*, если для него существует запретная мультиграмма. В противном случае A будет называться *автоматом без запрета или автоматом-генератором*.

Пусть $A = (X, S, Y, h, f)$ – конечный автомат с входным алфавитом X, множеством состояний S, выходным алфавитом Y, функциями перехода $h: S\times X\to S$ и выхода $f: S\times X\to Y$, определяемыми соответственно частичными функциями перехода $(h_x)_{x\in X}$ и частичными функциями выхода $(f_x)_{x\in X}$, $h_x: S\to S$, $f_x: S\to Y$. Введем следующие обозначения:

– $|S|$ – мощность множества S;

– 2^S – множество всех подмножеств множества состояний S автомата A, в частности, пустое множество $\varnothing$ и S принадлежат 2^S;

– $my = \{hx(s);\ s \in m,\ m \in 2S,\ fx(s) = y,\ x \in X\},\ y \in Y$;

– $A_S = (Y, 2^S, \delta)$ – автомат без выходов (автомат Медведева) с входным алфавитом Y, множеством состояний 2^S, функцией перехода δ, определенной частичными функциями перехода $(\delta_y)_{y \in Y}$:

$$\delta_y (m) = m^y,\ m \in 2^S,\ y \in Y.$$

Автомат A_S является автоматом, представляющим язык, который перечисляется автоматом А [33. – С. 185, 32, 33]. Легко показывается, что каждой выходной мультиграмме y(1), y(2), ..., y(k), полученной с автомата А при некотором его начальном состоянии $s \in S$, соответствует в графе переходов автомата A_S путь вида

$$m_1 \to^{y(1)} m_2 \to^{y(2)} \ldots \to m_k \to^{y(k)} m_{k+1},$$

где m_1 – любое подмножество множества S, содержащее состояние $s \in S$, а m_j, $j \in [2, k+1]$ – некоторые непустые подмножества из 2^S.

Верно также и обратное, если имеется такой путь в графе переходов автомата A_S, то найдутся состояние $s \in m_1$ и некоторая входная последовательность автомата А, которым соответствует выходная мулътиграмма y(1), y(2), ..., y(k), автомата А.

Кроме того, мультиграмма y`(1), y`(2), ..., y`(k) не может быть получена на выходе автомата А, то есть является запретной для автомата тогда и только тогда, когда в графе переходов автомата A_S существует путь указанного выше вида при $m_1 = S$ и $m_{k+1} = \varnothing$ при некотором k. Точнее говоря, запретные для А мультиграммы однозначно определены путями в графе переходов автомата A_S, ведущими из состояния S в состояние $\varnothing$ (напомним, что $S, \varnothing \in 2^S$). Заметим, что число состояний множества $|2^S|$ автомата A_S равно $2^{|S|}$.

В [26; 19] доказано, что если перечисляющий автомат имеет |S| состояний, то распознающий – не более $2^{|S|}$, причем эта оценка не улучшаема. В [18] доказано, что если язык перечисляется автоматом Мура с |S| состояниями, то он представим в подходящем автомате с $2^{C(|S|)}$ состояниями, где $\frac{C(|S|)}{\frac{|S|}{2}} \to 1$ при $|S| \to \infty$. Поэтому справедлива теорема 1 [45].

Теорема 1. Существует алгоритм, проверяющий, является ли каждый заданный автомат А автоматом с запретом. Если A = (X, S, Y, h, f) – автомат с запретом, то длина его запрета ограничена сверху величиной $2^{|S|} - 1$. Если А – автомат Мура, то длина его запрета

L(A) ограничена сверху величиной $2^{C(|S|)} - 1$, где $\frac{C(|S|)}{\frac{|S|}{2}} \to 1$ при $|S| \to \infty$.

Положим, что $L(m,n,p) = \max\limits_{|X|=m,|S|=n,|Y|=p} L(A)$, где максимум берется по всем конечным автоматам, у которых алфавиты X, S, Y состоят из m, n, p символов соответственно.

В параграфе 6 [24] и А. С. Подколзиным в [28] получен ряд оценок длины запрета автоматов:

1) $L(m,n,p) \le 1 + \left[\frac{\ln n}{\ln p - \ln m}\right]$;

2) если $p \ge n, m \ge p + n - 2$, то $L(m,n,p) = 2^n - 1$;

3) если $p \ge 12, p < n, m \ge p + 16\left[\frac{p-3}{9}\right]^2$, то $L(m,n,p) > 2^n(1 - 2^{1-c})$, где $c = \left[\frac{p-3}{9}\right]$;

4) если $p \ge 3$, $m \ge p+1$, $n - p \to \infty$, то $\frac{2\lg_2 L}{n-p} \to 1$ [28];

5) если $n - p \to \infty$, то $\lg_2 L$ асимптотически не превосходит $\frac{n-p}{2}$ [28].

Определение 1. Состояние s автомата Мили A = (X, S, Y, h, f) называется полным по выходу, если уравнение относительно $x \in X$

$$f_x(s) = y$$

разрешимо при любом $y \in Y$.

Состояние s автомата Мура A = (X, S, Y, h, λ) (λ – выходная функция) называется муровски полным по выходу, если уравнение

$$\lambda h_x(s) = y$$

разрешимо относительно $x \in X$ при любом $y \in Y$.

Определение 2. Состояние s автомата A = (X, S, Y, h, f) называется полным по входу, если система двух уравнений относительно неизвестных $x \in X$, $s` \in S$,

$$h_x(s') = s$$
$$f_x(s') = y$$

разрешима при любом $y \in Y$.

Оба приведенных понятия имеют весьма прозрачную интерпретацию в терминах графа переходов автомата А: полнота по выходу состояния s означает существование ориентированных дуг, исходя-

щих из s, выходные отметки которых составляют весь выходной алфавит Y автомата A. Аналогично интерпретируется и состояние s автомата A, полное по входу. Отличие лишь в том, что теперь надо рассматривать входящие в s-ориентированные дуги. Из данных определений непосредственно вытекает теорема 2.

Теорема 2. Автомат A, у которого все состояния являются одновременно полными по входу или же полными по выходу (муровски полными по выходу), является автоматом без запрета.

Пример 1. Пусть автомат Мура $A = (X, S, Y, h, \lambda)$ представляет собой двоичную проходную линию задержки, то есть $X = Y$ является полем F_2 из двух элементов, S-координатным векторным пространством над полем F_2 размерности n. Частичные функции переходов $(h_x)_{x\in X}$ определены соотношением

$$h_x(x_1, ..., x_n) = (x_2, x_3, ..., x_n, x),$$

где $(x_1, ..., x_n)\in S$, $x_j\in F_2$, а λ – фиксированная функция на S со значениями в F_2, причем переменные x_1, и x_n являются существенными переменными функции λ. Состояния линии задержки A будут муровски полными по выходу тогда и только тогда, когда

$$\lambda(x_1, ..., x_{n-1},0) \neq \lambda(x_1, ..., x_{n-1}, 1)$$

при каждом двоичном наборе $x_1, ..., x_{n-1}$, то есть тогда и только тогда, если переменная x_n входит в двоичную функцию λ линейно. Аналогично показывается, что состояния линии задержки будут полными по входу в том и только в том случае, когда переменная x_1 входит в функцию λ линейно. Таким образом, из теоремы 2 вытекает известное достаточное условие того, чтобы линия задержки A была без запрета. Это условие таково: хотя бы одна из переменных x_1, x_n входит в функцию λ линейно (см. теорему 4 в [31]).

Ниже в данном пункте мы ограничиваемся рассмотрением класса автоматов A с двухбуквенными входным и выходным алфавитами. Обозначим через S_y множество всех состояний автомата $A = (X, S, Y, h, f)$, для которых

$$f_x(s) = y,\ y\in Y,$$

при любом $x\in X$.

Основной результат данного пункта работы составляет теорема 3.

Теорема 3. Если $A = (X, S, Y, h, f)$, $X = Y = F_2$, – автомат с запретом, то длина его запрета ограничена сверху величиной

$$C^{|S_0|}_{|S_0|+|S_1|}\cdot 2^{|S|-|S_0|-|S_1|}.$$

Доказательство. Предварительно докажем ряд вспомогательных лемм.

Лемма 1. Для любого состояния $m \in 2^S$ автомата $A_S = (Y, 2^S, \delta)$ (построенного для $A = (X, S, Y, h, f)$, $X = Y = F_2$) существует $y \in Y$, при котором мощность множества $\delta_y(m)$ не превосходит мощности множества m. Если дополнительно для данного $y \in Y$ выполняется неравенство

$$|m \cap S_{y+1}| - |m \cap S_y| \geq k, \quad k \geq 0,$$

то $|m| - |\delta_y(m)| \geq k$.

Доказательство. Существует $y \in Y = F_2$ при котором мощности пересечений $m \cap S_y$ и $m \cap S_{y+1}$ (+ в поле F_2) удовлетворяют неравенству

$$|m \cap S_y| \leq |m \cap S_{y+1}|.$$

Мощность множества $\delta_y(m)$ не превосходит числа дуг, отмеченных выходным символом $y \in F_2$, идущих из состояний $s \in m$ автомата A, которое, очевидно, равно величине $2|m \cap S_y| + |m| - |m \cap S_y| - |m \cap S_{y+1}|$. Последнее число не превосходит $|m|$. Дополнительное утверждение леммы теперь очевидно.

Обозначим через K_N число состояний $m' \in 2^S$ автомата A_S, для которых

$$|m' \cap S_0| = |m' \cap S_1| \text{ и } |m`| = N.$$

Лемма 2. Пусть A – автомат с запретом. Тогда для любого состояния $m \in 2^S$ в графе переходов автомата A_S существует путь длины не больше $K_{|m|}$, ведущий из состояния m в некоторое состояние строго меньшей мощности.

Доказательство. Предположим, что не существует указанного в лемме 2 пути. Тогда каждый j-й приемник m` [1], $j \in \{1,..., K_{|m|} - 1\}$, состояния m автомата A_S характеризуется соотношением

$$|m' \cap S_0| = |m' \cap S_1|$$

и, как следует из доказательства леммы 1, при этих условиях должно выполняться равенство $|m'| = |m|$. Из этого факта и определения числа $K_{|m|}$ вытекает, что множество всех приемников состояния m совпадает с множеством всех j-х приемников $j \in \{1, ..., K_{|m|}-1\}$. Откуда следует, что не существует пути в графе автомата A_S, ведущего из состояния m в $\varnothing$, что противоречит условию леммы.

Перейдем теперь к доказательству теоремы 2. Утверждение леммы 2 состоит в том, что из любого состояния m в графе переходов автомата A_S существует путь длины, не превосходящей $K_{|m|}$, ведущий из m в состояние строго меньшей мощности. Следовательно,

в том же графе существует путь из состояния S в состояние $\varnothing \in 2^S$ длины, не превосходящей $\sum_{j=1}^{|S|-1} K_j$. Эта величина представляет собой число подмножеств m множества S мощности $|m| \le |S| - 1$, для которых

$$|m' \cap S_0| = |m' \cap S_1| ,$$

Очевидно,

$$\sum_{j=1}^{|S|-1} K_j = 2^{|S|-|S_0|-|S_1|} \sum_{j=0}^{\min(|S_0|,|S_1|)} C_{|S_0|}^{j} C_{|S_1|}^{j} = 2^{|S|-|S_0|-|S_1|} \cdot C_{|S_0|+|S_1|}^{|S_0|} .$$

Здесь использовано равенство (9)

$$\sum_{r=0}^{k} C_{\mathrm{m}}^{\mathrm{r}} C_{n}^{k-r} = C_{n+m}^{k}$$

из задачи 1.18 книги [15]. Теорема 3 полностью доказана.

14.3. Запреты двоичных функций

Двоичную проходную линию задержки (см. пример 1) иногда называют кодирующим устройством (КУ) [44] и определяют как устройство, перерабатывающее произвольную входную двоичную последовательность $x_1, x_2, ..., x_j, ...$ в выходную двоичную последовательность $y_1, y_2, ..., y_j, ...$ по следующему закону:

$$y_j = f(x_j, x_{j+1}, \ldots, x_{j+n-1}),\ j \in \{1, 2, \ldots\},$$

где $f(z_1, \ldots, z_n) = f(z)$ – некоторая двоичная функция от n переменных.

Далее в этом пункте используются следующие предположения: 1) $n \ge 2$; 2) переменные z_1 и z_n были являются существенными переменными в $f(z_1, \ldots, z_n) = f(z)$. Рассмотрим бесконечную систему уравнений, связывающих значения выходной последовательности КУ со значениями входной последовательности:

$$f(x_1, x_2, \ldots, x_n) = y_1,$$
$$f(x_2, x_3, \ldots, x_{n+1}) = y_2,$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$
$$f(x_j, x_{j+1}, \ldots, x_{j+n-1}) = y_j,$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$

Возможны два случая:

1) для любого натурального числа k система уравнений $f(x_j, x_{j+1}, \ldots, x_{j+n-1}) = y_j$, $j \in \{1, 2, \ldots, k\}$,

2) совместна при любых значениях правых частей либо

найдется такое натуральное число k* и такой набор $\left(y_1^*,...,y_{k^*}^*\right)\in F_2^{k^*}$, что система уравнений

$$f(x_j, x_{j+1}, \ldots, x_{j+n-1})=y^*_j,\ j\in\{1, 2, \ldots, k^*\},$$

несовместна, то есть отрезок выходной последовательности $\left(y_1^*,...,y_{k^*}^*\right)$ не может быть получен с помощью данного КУ ни при каких значениях $x_1,x_2,...,x_{k^*+n-1}$.

В первом случае говорят, что функция f(z) не имеет запрета или функция f(z) без запрета. Во втором случае говорят, что функция f(z) имеет запрет или функция f(z) с запретом. При этом k*-грамма $y_1^*, y_2^*, \ldots, y_k^*$ называется запретом функции f(z), а число k* – длиной запрета [31].

Заметим, что если $y_1^*, y_2^*, \ldots, y_m^*$ – запрет функции f(z), то для любой выходной последовательности $y_1, y_2, ..., y_j, ...$, полученной с данного устройства, $(y_{j+1}, \ldots, y_{j+m}) \neq (y_1^*, y_2^*, \ldots, y_m^*)$ при всех натуральных j.

Для формулировки критерия наличия запрета у двоичной функции напомним одно понятие, которое представляет и самостоятельный интерес.

Функция f(z) называется *сильно равновероятной* [31], если для любого натурального числа k и любого набора двоичных переменных $y_1, y_2, \ldots, y_k$ система уравнений

$$f(x_j, x_{j+1}, \ldots, x_{j+n-1}) = y_j,\ j\in\{1, 2, \ldots, k\},$$

имеет ровно 2^{n-1} решений.

14.4. Критерии наличия запрета двоичной функции

В [31] доказано следующее утверждение.

Теорема 4. Функция f(z) не имеет запрета тогда и только тогда, когда она сильно равновероятна.

Кодирующее устройство с функцией $f(z_1,...,z_n)$ называется КУ *с потерей информации* [27], если существуют две входные различные двоичные последовательности $x_1,x_2,...,x_L$ и $x'_1,x'_2,...,x'_L$ одинаковой длины $L\geq 2n-1$, преобразуемые этим устройством в одну и ту же последовательность такие, что их начала длины n–1 совпадают $(x_1,...,x_{n-1})=(x'_1,...,x'_{n-1})$ и совпадают их концы длины n–1 $\left(x_{L-(n-2)},...,x_L\right)=\left(x'_{L-(n-2)},...,x'_L\right)$. В противном случае КУ называется КУ *без потери информации*. Данное понятие впервые ввел Хаффмен [42]; при выполнении первого условия (КУ с потерей информации)

КУ называлось *необратимым***,** в противном случае (КУ без потери информации) – *обратимым***.**

Замечание. В работах [42, 31] приведены равносильные определения КУ с потерей информации (необратимых КУ). В них требовалось наличие различных входных последовательностей с одинаковыми началами и концами длины n.

Теорема 5. Функция f(z) имеет запрет тогда и только тогда, когда кодирующее устройство с этой функцией является кодирующим устройством с потерей информации [31].

14.5. Оценки длины запрета двоичной функции

В теореме 2 работы [31] доказано, что если $n \geq 3$ и для функции $f(z_1, \ldots, z_n)$ существует двоичный набор $y_1^*, \ldots, y_m^*$ длины m, для которого система уравнений

$$f(x_t, x_{t+1}, \ldots, x_{t+n-1}) = y^*_t, \ t \in \{1, 2, \ldots, m\},$$

имеет $2^{n-1} - \alpha$ решений, где $\alpha \geq 1$, то функция $f(z_1, \ldots, z_n)$ имеет запрет длины не более

$$m + 2^n(2^{n-2} - 1)(m + n - 1).$$

Ниже мы приводим и доказываем лучшую оценку длины запрета двоичной функции.

Теорема 6. Если для двоичной функции $f(z_1, \ldots, z_n)$ существует двоичный набор $y_1^*, \ldots, y_m^*$ длины m, для которого система уравнений

$$f(x_t, x_{t+1}, \ldots, x_{t+n-1}) = y^*_t, \ t \in \{1, 2, \ldots, m\},$$

имеет $2^{n-1} - \alpha$ решений, где $\alpha \geq 1$, то функция $f(z_1, \ldots, z_n)$ имеет запретную комбинацию длины

$$m + (n + m - 1)\left[\frac{(n-1) \cdot 2^{n-1} \ln 2}{\alpha}\right],$$

где $[\upsilon]$ – целая часть числа υ. В частности, длина запрета функции $f(z_1, \ldots, z_n)$ не больше

$$m + (n + m - 1)\left[(n-1) \cdot 2^{n-1} \ln 2\right].$$

Доказательство. Рассмотрим все двоичные наборы вида

$$y_1^*, \ldots, y_m^*, y_{m+1}, \ldots, y_{m+n-1}, y_1^*, \ldots, y_m^*, y_{(2m+n-1)+1}, \ldots, y_{2m+2(n-1)},$$

$$\ldots, y_{km+(k-1)(n-1)+1}, \ldots, y_{km+k(n-1)}, y_1^*, \ldots, y_m^*$$

в качестве выходных последовательностей КУ с функцией f(z).

Всего существует $(2^{n-1})^k$ различных наборов данного вида.

Так как прообразы для рассматриваемых наборов имеют длину (k+1)(m+n–1), а их общее число равно $\left(2^{n-1}-\alpha\right)^{k+1}$, то среднее число прообразов для одного набора рассматриваемого вида равно

$$\left(\frac{2^{n-1}-\alpha}{2^{n-1}}\right)^{k}\cdot\left(2^{n-1}-\alpha\right).$$

Найдем $\bar{k}$, при котором эта величина меньше 1, или, что то же самое,

$$\left(1-\frac{\alpha}{2^{n-1}}\right)^{\bar{k}+1}<\frac{1}{2^{n-1}}.$$

При этом $\bar{k}$ функция $f(z_1, \ldots, z_n)$ будет иметь запрет длины

$$\left(\bar{k}+1\right)\cdot m+\bar{k}\cdot(n-1)=m+\bar{k}\left(n+m-1\right).$$

Воспользуемся неравенством $1-x<e^{-x}$ для x > 0.

Имеем

$$\left(1-\frac{\alpha}{2^{n-1}}\right)^{\bar{k}+1}<e^{-\frac{\alpha\left(\bar{k}+1\right)}{2^{n-1}}}.$$

Найдем теперь $\bar{k}$ из неравенства

$$e^{-\frac{\alpha\left(\bar{k}+1\right)}{2^{n-1}}}\le\frac{1}{2^{n-1}}.$$

Логарифмируя обе части неравенства, имеем

$$-\frac{\alpha\left(\bar{k}+1\right)}{2^{n-1}}\le-(n-1)\ln 2,$$

или

$$\bar{k}\ge\frac{(n-1)\cdot 2^{n-1}\ln 2}{\alpha}.$$

Беря теперь в качестве $\bar{k}$

$$\bar{k}=\frac{(n-1)\cdot 2^{n-1}\ln 2}{\alpha},$$

получаем требуемое утверждение теоремы.

Следствие 1. Если двоичная функция $f(z_1, \ldots, z_n)$ неравновероятна, то она имеет запрет длины не более

$$1+n\left[(n-1)\cdot 2^{n-1}\ln 2\right].$$

Данная оценка лучше оценки

$$1+n2^{n}(2^{n-2}-1),$$

приведенной в следствии теоремы 2 работы [31].

Теорема 7. Если двоичная функция $f(z_1, \ldots, z_n)$ имеет запрет, то его длина не больше

$$\left(2^{n-2}\left(2^{n-1}-1\right)+1\right)\cdot n\cdot(\left[(n-1)\cdot 2^{n-1}\ln 2\right]+1)+n^2-n+1,$$

где $[\nu]$ – целая часть числа ν.

Доказательство. Пусть $\gamma(f,k)$ – максимальное по всем возможным наборам $y_1, \ldots, y_k$ число решений системы уравнений

$$f\left(x_j, x_{j+1}, \ldots, x_{j+n-1}\right) = y_j, \quad j \in \{1, \ldots, k\}.$$

Докажем сначала вспомогательную лемму.

Лемма 4. Если двоичная функция $f(z_1, \ldots, z_n)$ имеет запрет, то существует такое $L \le \frac{2^{n-1}\left(2^{n-1}-1\right)}{2} + n$, что

$$\gamma\left(f, L\cdot k - (n-1)\right) \ge 2^k$$

при всех $k \in \{1, 2, \ldots\}$.

Доказательство. Сначала докажем наличие для КУ с функцией f и потерей информации различных входных последовательностей с одинаковыми началами и концами длины n–1 перерабатывающихся в КУ в одну и ту же выходную последовательность длины L–(n–l), где

$$L \le \frac{2^{n-1}\left(2^{n-1}-1\right)}{2} + n.$$

По теореме 5 КУ с функцией, имеющей запрет, является КУ с потерей информации. Среди всех пар входных последовательностей с одинаковыми началами и концами длины n–1, перерабатываемых КУ в одну и ту же выходную последовательность, выберем пару $(x_1, \ldots, x_L)$ и $(x'_1, \ldots, x'_L)$ с минимальной длиной $L \ge 2n-1$.

Рассмотрим для выбранной пары последовательностей последовательности их (n–1)-грамм

$$\tilde{x}_1, \tilde{x}_2, \ldots, \tilde{x}_{L-n+1}, \tilde{x}_{L-n+2} \; u \; \tilde{x}'_1, \tilde{x}'_2, \ldots, \tilde{x}'_{L-n+1}, \tilde{x}'_{L-n+2},$$
$$\left(\tilde{x}_1 = \tilde{x}'_1, \; \tilde{x}_{L-n+2} = \tilde{x}'_{L-n+2}\right)$$

где

$$\tilde{x}_j = x_j, x_{j+1}, \ldots, x_{j+n-2}, \quad \tilde{x}'_j = x'_j, x`_{j+1}, \ldots, x`_{j+n-2}, \quad j \in \{1, \ldots, \text{L-n}+2\}.$$

Так как выбранные последовательности перерабатываются КУ в одну и ту же выходную последовательность и имеют минимальную длину, то имеем:

1) $\tilde{x}_j \ne \tilde{x}'_j, \quad j \in \{2, \ldots, \text{L-n}+1\}$,

2) $\begin{pmatrix} \tilde{x}_j \\ \tilde{x}'_j \end{pmatrix} \ne \begin{pmatrix} \tilde{x}_k \\ \tilde{x}'_k \end{pmatrix}, \quad j,k \in \{2, \ldots, \text{L-n}+1\}, \quad j \ne k,$

3) $\begin{pmatrix} \tilde{x}_j \\ \tilde{x}'_j \end{pmatrix} \ne \begin{pmatrix} \tilde{x}'_k \\ \tilde{x}_k \end{pmatrix}, \quad j,k \in \{2, \ldots, \text{L-n}+1\}, \quad j \ne k.$

Поэтому исходя из элементарных комбинаторных фактов получаем

$$L-n+2-2\le C^2_{2^{n-1}}=\frac{2^{n-1}\left(2^{n-1}-1\right)}{2},$$

или

$$L\le\frac{2^{n-1}\left(2^{n-1}-1\right)}{2}+n.$$

Лемма 4 доказана.

Продолжим доказательство теоремы 7. Пусть функция f(z) имеет запрет. По лемме 4 имеем

$$\gamma\left(f,Ln-(n-1)\right)\ge 2^n>2^{n-1}$$

при некотором

$$L\le\frac{2^{n-1}\left(2^{n-1}-1\right)}{2}+n.$$

Следовательно, найдется набор двоичных переменных $y_1^*,\dots,y_m^*$ при $m=L\cdot n-(n-1)$, для которого число решений системы уравнений

$$f\left(x_j,x_{j+1},\dots,x_{j+n-1}\right)=y_j^*,\quad j\in\{1,\dots,m\},$$

есть величина $2^{n-1}-\alpha$, где $\alpha\ge 1$. По теореме 6 функция f(z) имеет запретную комбинацию длины

$$m+(n+m-1)\left[\frac{(n-1)2^{n-1}\ln 2}{\alpha}\right]\le L\cdot n-n+1+L\cdot n\left[\frac{(n-1)2^{n-1}\ln 2}{\alpha}\right]\le$$

$$\le\left(\frac{2^{n-1}\left(2^{n-1}-1\right)}{2}+n\right)\cdot n\cdot\left[(n-1)2^{n-1}\ln 2\right]+\left(\frac{2^{n-1}\left(2^{n-1}-1\right)}{2}+n\right)\cdot n-n+1.$$

Последняя величина совпадает с

$$\left(2^{n-2}\left(2^{n-1}-1\right)+1\right)\cdot n\cdot\left(\left[(n-1)\cdot 2^{n-1}\ln 2\right]+1\right)+n^2-n+1,$$

что и требовалось показать.

Теорема 7 оценивает минимальную длину запрета (примерно $n^2 2^{3n}$) произвольной двоичной функции f(z), имеющей запрет в худшем случае. Заметим, что полученная ранее для этого случая оценка имела вид $2^{2^n}-1$ [31. – С. 50].

Глава 15. ВНЕШНЕ ПЕРИОДИЧЕСКИЕ АВТОМАТЫ

15.1. Введение

У авторов А. П. Алферова, А. Ю. Зубова, А. С. Кузьмина, А. В. Черемушкина [1] указано, что для обеспечения криптографической стойкости поточных шифров простой замены их управляющие блоки УБ и шифрующие блоки ШБ должны удовлетворять целому ряду требований, одно из которых состоит в обеспечении больших периодов выходных последовательностей УБ и больших периодов последовательностей шифрпреобразований ШБ. При исследовании этих вопросов в терминах конечных автоматов большое значение будет играть следующее вспомогательное, почти тривиальное утверждение.

Утверждение. Для любых натуральных чисел a, b из условия (a, b) = d следует: существуют *натуральные числа n(1), n(2),* при которых

$$an(1) – bn(2) = d.$$

Ниже описываются автоматы, которые при любом начальном состоянии перерабатывают любую чисто периодическую входную последовательность в выходную чисто периодическую последовательность. Указан алгоритм, проверяющий, обладает ли данный автомат таким свойством. Введены и оценены сверху параметры его сложности.

15.2. Автоматы с L-потерей информации о выходе

Пусть $A = (X, S, Y, (h_x)_{x\in X}, (f_x)_{x\in X})$ – конечный автомат. Напомним следующие обозначения:

– $P(s) = h_P s$ заключительное состояние, полученные в результате подачи входного слова P на автомат A с начальным состоянием $s\in S$;

– $\omega \mid L$ – ω делит L.

Под периодом периодической последовательности далее понимается ее минимальный период.

Определение 1. Автомат A называется автоматом с L-потерей информации о выходе, если существуют входное слово P длины $|P| = L$ $(L\geq 1)$, и состояния $s_1, s_2\in S$, для которых имеют место соотношения

$$A(s_1, P) \neq A(s_2, P),$$

$$P(s_1) = P(s_2),$$

а при любом входном слове длины, меньшей L, не существует состояний с указанным свойством. Очевидно, граф переходов автомата A с L-потерей информации о выходе содержит диаграмму вида (рис. 13).

$$\begin{matrix} s_1 \xrightarrow{P/A(s_1,P)} \\ s_2 \xrightarrow[P/A(s_2,P)]{} \end{matrix} s' = P(s_1) = P(s_2),$$

Рис. 13

где $A(s_1, P) \neq A(s_2, P)$, $|P| = L$.

Определение 2. Автомат A, не являющейся автоматом с L-потерей информации *о выходе* ни при каком L, называется автоматом без потери информации о выходе.

Лемма 1. Пусть A – автомат с L_A-потерей информации о выходе. Тогда

$$L_A \leq \frac{|S|(|S|-1)}{2} + 1.$$

Доказательство. Пусть выполнены условия леммы 1 и P, s_1, s_2 таковы, что

$$P = x_1, x_2, \ldots, x_L; \quad |P| = L = L_A; P(s_1) = P(s_2) = s';$$
$$A(s_1, P) \neq A(s_2, P),$$

при этом очевидно, что

$$f_{x_1} s_1 \neq f_{x_1} s_2$$

и

$$f_{x_j} h_{x_{j-1}} \ldots h_{x_1} s_1 = f_{x_j} h_{x_{j-1}} \ldots h_{x_1} s_2$$

для $j \in \{2, \ldots, L\}$. Более того, легко показывается, что при любом $j \in \{1, \ldots, L-1\}$ состояния $h_{x_j} \ldots h_{x_1} s_1; h_{x_j} \ldots h_{x_1} s_2$ различны. Поэтому для доказательства леммы 1 достаточно показать, что среди множества

$$M = \left\{ h_{x_j} \ldots h_{x_1} s_1, h_{x_j} \ldots h_{x_1} s_2 \right\}_{j \in [1, L-1]}$$

неупорядоченных пар различных состояний нет одинаковых пар. Предположим, что такие пары имеются. Именно пусть, например, для некоторых $k(1) < k(2)$, $k(1)$, $k(2)$ из $\{1, \ldots, L-1\}$ имеют место соотношения

$$h_{x_{k(1)}} \ldots h_{x_1} s_1 = h_{x_{k(2)}} \ldots h_{x_1} s_2,$$
$$h_{x_{k(1)}} \ldots h_{x_1} s_2 = h_{x_{k(2)}} \ldots h_{x_1} s_1.$$

Случай:

$$h_{x_{k(1)}} \ldots h_{x_1} s_1 = h_{x_{k(2)}} \ldots h_{x_1} s_1,$$
$$h_{x_{k(1)}} \ldots h_{x_1} s_2 = h_{x_{k(2)}} \ldots h_{x_1} s_2$$

рассматривается аналогично.

Тогда для входного слова

$$\overline{P} = x_1, x_2, \ldots, x_{k(1)}, x_{k(2)+1}, \ldots, x_L$$

длины L – k(2) + k(1) и состояний s_1, s_2 имеем

$$\overline{P}(s_1) = \overline{P}(s_2),$$
$$A(s_1, \overline{P}) \neq A(s_2, \overline{P}),$$

что противоречит условию леммы 1. Таким образом, лемма 1 доказана.

Лемма 2. Пусть A = (X, S, Y, $(h_x)_{x \in X}$, λ) – автомат Мура с L_A-потерей информации о выходе и $\{N_y : y \in Y\}$ – мощности его классов 1-неотличимых состояний $\left(\sum_{y \in Y} N_y = |S|\right)$. Тогда

$$L_A \leq 1 + \sum_{y \in Y} \frac{N_y (N_{y-1})}{2}.$$

Доказательство. Воспользовавшись обозначениями, введенными при доказательстве леммы 1, и сформулированными там утверждениями, можно заключить, что множество M может быть разбито на классы M_y, $y \in Y$, где M_y представляет собой множество всех пар $(a, b) \in M$, для которых

$$\lambda(a) = \lambda(b) = y.$$

Очевидно,

$$\bigcup_{y \in Y} M_y = M,$$

причем мощности $|M_y|$ классов M_y удовлетворяют следующим оценкам:

$$|M_y| \leq \frac{N_y (N_y - 1)}{2}, \quad y \in Y.$$

Из этих оценок и вытекает утверждение леммы 2.

15.3. Критерий внешней периодичности автомата

Определение 3. Автомат A называется внешне периодическим (внутренне периодическим), если для любой его входной чисто периодической последовательности P и любого его начального состо-

яния $s \in S$ его выходная последовательность A(s, P) (его последовательность состояний) является чисто периодической последовательностью.

Теорема 1. Следующие условия эквивалентны:

1) автомат A является внешне периодическим автоматом;

2) автомат A является автоматом без потери информации о выходе.

Доказательство. Пусть A – внешне периодический автомат с $L = L_A$ – потерей информации о выходе и s_1, s_2, $P = x_1, x_2, ..., x_L$ таковы, что

$$A(s_1, P) \neq A(s_2, P),$$
$$P(s_1) = P(s_2).$$

Тогда для входной периодической последовательности $\overline{x_1}, \overline{x_2}, \ldots, \overline{x_L}, \ldots$ с условиями

$$(\overline{x_1}, \overline{x_2}, \ldots, \overline{x_L}) = (x_1, x_2, ..., x_L) \text{ и } \overline{x_j} = \overline{x_{j+L}}$$

для любого j и последовательности $A(s_1, \overline{x_1}, \overline{x_2}, \ldots, \overline{x_L}, \ldots)$, $A(s_2, \overline{x_1}, \overline{x_2}, \ldots, \overline{x_L}, \ldots)$ – чисто периодические. Кроме того, очевидно, что начиная с номера L+1 знаки таких последовательностей совпадают. Поэтому должны совпадать и их начальные знаки, то есть

$$A(s_1, P) = A(s_2, P),$$

что противоречит начальному допущению. Таким образом, показано, что условие 1 влечет условие 2.

Предположим теперь, что A – не внешне периодический автомат. Пусть $P = x_1, x_2, ..., x_L$, а его входная последовательность имеет вид R = P, P, ..., P, ... (конкатенация слов P). Очевидно, последовательность P – периодическая, некоторого периода $\omega | L$. Пусть s_1 – состояние автомата A, при котором последовательность $A(s_1, R)$ не является чисто периодической. Обозначим через $A_M(s_1, R) = s_1, s_2, ...$ последовательность состояний автомата A, отвечающую входной последовательности R и начальному состоянию $s_1 \in S$. В ее подпоследовательности

$$s_{L+1}, s_{2L+1}, s_{3L+1}, \ldots$$

имеются одинаковые состояния, так как порядок множество состояний S автомата A конечно. Пусть, например,

$$s_{Lr(1)+1} = s_{Lr(2)+1}, \quad r(2) > r(1).$$

Не ограничивая общности доказательства, будем считать, что $r(2) - r(1) > r(1)$.

Положим для краткости

$$(P)^k = \underbrace{P, P, \ldots, P}_{k}.$$

Несложно проверить, что выходная последовательность $A(s_1, R)$ автомата A имеет следующий вид:

$$A(s,R) = A(s_1, (P^{r(1)})), A\left(s_{1+Lr(1)}, (P)^{r(2)-2r(1)}\right), A\left(s_{1+L(r(2)-r(1))}, (P)^{r(1)}\right),$$

$$A\left(s_{1+Lr(1)}, (P)^{r(2)-2r(1)}\right), A\left(s_{1+L(r(2)-r(1))}, (P)^{r(1)}\right), \ldots \quad .$$

Ясно, что

$$A\left(s_1, (P)^{r(1)}\right) \neq A\left(s_{1+L(r(2)-r(1)}, (P)^{r(1)}\right),$$

так как в противном случае последовательность $A(s_1, R)$ была бы чисто периодической последовательностью с периодом

$$\omega \mid L(r(2) - r(1)).$$

Таким образом, установлено, что граф переходов автомата A содержит диаграмму вида (рис. 14).

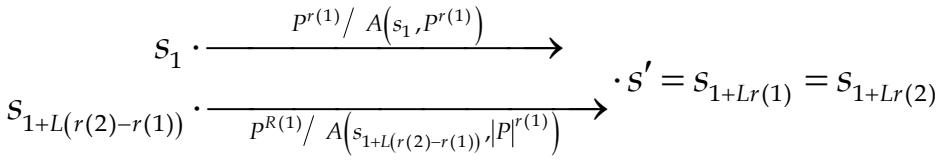

Рис. 14

Следовательно, автомат A является автоматом с L – потерей информации о выходе $L \leq Lr(1)$.

Из теоремы 1 непосредственно вытекает следствие 1.

Следствие 1. Автомат A является внутренне периодическим тогда и только тогда, когда его частичные функции переходов осуществляют биекции S и S, то есть автомат A является перестановочным.

Теорема 2. Автомат A является внешне периодическим тогда и только тогда, когда для любой его чисто периодической входной последовательности P периода

$$\omega \leq \frac{|S|(|S|-1)}{2} + 1$$

и любого состояния $s \in S$ последовательность $A(s, P)$ является чисто периодической последовательностью.

Доказательство. Предположим, что автомат A не является внешне периодическим автоматом. Тогда согласно теореме 1 он является автоматом с L_A-потерей информации о выходе. В первой ча-

сти доказательства теоремы 1 показано, что в этом случае существуют чисто периодическая последовательность P периода $\omega \le L_A$ и состояние $s \in S$, для которых последовательность A(s, P) не является чисто периодической последовательностью. В то же время согласно лемме 1

$$L_A \le \frac{|S|(|S|-1)}{2},$$

откуда и следует утверждение теоремы 2.

Использование леммы 2 для автомата Мура A позволяет аналогично теореме 2 доказать следующее утверждение.

Теорема 3. Автомат Мура A является внешне периодическим автоматом тогда и только тогда, когда для любого $s \in S$ и любой его чисто периодической последовательности P периода

$$\omega \le 1 + \sum_{y \in Y} \frac{N_y (N_y - 1)}{2}$$

(N_y – мощности классов 1-неотличимых состояний) последовательность A(s, P) является чисто периодической последовательностью.

Следствие 2. Существует алгоритм, проверяющий, является ли заданный автомат внешне периодическим автоматом.

Доказательство. Действительно, для автомата Мура A (согласно теореме 2) исследуемых последовательностей A(s, P) при периодической входной последовательности P периода $\omega(P) \le \frac{|S|(|S|-1)}{2} + 1$ и начальном состоянии s, – конечное число. Следовательно, достаточно доказать существование алгоритма, проверяющего, является ли фиксированная последовательность A(s, P) при $\omega(P) \le \frac{|S|(|S|-1)}{2} + 1$, $s \in S$ чисто периодической последовательностью. Существование же его следует из того факта, что приведенная длина исследуемой последовательности A(s, P) ограничена сверху величиной $|S|\omega(P)$ [7].

Глава 16. ПЕРИОДИЧЕСКИ ВНЕШНЕ НАСЛЕДСТВЕННЫЕ ПЕРЕСТАНОВОЧНЫЕ АВТОМАТЫ

В данной главе указаны алгоритмы, проверяющие следующее свойство заданного конечного перестановочного автомата: для любой периодической входной последовательности и любого начального состояния период соответствующей выходной последовательности кратен периоду входной последовательности. Оценены параметры сложности таких алгоритмов.

16.1. Автоматы с L-потерей информации

Пусть $A = (X, S, Y, (h_x)_{x\in X}, (f_x)_{x\in X})$ – конечный автомат.

Через $A(s, P)$ ($A_M(s, P)$) обозначим выходную последовательность автомата A (последовательность его состояний), отвечающую его входной последовательности P и начальному состоянию $s\in S$.

Напомним ряд необходимых нам определений [33; 16].

Определение 1. Состояние $s\in S$ автомата A называется состоянием с *L-потерей информации* (с потерей информации), если существуют различные входные слова x(1), x(2), …, x(L), и x`(1), x`(2), …, x`(L) длины $L = L_s$ $x(j), x`(j)\in X$, для которых выполнены соотношения:

$$h_{x(L)}h_{x(L-1)}...h_{x(1)}s = h_{x`(L)}h_{x`(L-1)}...h_{x`(1)}s, \qquad (13)$$

$$f_{x(1)}s = f_{x`(1)}s$$

$$f_{x(2)}h_{x(1)}s = f_{x`(2)}h_{x`(1)}s$$

.....

$$f_{x(L)}h_{x(L-1)}...h_{x(1)}s = f_{x`(L)}h_{x`(L-1)}...h_{x`(1)}s$$

и не существуют различные входные слова длины, меньшей L_s, с тем же условием.

Если состояние $s\in S$ автомата A не является состоянием с L-потерей информации ни для какого конечного L, то будем говорить, что s есть состояние без потери информации, в противном случае s – состояние с потерей информации.

В графе переходов автомата A состояние s с L-потерей информации характеризуется существованием подграфа вида (рис. 15).

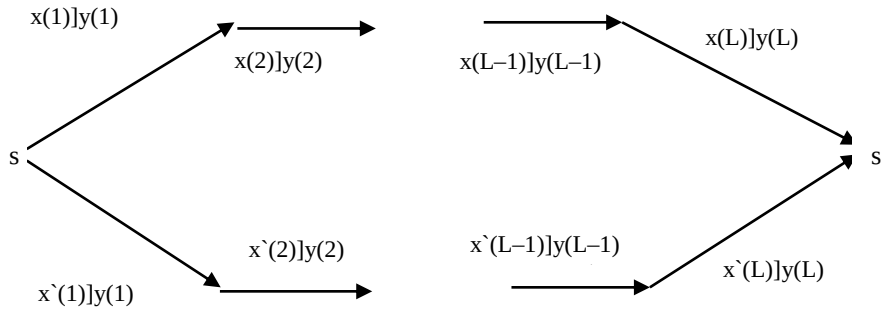

Рис. 15

Определение 2. Автомат A называется автоматом без потери информации, если любое его состояние является состоянием без потери информации. В противном случае автомат A называется автоматом с L-потерей информации, где $L = L_A$ совпадает с минимальным L_s, где минимум берется по всем состояниям $s \in S$ с потерей информации.

Обозначим через N_y, $y \in Y$, мощность множества тех состояний $s \in S$ автомата A, для которых существует элемент $x \in X$, $x = x(s)$ такой, что $f_x s = y$. Справедливо следующее утверждение.

Лемма 1. Пусть A – автомат с L_A-потерей информации. Тогда

$$L_A \le 1 + \frac{|S|(|S|-1)}{2},$$

$$L_A \le 1 + \sum_{y \in Y} \frac{N_y(N_y - 1)}{2}.$$

Доказательство. Пусть $s \in S$ таково, что $L_s = L_A = L$, а x(1), x(2), …, x(L), x`(1), x`(2), …, x`(L), $x(1) \ne x`(1)$ – входные слова автомата A, для которых выполняются соотношения (13).

Положим

$$h_{x(j)} h_{x(j-1)} \ldots h_{x(1)} s = s_j,$$

$$h_{x`(j)} h_{x`(j-1)} \ldots h_{x`(1)} s = s`_j, \quad j \in \{1, \ldots, L-1\}.$$

Очевидно, $s_j \ne s`_j$, $j \in \{1, \ldots, L-1\}$. Покажем, что среди неупорядоченных наборов

$$(s_j, s`_j), \quad j \in \{1, \ldots, L-1\}$$

каждый набор встречается не более одного раза.

Действительно, предположим, например, что для $j(1) < j(2)$

$$s_{j(1)} = s`_{j(2)},$$

$$s`_{j(1)} = s_{j(2)}.$$

Случай $s_{j(1)} = s_{j(2)}$, $s`_{j(1)} = s`_{j(2)}$ рассматривается аналогично. Тогда, очевидно, для входных слов

$$x(1), x(2), ..., x(j(1)), x`(j(2)+1), ..., x`(L),$$
$$x`(1), x`(2), ..., x`(j(1)), x(j(2)+1), ..., x(L), \quad x(1) \neq x`(1)$$

имеем

$$f_{x(1)}s = f_{x`(1)}s;$$
$$.....$$
$$f_{x(j(1))}h_{x(j(1)-1)}...h_{x(1)}s = f_{x`(j(1))}h_{x`(j(1)-1)}...h_{x`(1)}s;$$
$$f_{x`(j(2)+1))}\, h_{x(j(1))}h_{x(j(1)-1)}...h_{x(1)}s = f_{x(j(2)+1))}h_{x`(j(1))}h_{x`(j(1)-1)}...h_{x`(1)}s;$$
$$f_{x`(L)}h_{x`(L-1)}...h_{x`(j(2)+1)}h_{x(j(1))}...h_{x(1)}s = f_{x(L)}h_{x(L-1)}...h_{x(j(2)+1)}h_{x`(j(1))}...h_{x`(1)}s;$$
$$h_{x`(L)}h_{x`(L-1)}...h_{x`(j(2)+1)}h_{x(j(1))}...h_{x(1)}s = h_{x(L)}h_{x(L-1)}...h_{x(j(2)+1)}h_{x`(j(1))}...h_{x`(1)}s.$$

Это противоречит предположению о том, что s является состоянием с L_s-потерей информации при $L_s = L$. Таким образом, среди наборов неупорядоченных пар состояний $(s_j, s`_j)$, $j \in \{1, ..., L-1\}$ нет одинаковых пар. Отсюда, в частности, можно сделать выводы:

1) $L = L_A \leq 1 + \frac{|S|(|S|-1)}{2}$;

2) для любой пары состояний $(s_j, s`_j)$ существует $x \in X$, при котором

$$f_x s_j = f_x s`_j$$

и, следовательно, число этих пар не превосходит величины

$$\sum_{y \in Y} \frac{N_y(N_y - 1)}{2},$$

откуда и следует доказываемая вторая оценка

$$L_A \leq 1 + \sum_{y \in Y} \frac{N_y(N_y - 1)}{2}.$$

16.2. Периодически внешне наследственные автоматы

Далее предполагается, что изучаемый автомат $A = (X, S, Y, (h_x)_{x \in X}, (f_x)_{x \in X})$ *является перестановочным автоматом,* то есть его частичные функции переходов $(h_x)_{x \in X}$ осуществляют взаимно однозначные преобразования множества S.

Если $P = x(1), x(2), ...$ – периодическая последовательность элементов входного алфавита X и s – некоторое состояние автомата A, то через $A_M(s, P) = s, h_{x(1)}s, h_{x(2)}h_{x(1)}s, ...$ будем обозначать последовательность состояний автомата A, отвечающую входной последовательности P и начальному состоянию $s \in S$. Через $A(s, P) = f_{x(1)}s, f_{x(2)}h_{x(1)}s, ...$ будем обозначать выходную последовательность автомата A, отвечающую входной последовательности P и начальному состоянию s.

Пусть $\omega(P)$ – период последовательности P. Известно, что последовательности $A_M(s, P)$, $A(s, P)$ являются периодическими последовательностями (имеется в виду чисто периодическими), периоды которых являются делителями числа $k(s,P) \cdot \omega(P)$, где $k(s, P)$ – минимальное натуральное число k, для которого выполнено условие

$$(h_{x(\omega(P))}h_{x(\omega(P)-1)}...h_{x(1)})^k s = s.$$

Другими словами, $k(s, P)$ – длина цикла подстановки

$$h_{x(\omega(P))}h_{x(\omega(P)-1)}...h_{x(1)},$$

содержащей состояние s.

Кроме того, если перестановочный автомат A является автоматом Мура, то период выходной последовательности $A(s, P)$ делит период последовательности $A_M(s, P)$, что в общем случае для перестановочных автоматов Мили не имеет места.

Введем ряд определений.

Определение 3. Перестановочный автомат A называется периодически внешне наследственным (периодически внутренне наследственным), если для любой периодической входной последовательности P и любого начального состояния s автомата A период выходной последовательности $A(s,P)$ (последовательности состояний $A_M(s,P)$ автомата A) кратен периоду входной последовательности P.

Определение 4. Перестановочный автомат $A = (X, S, Y, (h_x)_{x\in X}, (f_x)_{x\in X})$ называется внешне консервативным, если для любой входной последовательности P периода $\omega(P)$ и любого начального состояния $s \in S$ период выходной последовательности $A(s, P)$ равен $k(s,P) \cdot \omega(P)$.

Очевидно, что внешне консервативный автомат A является периодически внешне наследственным. Если, кроме того, A – автомат Мура, то он также и периодически внутренне наследственен. Приводимые ниже примеры показывают, что внешне консервативные автоматы существуют.

Пример 1. Пусть $A = (X, S, Y, (h_x)_{x\in X}, (f_x)_{x\in X})$ является перестановочным автоматом, где $Y = X \times S$ и $f_x s = (x, s)$, $(x, s) \in Y$.

Легко проверяется, что данный автомат A является внешне консервативным автоматом.

Пример 2. Пусть перестановочный автомат Мура $A = (X, S, Y, (h_x)_{x\in X}, \lambda)$ является неавтономным регистром сдвига, например, $X = F_2$ – поле из двух элементов, $S = F_2^n$, для $(\varepsilon_n, \varepsilon_{n-1}, ..., \varepsilon_1) \in F_2^n$

$$h_0(\varepsilon_n, \varepsilon_{n-1}, ..., \varepsilon_1) = (\varphi(\varepsilon_n,\varepsilon_{n-1}, ..., \varepsilon_1), \varepsilon_n, \varepsilon_{n-1}, ..., \varepsilon_2)$$

$$h_1(\varepsilon_n, \varepsilon_{n-1}, ..., \varepsilon_1) = (\varphi(\varepsilon_n, \varepsilon_{n-1}, ..., \varepsilon_1)+1, \varepsilon_n, \varepsilon_{n-1}, ..., \varepsilon_2),$$

где сложение + по модулю 2, $\varphi(z_n, z_{n-1}, ..., z_1)$ – двоичная функция вида

$$\varphi(z_n, z_{n-1}, ..., z_1) = \Phi(z_n, z_{n-1}, ..., z_2) + z_1, \quad \Phi: F_2^{n-1} \to F_2$$

$$\lambda(\varepsilon_n, \varepsilon_{n-1}, ..., \varepsilon_1) = \varepsilon_1.$$

Легко проверить, что этот автомат внешне консервативен.

Замечание 1. Пусть $A = A_1 \to A_2 \to ... \to A_k$ – последовательное соединение автоматов $A_1, \ldots, A_k$. Легко видеть, что если автоматы $A_1, ..., A_k$ внешне консервативные (периодически внешне наследственные), то и автомат A внешне консервативен (периодически внешне наследственен).

Из *замечания 1* видно, какую важную роль в вопросах синтеза автоматов с гарантированным периодом выходной последовательности играют внешне консервативные и периодически внешне наследственные автоматы. Однако из их определения не ясно даже, можно ли за конечное число шагов определить, является ли данный автомат внешне консервативным (периодически внешне наследственным). Ранее В. А. Башевым был получен критерий периодически внутренней наследственности автомата, из которого, в частности, следует существование алгоритма для проверки периодически внутренней наследственности автомата. Для перестановочных автоматов критерий формулируется так: для любой периодической входной последовательности P периода $\omega(P)$ перестановочного автомата $A = (X, S, Y, (h_x)_{x\in X}, (f_x)_{x\in X})$ и любого его начального состояния $s\in S$ период последовательности состояний $A_M(s, P)$, отвечающей P и s, кратен $\omega(P)$ тогда и только тогда, когда при любых различных $x, x` \in X$

$$h_x s \neq h_{x`} s,$$

при любом $s\in S$.

Вопрос о существовании алгоритмов для определения внешней наследственности (а также сильной консервативности) до сих пор оставался открытым. В данной части работе показывается существование указанных алгоритмов, и даются верхние оценки параметров их сложности.

Лемма 2. Для перестановочного автомата $A = (X, S, Y, (h_x)_{x\in X}, (f_x)_{x\in X})$ с L_A-потерей информации существуют входная последовательность P периода:

$$\omega(P) \le 2\left(\min\left(\frac{|S|(|S|-1)}{2}, \sum_{y \in Y} \frac{N_y(N_y-1)}{2} \right) + |S| \right)$$

и состояние s, для которых период выходной последовательности A(s, P) не кратен ω(P).

Доказательство. По условию леммы найдется состояние s автомата A с L-потерей информации, где $L = L_s = L_A$, в частности, можно указать два входных слова x(1), x(2), …, x(L) и x`(1), x`(2), …, x`(L), для которых

$f_{x(1)}s = f_{x`(1)}s = y_1$;

$f_{x(2)}h_{x(1)}s = f_{x`(2)}h_{x`(1)}s = y_2$;

.....

$f_{x(L)}h_{x(L-1)}...h_{x(1)}s = f_{x`(L)}h_{x`(L-1)}...h_{x`(1)}s = y_L$;

$h_{x(L)}h_{x(L-1)}...h_{x(1)}s = h_{x`(L)}h_{x`(L-1)}...h_{x`(1)}s = s`$,

где $y_j \in Y$, $j \in \{1, ..., L\}$, причем $x(1) \neq x`(1)$.

Выберем в графе переходов автомата A путь, ведущий из состояния s' в s. Это можно сделать в силу перестановочности автомата A. Пусть это будет путь, отвечающий последовательности состояний

$$s`, h_{x``(1)}s`, h_{x``(2)}h_{x``(1)}s`, ..., h_{x``(m)}...h_{x``(1)}s`,$$

входной последовательности x``(1), x``(2), ..., x``(m) и выходной последовательности $y``_1, y``_2, ..., y``_m$. Очевидно, можно считать, что $m \le |S|-1$. Рассмотрим периодическую последовательность P

$$P = z(1), z(2), z(3), ...,$$

где $z(k) = z(k+2(L+m)$, $k \in \{1, 2, ...\}$ и

$$z(t) = x(t), 1 \le t \le L;$$
$$z(t+L) = x``(t), 1 \le t \le m;$$
$$z(t+L+m) = x`(t), 1 \le t \le L;$$
$$z(t+2L+m) = x``(t), 1 \le t \le m.$$

Тогда последовательность A(s, P) имеет вид

$$A(s, P) = y_1, y_2, ..., y_L, y``_1, y``_2, ..., y``_m, y_1, y_2, ..., y_L, y``_2, ..., y``_m, ...$$

и ее период делится на m+L. Если бы этот период был кратен периоду ω(P) последовательности P, то m+L делилось бы на ω(P), откуда, в частности, следовало бы

$$z(1) = z(m+L+1),$$

то есть x(1) = x`(1), что невозможно в силу выбора последовательностей x(1), x(2), …, x(L) и x`(1), x`(2), …, x`(L).

Согласно лемме 1

$$L = L_A \le 1 + \min\left(\frac{|S|(|S|-1)}{2}, \sum_{y\in Y}\frac{N_y(N_y-1)}{2}\right),$$

поэтому период ω(P) построенной последовательности P оценивается следующим образом:

$$\omega(P) \le 2\left(\min\left(\frac{|S|(|S|-1)}{2}, \sum_{y\in Y}\frac{N_y(N_y-1)}{2}\right)+|S|\right)$$

Замечание 2. Лемма 2 показывает, что периодически внешне наследственный автомат всегда является автоматом без потери информации. Обратное утверждение, вообще говоря, не справедливо. Действительно, рассмотрим автомат Мура $A = (X, S, Y, (h_x)_{x\in X}, \lambda)$, где $X = \{0, 1\}$, $S = \{1, 2, 3, 4\}$, $Y = \{0, 1\}$, а h_0, h_1 – подстановки:

$$h_0 = \begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix},\ h_1 = \begin{pmatrix}1&2&3&4\\4&1&2&3\end{pmatrix},$$

$$\lambda(1) = \lambda(2) = 0,\ \lambda(3) = \lambda(4) = 1.$$

Граф переходов автомата A имеет вид (рис. 16).

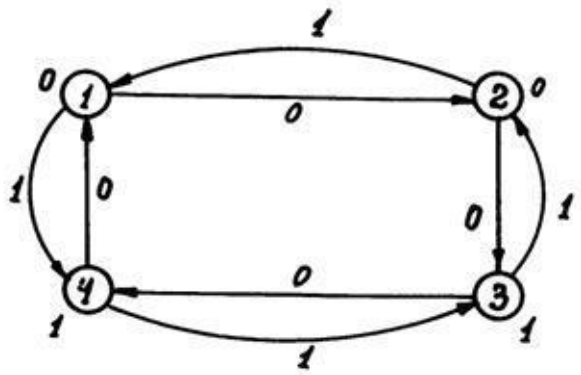

Рис. 16

Очевидно, что данный автомат является перестановочным и непосредственная проверка показывает, что он без потери информации. Тем не менее для входной последовательности X = 0, 1, 0, 1, 0, 1, … периода ω(P) = 2 и начального состояния s = 1 период выходной последовательности A(s, P) равен 1 и, таким образом, не кратен ω(P).

Для автомата $A = (X, S, Y, (h_x)_{x\in X}, (f_x)_{x\in X})$, $|X| \ge 2$, $|Y| \ge 2$ выберем подходящую нумерацию элементов выходного алфавита Y, при которой

$$N_{y^{(1)}} \ge N_{y^{(2)}} \ge \ldots \ge N_{y^{(r)}},\ \ Y = \{y^{(1)}, y^{(2)}, \ldots, y^{(r)}\}.$$

Заметим, что $N_{y^{(j)}} \le |S|$, $j \in \{1, ..., r\}$, и будем предполагать, что $N_{y^{(r)}} \ge 1$, то есть $Y = \bigcup_{x \in X} f_x(S)$.

Лемма 3. Пусть

$$A = (X, S, Y, (h_x)_{x \in X}, (f_x)_{x \in X}), |X| \ge 2, |Y| \ge 2, Y = \bigcup_{x \in X} f_x(S)$$

является перестановочным автоматом без потери информации. Если для любой входной последовательности P периода

$$\omega(P) \le 2N_{y^{(2)}} |S|(|S|-1)(|S|-2)...(|S|-N_{y^{(2)}}+1)$$

и любого начального состояния s автомата A период выходной последовательности A(s, P) кратен периоду ω(P) входной последовательности P, то автомат A является периодически внешне наследственным.

Доказательство. Предположим, что выполнено условие леммы 3, но, тем не менее, существуют периодические входные последовательности и состояния, для которых период соответствующих выходных последовательностей не кратен периодам входных последовательностей. Среди них выберем последовательность P периода ω(P) = ω и состояние $s_1 \in S$, для которых величина $k(s_1, P) \cdot \omega(P)$ минимальна. Пусть последовательность P имеет вид P = x(1), x(2), …, где x(j) = x(j+ω) для любого j. Тогда

$$A_M(s_1, P) = s_1, s_2, ...,$$

где $s_j = h_{x(j-1)}...h_{x(1)}s_1$, $j \in \{2, 3, ...\}$ и

$$A(s_1, P) = y_1, y_2, ...,$$

где $y_j = f_{x(j)}h_{x(j-1)}...h_{x(1)}s_1$, $j \in \{1, 2, ...\}$.

Если W – период последовательности A(s, P), то $W \mid k(s_1, P) \cdot \omega(P)$, то есть для некоторого $L \ge 2$ имеем

$$k(s_1, P) \cdot \omega(P) = k\omega = LW.$$

Оценим сверху величину LW. Для этого покажем, прежде всего, что для любого $j \in \{1, ..., W\}$ состояния

$$s_j, s_{j+W}, ..., s_{j+(L-1)W}$$

попарно различны. Предположим обратное. Пусть для некоторого $j` \in \{1, ..., W\}$ справедливо равенство

$$s_{j`+k(1)W} = s_{j`+k(2)W}, \quad k(1) < k(2), \quad k(1), k(2) \in \{0, 1, ..., L-1\}.$$

Для P = x(1), x(2), ... обозначим последовательность P^j = x(j), x(j+1), ... через P^j.

Возможны два случая:

1) $P^{j`+k(1)W} = P^{j`+k(2)W}$;

2) $P^{j`+k(1)W} \ne P^{j`+k(2)W}$.

Первый случай можно исключить, так как при его выполнении имеем равенство

$$(P^{j`+k(1)W}, s_{j`+k(1)W}) = (P^{j`+k(2)W}, s_{j`+k(2)W}),$$

что равносильно

$$(P, s_1) = (P^{(k(2)-k(1))W+1}, s_{(k(2)-k(1))W+1}),$$

откуда следует, что $(k(2)-k(1))W \geq k\omega$. Последнее неравенство противоречит выбору k(1), k(2).

Во втором случае имеем

$$A(P^{j`+k(1)W}, s_{j`+k(1)W}) = A(P^{j`+k(2)W}, s_{j`+k(2)W}),$$

$$s_{j`+k(1)W+k\omega} = s_{j`+k(1)W} = s_{j`+k(2)W} = s_{j`+k(2)W+k\omega}$$

и автомат A оказывается автоматом с L_A-потерей информации, причем $L_A \leq k\omega$, что противоречит условию леммы 3. Таким образом, для любого $j \in \{0, 1, ..., W\}$ состояния

$$s_j, s_{j+W}, \ldots, s_{j+(L-1)W}$$

попарно различны. Учитывая теперь равенства

$$f_{x(j)}s_j = f_{x(j+W)}s_{j+W} = \ldots = f_{x(j+(L-1)W)}s_{j+(L-1)W},$$

получаем $L \leq N_{y^{(1)}}$. Кроме того, при условии $W \neq 1$ имеем $L \leq N_{y^{(2)}}$.

Для получения оценки сверху величины LW нам остается оценить величину W. Покажем, что

$$W \leq 2|S|(|S|-1)...(|S|-L+1).$$

Для этого, очевидно, достаточно показать, что при $W \geq 3$ среди наборов состояний

$$\begin{pmatrix} s_1 \\ s_{1+W} \\ . \\ . \\ . \\ s_{1+(L-1)W} \end{pmatrix}, \begin{pmatrix} s_2 \\ s_{2+W} \\ . \\ . \\ . \\ s_{2+(L-1)W} \end{pmatrix}, \ldots, \begin{pmatrix} s_W \\ s_{2W} \\ . \\ . \\ . \\ s_{LW} \end{pmatrix}$$

каждый набор встречается не более двух раз.

Допустим обратное. Без ограничения общности будем считать, что первый набор

$$s_1, s_{1+\Omega}, \ldots, s_{1+(L-1)W}$$

встречается, по крайней мере, три раза, то есть существуют k(1), $k(2) \in \{2, 3, ..., W\}$, $k(1) < k(2)$ такие, что

$$s_1 = s_{k(1)} = s_{k(2)}$$

$$s_{1+W} = s_{k(1)+W} = s_{k(2)+W}$$

$$\ldots\ldots\ldots\ldots\ldots\ldots$$

$$s_{1+(L-1)W} = s_{k(1)+(L-1)W} = s_{k(2)+(L-1)W}.$$

Построим вспомогательные периодические последовательности P` и P``.

Последовательность P` определим так:

$$P` = x`(1), x`(2), ..., x`(j), ...,$$

где для любого j

$$x`(j) = x`(j+L(W–k(1)+1))$$

и начальное слово x`(1), x`(2), ..., x`(L(W–k(1)+1)) длины L(W–k(1)+1) последовательности P` имеет вид

x(k(1)), x(k(1)+1), ..., x(k(2)), x(k(2)+1), ..., x(W), x(k(1)+W), x(k(1)+W+1), ..., x(k(2)+W), x(k(2)+W+1), ..., x(2W), ..., x(k(1)+(L–1)W), x(k(1)+(L–1)W+1), ..., x(k(2)+(L–1)W), x(k(2)+(L–1)W+1), ..., x(LW).

Последовательность P`` определим условиями:

$$P`` = x``(1), x``(2), ..., x``(j), ...,$$

где для любого j

$$x``(j) = x`(j+L(W–k(2)+k(1)))$$

и начальное слово x``(1), x``(2), ..., x``(L(W–k(1)+1)) длины L(W–k(2)+k(1)) последовательности P`` имеет вид

x(1), x(2), ..., x(k(1)–1), x(k(2)), x(k(2)+1), ..., x(W), x(W+1), x(W+2), ..., x(k(1)–1+W), x(k(2)+W), x(k(2)+W+1), ..., x(2W), ..., x((L–1)W+1), x((L–1)W+2), ..., x(k(1)–1+(L–1)W), x(k(2)+(L–1)W), x(k(2)+1+(L–1)W), ..., x(LW).

Рассмотрим последовательности $A_M(s_1, P`)$, $A(s_1, P`)$, $A_M(s_1, P``)$, $A(s_1, P``)$. Последовательность $A_M(s_1, P`)$ запишем так:

$$A_M(s_1, P`) = s`_1, s`_2, ..., s`_j, ...,$$

где

$$s`_j = s`_{j+L(W–k(1)+1)}, j \in \{1, 2, ...\}$$

и начальная часть длины L(W–k(1)+1) последовательности $A_M(s_1, P`)$ имеет вид

$$s_1, s_{k(1)+1}, s_{k(1)+2}, \ldots, s_{k(2)}, s_{k(2)+1}, \ldots, s_W,$$

$$s_{1+W}, s_{1+k(1)+W}, s_{2+k(1)+W}, \ldots, s_{k(2)+W}, s_{1+k(2)+W}, \ldots, s_{2W}, \ldots, s_{1+(L–1)W},$$

$$s_{1+k(1)+(L–1)W}, s_{2+k(1)+(L–1)W}, \ldots, s_{k(2)+(L–1)W}, s_{k(2)+1+(L–1)W}, \ldots, s_{LW}.$$

Последовательность $A(s_1, P`)$ запишем так:

$$A(s_1, P`) = y`_1, y`_2, ...,$$

где

$$y`_j = y`_{j+W–k(1)+1}$$

и начальная часть длины W–k(1)+1 последовательности $A(s_1, P`)$ имеет вид

$$y_{k(1)}, y_{k(1)+1}, \ldots, y_{k(2)}, y_{k(2)+1}, \ldots, y_W.$$

Легко видеть, что

$$k(s_1, P`) \cdot \omega(P`) < k(s_1, P) \cdot \omega(P).$$

Из условия минимальности числа $k(s_1,P) \cdot \omega(P)$ и полученного неравенства следует, что период W` выходной последовательности $A(s_1, P`)$, кратен $\omega(P`)$. Кроме того, очевидно, что $W` \mid W–k(1)+1$ и поэтому $\omega(P`) \mid W-k(1)+1$, откуда следует, что для $m \in \{k(1), k(1)+1, ..., W\}$

$$x(m) = x(m+W) = ... = x(m+(L–1)W). \qquad (14)$$

Рассмотрим вторую последовательность P`` и соответствующие ей последовательности $A_M(s_1,P``)$, $A(s_1,P``)$. Аналогично показывается, что выполняются следующие соотношения

$$x(m) = x(m+W) = \ldots = x(m+(L–1)W), \quad m \in \{1,2, ..., k(1)–1\}. \qquad (15)$$

Выписанные равенства (14), (15) означают кратность величины W периоду ω последовательности P. Полученное противоречие доказывает, что

$$W \le 2|S|(|S|–1)...(|S|–L+1),$$

откуда при $W > 1$ имеем

$$LW \le 2N_{y^{(2)}}|S|(|S|–1)...(|S|–N_{y^{(2)}}+1).$$

Кроме того, легко видеть, что эта оценка справедлива и для $W = 1$. Следовательно,

$$\omega(P) \le 2N_{y^{(2)}}|S|(|S|–1)...(|S|–N_{y^{(2)}}+1).$$

Последняя оценка противоречит условию леммы 3. Таким образом, лемма 3 полностью доказана.

16.3. Критерий внешней наследственности автомата

Из лемм 2 и 3 вытекает теорема 1.

Теорема 1. Перестановочный автомат

$$A = (X, S, Y, (h_x)_{x \in X}, (f_x)_{x \in X}), |X| \ge 2, |Y| \ge 2, Y = \bigcup_{x \in X} f_x(S)$$

является периодически внешне наследственным автоматом тогда и только тогда, если для любого начального состояния s автомата A и любой его входной периодической последовательности P периода $\omega(P)$, не превосходящего максимума следующих двух чисел

$$2N_{y^{(2)}}|S|(|S|–1)...(|S|–N_{y^{(2)}}+1),$$

$$2\left(\min\left(\frac{|S|(|S|–1)}{2}, \sum_{y \in Y}\frac{N_y(N_y–1)}{2}\right)+|S|\right),$$

период выходной последовательности A(s, P) кратен $\omega(P)$.

Следствие 1. Существует алгоритм, проверяющий, является ли данный автомат периодически внешне наследственным.

Лемма 4. Пусть перестановочный автомат

$$A = (X, S, Y, (h_x)_{x\in X}, (f_x)_{x\in X}), |X| \geq 2, |Y| \geq 2, \ Y = \bigcup_{x\in X} f_x(S)$$

является автоматом без потери информации. Если для любой входной периодической последовательности P периода

$$\omega(P) \leq N_{y^{(2)}} |S|(|S|-1)...(|S|-N_{y^{(2)}}+1)$$

и любого начального состояния s автомата A период последовательности A(s, P) равен $k(s, P) \cdot \omega(P)$, то автомат A является внешне консервативным.

Доказательство. Доказательство леммы 4 почти полностью совпадает с доказательством леммы 3. В обозначениях, примененных при доказательстве леммы 3, имеющееся отличие доказательства леммы 4 от леммы 3 состоит в том, что среди наборов

$$\begin{pmatrix} s_j \\ s_{j+W} \\ . \\ . \\ . \\ s_{j+(L-1)W} \end{pmatrix}, j\in\{1, 2, ..., W\}$$

каждый набор встречается не более одного раза (в доказательстве леммы 3 – не более двух раз). Покажем это. Пусть, например,

$$t\in\{2, ..., W\};$$
$$s_1 = s_t;$$
$$s_{1+W} = s_{t+W};$$
$$.....$$
$$s_{1+(L-1)W} = s_{t+(L-1)W}.$$

Построим вспомогательную последовательность P^:

$$P^\wedge = x^\wedge(1), x^\wedge(2), ..., x^\wedge(j), ...,$$

где для любого j

$$x^\wedge(j) = x^\wedge(j+L(W-t+1)$$

и начальное слово длины L(W–t+1) последовательности P^ имеет вид

$$x(t), x(t+1), ..., x(W), x(t+W), x(t+1+W), ..., x(2W), ..., x(t+(L-1)W),$$
$$x(t+1+(L-1)W), ..., x(LW) .$$

Тогда последовательности $A_M(s_1, P^\wedge)$, $A(s_1, P^\wedge)$ имеют вид:

$$A_M(s_1, P^\wedge) = s^\wedge_1, s^\wedge_2, ...,$$

где $s^\wedge_j = s^\wedge_{j+L(W-t+1)}$ для любого j и

$s^\wedge_1, s^\wedge_2, \ldots, s^\wedge_{L(W-t+1)} = s_1, s_{1+t}, \ldots, s_W, s_{1+W}, s_{1+t+W}, \ldots, s_{2W}, \ldots, s_{1+(L-1)W}, s_{1+t+(L-1)W}, \ldots, s_{LW},$

а $A(s_1, P^\wedge) = y^\wedge_1, y^\wedge_2, \ldots$, где $y^\wedge_j = y^\wedge_{j+W-t+1}$ для любого j и

$$y^\wedge_1, y^\wedge_2, \ldots, y^\wedge_{W-t+1} = y_t, y_{t+1}, \ldots, y_W.$$

Очевидно, что

$$k(s_1, P^\wedge) \cdot \omega(P^\wedge) < k(s_1, P) \cdot \omega(P).$$

Поэтому, согласно предположению, период $W^\wedge$ последовательности $A(s_1, P^\wedge)$ равен $k(s_1, P^\wedge) \cdot \omega(P^\wedge)$. Так как

$$W^\wedge \mid W-t+1, \text{ то } k(s_1, P^\wedge) \cdot \omega(P^\wedge) \mid W-t+1.$$

Если τ – период последовательности $A_M(s_1, P^\wedge)$, то $\tau \mid k(s_1, P^\wedge) \cdot \omega(P^\wedge)$. Следовательно,

$$\tau \mid W-t+1 .$$

Из последнего соотношения вытекает $s_t = s_{t+W}$, что при $L > 1$ невозможно, как мы убедились ранее. Таким образом, заключаем, что при $L > 1$

$$W \le |S|(|S|-1)\ldots(|S|-L+1).$$

Очевидно, эта оценка справедлива также и при $L = 1$. В остальном доказательство леммы 4 уже полностью совпадает с доказательством леммы 3.

Из лемм 2, 4 непосредственно вытекает теорема 2.

Теорема 2. Перестановочный автомат

$$A = (X, S, Y, (h_x)_{x\in X}, (f_x)_{x\in X}), |X| \ge 2, |Y| \ge 2, \ Y = \bigcup_{x\in X} f_x(S)$$

является внешне консервативным автоматом тогда и только тогда, если для любого начального состояния s автомата A и любой его входной периодической последовательности P периода $\omega(P)$, не превосходящего максимума двух чисел:

$$N_{y^{(2)}} |S|(|S|-1)\ldots(|S|-N_{y^{(2)}}+1);$$

$$2\left(\min\left(\frac{|S|(|S|-1)}{2}, \sum_{y\in Y}\frac{N_y(N_y-1)}{2}\right)+|S|\right),$$

период выходной последовательности $A(s, P)$ равен величине $k(s, P) \cdot \omega(P)$.

Следствие 2. Существует алгоритм, проверяющий, является ли данный перестановочный автомат сильно консервативным.

Глава 17. ПЕРИОДЫ ВЫХОДНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ АВТОМАТА ПРИ ЗАДАННОЙ ПЕРИОДИЧЕСКОЙ ВХОДНОЙ ПОСЛЕДОВАТЕЛЬНОСТИ

В данном разделе оцениваются снизу периоды выходных последовательностей автоматов при заданной входной периодической последовательности.

17.1. Краткий обзор результатов по данной теме. Обозначения, основные понятия, вспомогательные результаты

Основным результатом по оценке снизу периода выходной последовательности конечного автомата, отвечающей его начальному состоянию и входной периодической последовательности, является результат, представленный в теореме 2.2. работы [33], состоящий в том, что минимальный период W выходной последовательности автомата не превосходит величины $|S|\omega$, где $|S|$ – число состояний автомата, а ω – минимальный период входной последовательности. В [13] и [20] приведены утверждения, суть которых состоит в том, что W является делителем числа $k`\omega$ при некотором $k` \le |S|$.

В связи с большой сложностью проблемы оценки снизу периодов выходных последовательностей конечных автоматов при заданных начальных состояниях и входной периодической последовательности естественным подходом к ее удовлетворительному решению является выделение тех или иных классов автоматов в качестве объектов исследований. Например, ряд работ посвящен вопросам периодичности выходных последовательностей линейных автономных автоматов, в частности, в этом классе выделяются работы, в которых указываются способы построения линейных рекуррентных последовательностей максимального периода в разнообразных алгебраических структурах.

В данном разделе используются другие подходы к решению обсуждаемой проблемы. Один из них заключается в установлении связей между наличием факта взаимной простоты периодов входной и выходной последовательности автомата и различными обобщениями понятия автономности автомата.

Основные результаты работы могут быть сформулированы следующим образом.

1. Если приведенный автомат не имеет автономных состояний, то при периодической входной последовательности простого периода P, содержащей на своем периоде все k-граммы входного алфавита автомата для $k > \frac{|S|^2}{2} + \frac{3|S|}{2} - 2$, (|S| – число состояний автомата) период выходной последовательности автомата с любого начального состояния будет кратен P.

2. Класс так называемых перестановочных автоматов состоит из двух подклассов – автоматов с потерей информации и автоматов без потери информации. Автором доказано, что автоматы из первого подкласса таковы, что период выходной последовательности может сократиться по сравнению с периодом входной последовательности в любое число раз. Автоматы из второго подкласса таким свойством не обладают. Именно для любого перестановочного автомата без потери информации при любой входной последовательности P периода ω(P) и любого состояния период выходной последовательности будет не меньше $\frac{\omega(P)}{|S|}$.

Предложенные в данном разделе подходы к получению нижних оценок периодов выходных последовательностей автоматов отличны и от методики расчета мер приближенных периодов выходных последовательностей автомата, предложенной в [8]. Напомним, что в последней работе решена поставленная выше проблема, но для последовательностей состояний автомата и рассчитаны дополнительно меры приближенной периодичности этих последовательностей состояний. В работе [37] ранее был указан широкий класс последовательных соединений автономного автомата с неавтономным автоматом с гарантированным обобщенным периодом выходных последовательностей (G-изопериодом в терминологии автора). Приводимые в данном разделе результаты получены автором под руководством В. А. Башева.

Напомним необходимые нам в данном разделе понятия и обозначения:

Для P = x(1), x(2), …, x(j) …, из X* и $s \in S$ положим

$$s_j = h_{x(j-1)} \ldots h_{x(1)} s_1,\ y_j = f_j\, h_{x(j-1)} \ldots h_{x(1)} s_1.$$

Через h(s, x(1), …, x(к)) обозначим заключительное состояние автомата A с начальным состоянием s при входном слове x(1), …, x(к), то есть

$$h(s, x(1), \ldots, x(к)) = h_{x(к)} h_{x(к-1)} \ldots h_{x(1)} s\ .$$

Напомним, что автомат A называется перестановочным, если $(h_x)_{x\in X}$ – биекции. Автомат A называется приведенным автоматом, если для любых различных состояний s_1, s_2 из S найдется входное слово P (зависящее от s_1, s_2), при котором $A(s_1, P) \neq A(s_2, P)$.

Состояние $s\in S$ автомата A называется *внешне к-автономным*, если $A(s, P) = A(s, P`)$ для любых $P, P`\in X^к$. Состояние $s\in S$ называется *внешне автономным*, если $A(s, P) = A(s, P`)$ для любых сравнимых слов $P, P`\in X^*$. Автомат A называется *внешне к-автономным*, если каждое его состояние внешне к-автономно и *внешне автономным*, если он внешне к-автономен при любом к, то есть каждое его состояние внешне автономно. Несложно доказывается, что автомат Мура внешне автономен тогда и только тогда, если его приведенная форма внутренне автономна, то есть для любого $s\in S$

$$h_{x(k)}\ldots h_{x(2)}h_{x(1)}s = h_{x`(k)}\ldots h_{x`(2)}h_{x`(1)}s$$

при любых сравнимых словах $x(1), \ldots, x(k), x`(1), \ldots, x`(k)$ из X^*.

Напомним, что входная последовательность $P = x(1), \ldots, x(к)$ автомата $A = (X, S, У, h, f)$ называется *установочной* (для A), если для любых $s, s` \in S$ из условия

$$A(s, P) = A(s`, P),$$

вытекает

$$h(s, P) = h(s`, P).$$

Ниже под периодической последовательностью будет пониматься смешанно-периодическая последовательность. Использование ее частного случая – чисто периодической последовательности (смешанно периодической последовательности без подхода) будет оговариваться отдельно. Периодом периодической последовательности P будем называть ее минимальный период.

Слова $(P_1, P_2, \ldots, P_к)\in X^*$ *называются сравнимыми*, если они имеют конечную одинаковую длину или они бесконечные.

В изучении периодов выходных последовательностей автомата при заданной периодической входной последовательности большое значение будут играть следующие понятия.

Определение 1. Система сравнимых входных слов $P_1, P_2, \ldots, P_к$ (возможно, $k = \infty$) автомата $A = (X, S, У, h, f)$ называется слабо неотличимой относительно A (или, кратко, слабо неотличимой), если найдутся состояния $s_1, s_2, \ldots, s_к$ из S, при которых

$$A(s_1, P_1) = A(s_2, P_2) = \ldots = A(s_к, P_к).$$

В противном случае система слов $P_1, P_2, \ldots, P_к$ называется сильно различимой относительно A (сильно различимой).

Определение 2. Автомат A называется слабо k-автономным, если система всех его входных слов длины k слабо неотличима (относительно A).

Определение 3. Степенью слабой автономности $\sigma(A)$ автомата A называется максимальное число k, если оно существует, при котором он слабо k-автономен. В противном случае полагаем $\sigma(A) = \infty$.

Определение 4. Полнотой Q(P) последовательности P = x(1), x(2), …, x(j), … назовем максимальное k, если оно существует, при котором все k-граммы алфавита X содержатся в P. В противном случае полагаем $Q(P) = \infty$.

Ниже мы будем пользоваться следующим утверждением, играющим большую роль в изучении периодичности функционирования конечных автоматов. Для любых натуральных чисел a, b из условия (a, b) = d следует: *существуют натуральные* числа n(1), n(2), при которых

$$an(1) – bn(2) = d.$$

17.2. Периоды выходных последовательностей автомата без внешне автономных состояний при входной периодической последовательности заданной полноты

Через W(s, P) обозначим период выходной последовательности A(s, P) автомата A, полученной с его начального состояния $s \in S$ при входной периодической последовательности P = x(1), x(2), … В дальнейшем удобно представлять периодическую последовательность P в виде конкатенации ZV конечного слова Z = x(1), x(2), …, x(n), являющегося подходом P, и V= x(n+1), x(2), … – ее чисто периодической части. Если P чисто периодическая последовательность, то V – пустое слово. Заметим, что выходная последовательность A(s, P) для произвольного автомата A (даже при чисто периодической последовательности P) вообще говоря смешанно-периодическая.

Теорема 1. Пусть P = ZV входная периодическая последовательность автомата A периода $\omega(P)$.

1. Если $Q(V) > \sigma(A)$, то при любом начальном состоянии $s \in S$ автомата A

$$(\omega(P), W(s, P)) \neq 1.$$

2. Если ω(P) – простое число и V содержит сильно различимую систему сравнимых мультиграмм относительно автомата A, то при любом начальном состоянии $s \in S$ период W(s, P) кратен ω(P).

3. Если A – приведенный автомат Мили без внешне автономных состояний, ω(P) – простое число, $Q(V) > \frac{|S|^2}{2} + \frac{3|S|}{2} - 2$, то при любом начальном состоянии $s \in S$ W(s, P) кратен ω(P).

4. Если A – приведенный автомат Мура без внешне автономных состояний, ω(P) – простое число, $Q(V) > \frac{|S|^2}{2} + \frac{|S|}{2}$, то при любом начальном состоянии $s \in S$ W(s, P) кратен ω(P).

Доказательство. Для P = x(1), x(2), … положим P^j = x(j), x(j+1), … . Через A(s) обозначим связную компоненту автомата A, содержащую состояние $s \in S$. Доказательство теоремы 1 осуществим с помощью следующих вспомогательных трех лемм.

Лемма 1. Пусть P = x(1), x(2), … – входная чисто периодическая последовательность периода ω(P) автомата A = (X, S, Y, h, f). Тогда система сравнимых мультиграмм вида:

P^{kd+1} = x(kd+1), x(kd+2), …, $k \in \{0, 1, \ldots\}$, $P^{(1)}$ = P, d = (ω(P), W(s, P)) (16)

слабо неотличима относительно связной компоненты A(s) автомата A, содержащей состояние $s \in S$.

Доказательство леммы 1. Для произвольного состояния s_1 автомата A рассмотрим выходную (вообще говоря смешанно-периодическую) последовательность $A(s_1, P) = y_1, y_2, \ldots$ и последовательность состояний $A_M(s, P) = s_1, s_2, \ldots$, отвечающих входной последовательности P и начальному состоянию $s_1 \in S$. Легко видеть, что существует t, при котором последовательность $y_t, y_{t+1}, \ldots$ – чисто периодическая и она может быть получена при входной периодической последовательности P, то есть $A(s_t, P) = y_t, y_{t+1}, \ldots$. При этом связная компонента $A(s_t)$ автомата A содержится в компоненте $A(s_1)$. Для доказательства утверждения теоремы достаточно доказать, что множество слов (16) слабо неотличимо относительно связной компоненты $A(s_t)$ автомата A, содержащей состояние $s_t \in S$.

Положим для краткости: $s_t = s$, ω(P) = ω, $W(s_t, P) = W$. При (ω, W) = ω утверждение теоремы очевидно. Предположим, что (ω, W) = d ≠ ω. Пусть k – произвольное число. Существуют натуральные числа n(1), n(2), при которых kn(1)ω – kn(2)W = kd. Имеем

$$A(s, P) = A(s, P^1) = A(s, P^{kd-kd+1}) = A(s, P^{d - kn(1)\omega + kn(2)W+1}) = A(s, P^{kd + kn(2)W+1}). \quad (17)$$

Выберем натуральное число n(3) так, чтобы $\omega|n(2)+n(3)$ и продолжим равенства (17) следующим образом:

$$A(s, P^{kd + kn(2)W+1})=A(h_{x(kd+kn(2)W+n(3)W)}\ldots h_{x(kd+kn(2)W+1)}s, P^{kd+n(2)W+n(3)W+1}) =$$
$$= A(h_{x(kd+n(2)W+n(3)W)}\ldots h_{x(kd+n(2)W+1)}s, P^{kd+1}).$$

Здесь было учтено, что $\omega(P^{kd+1}) = \omega$. Очевидно, состояние

$$s^*_{kd+1} = h_{x(kd+n(2)W+n(3)W)}\ldots h_{x(kd+n(2)W+1)}s$$

принадлежит связной компоненте A(s) автомата A. Таким образом, доказано существование состояний $s^*_1, s^*_{d+1}, \ldots, s^*_{кd+1}$ связной компоненты A(s) автомата A, при которых

$$A(s^*_1, P) =A(s^*_{d+1}, P^{(d+1)}) = \ldots = A(s^*_{кd+1}, P^{(k)d+1)}),$$

что и доказывает лемму 1.

Из леммы 1 вытекает утверждение 2 теоремы 1. В качестве P в условиях леммы надо рассмотреть чисто периодическую часть V последовательности RV.

Теперь нам необходимо выяснить связи понятий слабой к-автономности автомата и его внешне к-автономности. Отметим, что слабая к-автономность автомата A равносильна слабой автономности его приведенной формы, в связи с чем исследование слабо к-автономных автоматов можно проводить, ограничиваясь рассмотрением приведенных автоматов.

Отметим, что для приведенных автоматов всегда существуют установочные последовательности. Обозначим через $L(A)_{уст}$ длину минимальной установочной последовательности для приведенной формы A/~ автомата A.

Обозначим через D(A) – диаметр автомата A, а через d(A) – его степень различимости.

Лемма 2. Слабо к-автономный автомат A при $к \geq L(A)_{уст}+ +D(A)+d(A)+1$ имеет внешне автономное состояние.

Доказательство. Без ограничения общности будем считать, что A = A/~. Покажем сначала, что слабо к-автономный автомат A при $к > L(A)_{уст}$ имеет внешне к-$L(A)_{уст}$-автономное состояние.

Пусть A слабо к-автономен, $к > L$, $L(A)_{уст} = L$. Это означает, что найдутся состояния $s_P \in S$, $P \in X^к$ и его выходное слово $y_1, y_2, \ldots, y_к$ автомата A, при которых

$$A(s_P, P) = y_1, y_2, \ldots, y_к$$

для каждого $P \in X^к$. В частности, для установочной последовательности $R \in X^L$ и произвольных слов $U \in X^{к–L}$ имеем

$$A(s_{RU}, RU) = y_1, y_2, \ldots, y_к , U \in X^{к–L}. \qquad (18)$$

(RU – конкатенация слов R, U).

Так как R – установочная последовательность для A, то найдется $s \in S$, при котором $h(s_{RU}, R) = s$ при всех $U \in X^{к-L}$. Из последних равенств и равенств (18) вытекает

$$A(s, U) = y_{L+1}, y_{L+2}, \ldots, y_к$$

при всех $U \in X^{к-L}$, то есть состояние s внешне (к-L)-автономно.

Пусть теперь $к \geq L(A)_{уст}+D(A)+d(A)+1$ автомат A слабо к-автономный. По доказанному выше A имеет внешне $(к-L(A)_{уст})$-автономное состояние $s \in S$. Из условий леммы следует, что $k`=(к-L(A)_{уст}) \geq D(A)+d(A)+1$. Несложно доказывается, что каждое состояние, достижимое из s является, по крайней мере, внешне (d(A)+1)-автономным. Для доказательства леммы 2 достаточно доказать, что автомат A(s), порожденный состоянием s является внешне автономным.

Итак, пусть автомат A(s) является внешне к-автономным при к = (d(A)+1) и s* – произвольное его состояние, а x(1), x(2), …, x(d+t+1); x`(1), x`(2), …, x`(d+t+1), d = d(A), $t \geq 1$ – произвольная пара его входных слов.

Предположим, что A(s) внешне (d+t)-автономен при некотором натуральном t. В этом случае, очевидно, состояния h(s*, x(1)), h(s*, x`(1)) будут d+t–1-неотличимы и, следовательно, неотличимы. Используя внешне (d+t)-автономность автомата A(s) и неотличимость указанных состояний, получаем

$$f_{x(d+t+1)}h_{x(d+t)}\ldots h_{x(2)}(h_{x(1)}s^*) = f_{x(d+t+1)}h_{x(d+t)}\ldots h_{x(2)}(h_{x`(1)}s^*) =$$
$$= f_{x`(d+t+1)}h_{x`(d+t)}\ldots h_{x`(2)}h_{x`(1)}s^*.$$

Таким образом, доказано, что из внешне d+t-автономности автомата A следует его внешне d+t+1-автономность, $t \geq 1$, откуда и вытекает внешне автономность автомата A(s). Утверждение леммы 2 доказано.

Лемма 3. Для приведенных автоматов A, не имеющих внешне автономных состояний,

$$\sigma(A) \leq \frac{|S|^2}{2} + \frac{3|S|}{2} - 2,$$

если A – автомат Мили и

$$\sigma(A) \leq \frac{|S|^2}{2} + \frac{|S|}{2},$$

если A – автомат Мура.

Доказательство. Т. Х. Хиббардом показано [41], что для любого приведенного автомата Мили

$$L(A)_{уст} \leq \frac{|S|(|S|-1)}{2},$$

а для приведенных автоматов Мура

$$L(A)_{уст} \le \frac{|S|(|S|-1)}{2} - |S|+2,$$

причем эти оценки как функции от числа состояний |S| не могут быть понижены. Известно также (например, [41; 16]), что для любого автомата A

$$D(A) \le |S|-1.$$

Поэтому

$$L(A)_{уст}+D(A)+d(A) \le \frac{|S|(|S|-1)}{2} +2|S|-2$$

для автоматов Мили и

$$L(A)_{уст}+D(A)+d(A) \le \frac{|S|^2}{2}+\frac{|S|}{2}$$

для автоматов Мура. Следовательно, по лемме 2 при $к \ge \frac{|S|(|S|-1)}{2}$ +2|S|–1 слабо к-автономный автомат Мили имеет внешне автономное состояние. По этой причине для автоматов Мили без внешне автономных состояний

$$\sigma(A) \le \frac{|S|^2}{2}+\frac{3|S|}{2}-2.$$

Аналогично показывается, что для автоматов Мура без внешне автономных состояний

$$\sigma(A) \le \frac{|S|^2}{2}+\frac{|S|}{2}.$$

Продолжим доказательство теоремы 1. Докажем теперь утверждение 1 теоремы 1. Пусть P = ZV – входная периодическая последовательность автомата A. Предположим, что существует $s_0 \in S$, при котором $(\omega(P), W(s_0, P)) = 1$. Очевидно, найдется состояние $s \in S$, при котором $W(s, V)) = W(s_0, P))$. По лемме 1 система сравнимых мультиграмм вида

$$V^{k+1}, k \in \{0, 1, \ldots\}, V^1 = V,$$

слабо неотличима относительно связной компоненты A(s) автомата A, содержащей состояние $s \in S$. В частности, автомат A(s) слабо Q(V)-автономен. Поэтому его степень слабой автономности удовлетворяет неравенству

$$\sigma(A(s)) \ge Q(V).$$

Но $\sigma(A) \ge \sigma(A(s)$, в связи с чем $\sigma(A) \ge Q(V)$, что противоречит условию первого утверждения теоремы.

Пусть теперь A – приведенный автомат без внешне автономных состояний, $\omega(P)$ – простое число,

$$Q(V) > \frac{|S|^2}{2} + \frac{3|S|}{2} - 2.$$

Предположим, что $(\omega(P), W(s_0, P)) = 1$. Тогда по первому утверждению теоремы должно выполняться неравенство $\sigma(A) \geq Q(V)$. По лемме 3

$$\frac{|S|^2}{2} + \frac{3|S|}{2} - 2 \geq \sigma(A).$$

Следовательно, $\frac{|S|^2}{2} + \frac{3|S|}{2} - 2 \geq Q(V)$, что противоречит условиям утверждения 3 теоремы 1. Аналогично доказывается четвертое утверждение теоремы 1.

Снизить данные в пунктах 3, 4 ограничения на величину Q(V), понижая приведенные верхние оценки степени слабой автономности автоматов, не удается. Следующие примеры показывают, что для автоматов Мили приведенная в лемме 3 оценка их степени слабой автономности достижима, а для автоматов Мура – почти достижима.

Пример 1. Положим

$$X=\{1, \ldots, |S|\},\ S = \{s^{(1)}, s^{(2)}, \ldots, s^{(|S|)}\},\ Y =\{0, 1\},$$

$$h_x s^{(x)} = s^{(x+1)},\ x \neq |S|;\ h_{|S|} s^{(|S|)} = s^{(|S|)};\ h_x s^{(x+1)} = s^{(x)},\ x \neq |S|;\ h_x s^{(j)} = s^{(j)},\ x \neq j,$$

$$j \neq x+1;$$

$$f_x s^{(j)} = 1 \text{ при } x = j = |S|,\ f_x s^{(j)} = 0 \text{ в противном случае.}$$

Введенный автомат A = (X, S, Y, h, f) является перестановочным автоматом, кроме того, он не имеет внешне автономных состояний. Покажем, что автомат A слабо к-автономен при к = $\frac{|S|^2}{2} + \frac{|S|}{2} - 1$. Пусть слово P = x(1), x(2), …, x(к) таково, что (s(x), P) ≠ 0 (не является словом, состоящим сплошь из нулей) для всех $s^{(x)}$ из S. Для каждой пары (i, j), $1 \leq i \leq j \leq |S|$, очевидно, найдется целое число L = L(i, j), $1 \leq L \leq к$, при котором

$$h_{x(L-1)} h_{x(L-2)} \ldots h_{x(1)} s^{(i)} = s^{(j)} \text{ и } x(L) = j.$$

Здесь мы положили $h_{x(0)} s^{(i)} = s^{(i)}$. Для различных пар (i, j),(i`, j`) величины L(i, j), L(i`, j`) различны. Действительно, если L(i, j) = L(i`, j`), то j = i(L(i, j)) = i`(L(i`, j`)) = j`. Поэтому в силу перестановочности автомата A и i = i`, j = j`.

Таким образом, число различных чисел L(i, j) совпадает с числом различных пар (i, j), $1 \leq i \leq j \leq |S|$, которое, в свою очередь, очевидно, равно $\frac{|S|^2}{2} + \frac{|S|}{2}$. Учитывая, что $L(i, j) \leq к$, имеем

$$к \geq \frac{|S|^2}{2} + \frac{|S|}{2}.$$

Из этой оценки непосредственно вытекает, что для любой последовательности P длины меньшей чем $\frac{|S|^2}{2} + \frac{|S|}{2}$ найдется состояние $s^{(i)} \in S$ автомата A, при котором $A(s^{(i)}, P)$ есть последовательность, состоящая из нулей. Автомат A оказывается по крайней мере слабо к-автономным при

$$к = \frac{|S|^2}{2} + \frac{|S|}{2} - 1.$$

Пример 2. Положим X = {1, 2, …, |S|}, а S, Y, частичные функции переходов $(h_x)_{x \in X}$ определим, как и в примере 1. Кроме того, положим $f_x = \lambda$ для всех $x \in X$. Рассматриваемый автомат A является перестановочным автоматом Мура, без внешне автономных состояний. Аналогично примеру 1 покажем, что автомат A является слабо к-автономным для

$$к = \frac{|S|^2}{2} - \frac{|S|}{2}.$$

Отличие доказательства состоит в том, что множество чисел вида L(i, j) необходимо рассматривать при $1 \leq i \leq j \leq |S|-1$. Число таких пар (i, j) равно $\frac{|S|^2}{2} - \frac{|S|}{2}$. Поэтому $к \geq \frac{|S|^2}{2} - \frac{|S|}{2} + 1$ и, следовательно,

$$\sigma(A) \geq \frac{|S|^2}{2} - \frac{|S|}{2}.$$

Как видно из приведенных общих утверждений оценки параметра σ(A) слабой автономности автоматов в классе автоматов без внешне автономных состояний не могут быть существенно улучшены, например, по порядку. Поэтому, естественно, возникает вопрос, нельзя ли в общем случае оценку σ(A) существенно понизить, если искать ее для почти всех автоматов. Из приведенных результатов и результатов работ [21; 23] по оценкам диаметра D(A), степени различимости d(A) и длины $L(A)_{уст}$ установочного эксперимента следует, что для почти всех приведенных автоматов $A = (X, S, У, h, f_x)$, $|X| \geq 2$, $|У| \geq 2$ без внешне автономных состояний

$$\sigma(A) \leq 5\log_{|Y|}|S| + \frac{1}{6}\log_{|X|}|S|.$$

Для практического использования утверждения теоремы 1 необходимо выделить классы автоматов с небольшой степенью сла-

бой автономности. Поэтому представляет интерес оценки слабой автономности приводимых ниже линейных векторных автоматов.

17.3. Периоды выходных последовательностей линейного векторного автомата при заданной входной периодической последовательности

Далее мы уточним утверждение леммы 3 и утверждения 1, 2 теоремы 1 для некоторых классов линейных автоматов.

Пусть $A = (X, V_n(q)\backslash 0, F_q, (B_x)_{x\in X}, (C_x)_{x\in X})$ – линейный автомат с входным алфавитом X, множеством состояний $V_n(q)\backslash 0$, являющимся векторным пространством $V_n(q)$ над полем F_q с исключенным нулевым вектором, выходным алфавитом F_q, частичными функциями переходов $(B_x)_{x\in X}$, являющимися линейными преобразованиями векторного пространства $V_n(q)$, частичными функциями выхода $(C_x)_{x\in X}$, осуществляющими линейные отображения $V_n(q)$ в F_q.

Лемма 4. Если $s\in V_n(q)\backslash 0$ – внешне к-автономное состояние, $к \geq 2n$ автомата $A = (X, V_n(q)\backslash 0, F_q, (B_x)_{x\in X}, (C_x)_{x\in X})$, то оно внешне автономно.

Доказательство. Рассмотрим систему векторов s:

$$\{B_{x(1)}s: x(1)\in X\},$$
$$\{B_{x(2)}B_{x(1)}s;\ x(2)x(1)\in X^2\},$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \qquad (CB(j))$$
$$\{B_{x(j)}\ldots B_{x(1)}s;\ x(j)\ldots x(1)\in X^j\},$$

ранг которой будем обозначать через r(j).

Легко видеть, что

$$1 \leq r_1 \leq r_2 \leq \ldots \leq r_j \leq r_{j+1}\ldots,$$

кроме того, из $r_j = r_{j+1}$ для некоторого j следует $r_j = r_{j+к}$ при любом $к \geq 0$. Поэтому $r_{n-1} = r_n \leq n$.

Выберем в системе CB(n–1) $r = r_{n-1}$ линейно независимых векторов: $s, s_1, s_2, \ldots, s_{r-1}$. Если теперь предположить, что состояние s внешне к-автономно, $к \geq 2n$, то, очевидно, должны быть внешне (к–n+1)-автономными состояния $s, s_1, s_2, \ldots, s_{r-1}$. Используя свойство линейности автомата, заключаем, что все достижимые из s состояния автомата A внешне (к–n+1)-автономны. То есть, внешне (к–n+1)-автономен автомат A(s), порожденный состоянием s.

Так как степень различимости d(A) любого линейного автомата A не превосходит его размерности n, то степень различимости d(A(s)) его подавтомата A(s) не превосходит n.

Итак, A(s) (к–n+1)-автономен, к ≥ 2n и d(A(s)) ≤ n. Следовательно, A(s) К-автономен при некотором К ≥ d(A(s))+1. Теперь несложно доказать, что из этого факта следует внешне автономность состояния s линейного автомата A.

Напомним, что *диагностической* последовательностью произвольного автомата (X, S, У, h, f) называется любое его входное слово P (если оно существует), при котором для любых s, s`∈S из условия

$$A(s, P) = A(s`, P),$$

вытекает s = s`. Отметим, что диагностическая последовательность автомата является одновременно и установочной. Обозначим через $L(A)_{диаг}$ минимальную длину диагностической последовательности для автомата A.

Легко доказывается, что входное слово x(1), x(2), …, x(к) линейного автомата $A = (X, Vn(q)\backslash 0, F_q, (B_x)_{x\in X}, (C_x)_{x\in X})$ является диагностическим тогда и только тогда, когда ранг системы

$$C_{x(1)}, C_{x(2)}B_{x(1)}, \ldots, C_{x(к)}B_{x(к-1)}\ldots B_{x(1)}$$

линейных функций равен n.

Теорема 2. Пусть $A = (X, V_n(q)\backslash 0, F_q, (B_x)_{x\in X}, (C_x)_{x\in X})$ – линейный автомат без внешне автономных состояний и $L(A)_{диаг} = n$. Тогда $\sigma(A) \le 3n-1$.

Доказательство. Если выполнены условия теоремы и $\sigma(A) \ge 3n$. В начале доказательства леммы 2 было обосновано утверждение, что произвольный слабо к-автономный автомат A при $к > L(A)_{уст}$ имеет внешне к-$L(A)_{уст}$-автономное состояние. Так как в нашем случае $L(A)_{уст} \le n$, то A имеет внешне 2n-автономное состояние $s\in S$ и тогда, по лемме 4 он имеет внешне автономное состояние, что противоречит условию теоремы.

Следствие 1. Пусть $A = (X, V_n(q)\backslash 0, F_q, (B_x)_{x\in X}, (C_x)_{x\in X})$ – линейный автомат без внешне автономных состояний и линейное преобразование B_a, $a\in X$ является полноцикловым преобразованием пространства $V_n(q)$. Тогда

$$\sigma(A) \le 3n-1.$$

Используя утверждения теоремы 2 и следствия 3, с помощью пункта 1, теоремы 1 легко строится класс линейных векторных автоматов периоды выходных последовательностей которых кратны заданному простому числу ω при входных периодических последовательностях P периода ω с полнотой периодических частей, больших 3n–1.

Утверждение 2 теоремы 1 позволяет указать и другие классы линейных векторных автоматов с указанным выше свойством выходных последовательностей. Введем сначала необходимые понятия.

Определение 5. Система сравнимых входных слов P_1, P_2, …, $P_к$ (возможно $k = \infty$) линейного автомата $A = (X, V_n(q)\backslash 0, F_q, (B_x)_{x\in X}, (C_x)_{x\in X})$ называется слабо невырожденно неотличимой относительно A (или, кратко, слабо неотличимой), если найдутся состояния s_1, s_2, …, $s_к$ из S, при которых

$$A(s_1, P_1) = A(s_2, P_2) = \ldots = A(s_к, P_к) \neq 0, \ldots, 0$$

В противном случае система слов P_1, P_2, …, $P_к$ называются сильно невырожденно различимой относительно A (сильно различимой).

Пусть $P_1 = x(1), x(2), \ldots, x(к)$ – входное слово линейного автомата $A = (X, Vn(q)\backslash 0, GF(q), (B_x)_{x\in X}, (C_x)_{x\in X})$. Обозначим через $r(P_1)$ ранг системы векторов

$$C_{x(1)}, C_{x(2)}B_{x(1)}, \ldots, C_{x(к)}B_{x(к-1)}\ldots B_{x(1)},$$

а через $L(A(P_1)$ – множество (пространство) линейных соотношений между векторами этой системы.

Теорема 3. Пусть $P = ZV$ – входная периодическая последовательность автомата $A = (X, V_n(q)\backslash 0, GF(q),(B_x)_{x\in X}, (C_x)_{x\in X})$ простого периода $\omega(P)$, а V содержит диагностическую последовательность автомата A и пару сравнимых слов $P_1 = x(1), x(2), \ldots, x(t)$ и $P_2 = x'(1), x'(2), \ldots, x'(t)$ с условием

$$\mathrm{rang}(L(A(P_1))\cup L(A(P_2))) = t.$$

Тогда при любом s из $V_n(q)\backslash 0$ период $W(s,P)$ кратен $\omega(P)$.

Доказательству теоремы 3 предпошлем две леммы.

Лемма 5. Входные слова $P_1 = x(1), x(2), \ldots, x(t)$ и $P_2 = x'(1), x'(2), \ldots, x'(t)$ линейного автомата $A = (X, V_n(q)\backslash 0, F_q, (B_x)_{x\in X}, (C_x)_{x\in X})$ сильно невырожденно различимы тогда и только тогда, когда

$$\mathrm{rang}(L(A(P_1))\cup L(A(P_2))) = t$$

Доказательство. Рассмотрим системы линейных уравнений

$C_{x(1)}s = y_1$,	$C_{x'(1)}s' = y_1$
$L(P_1, y)$: $C_{x(2)}B_{x(1)}s = y_2$,	$L(P_1, y)$: $C_{x'(2)}B_{x'(1)}s' = y_2$,
…….	…….
$C_{x(t)}B_{x(t-1)}\ldots B_{x(1)}s = y_t$	$C_{x'(t)}B_{x'(t-1)}\ldots B_{x'(1)}s' = y_t$

относительно неизвестных s, s' из $V_n(q)\backslash 0$.

Положим

$$\Delta_y^{P_1} = \begin{matrix} 1, \textit{если система } L(P_1, y) \textit{ совместна} \\ 0, \textit{ в противном случае} \end{matrix}$$

и аналогично

$$\Delta_y^{P_2} = \begin{matrix} 1, \textit{если система } L(P_2, y) \textit{ совместна} \\ 0, \textit{ в противном случае} \end{matrix}$$

Методами линейной алгебры легко получить

$$\sum \Delta_y^{P_1} \Delta_y^{P_2} = q^{t - rang(L(A(P_1)) \bigcup L(A(P_2)))},$$

где сумма взята по всем возможным наборам y = y_1, y_2, …, y_t из F_q^t. Левая часть этого равенства представляет собой число наборов y из F_q^t, при которых одновременно совместны системы L(P_1, y), L(P_2, y). В то же время сильная невырожденная различимость системы слов P_1, P_2 означает в этой терминологии, не что иное как

$$\sum_{y \neq 0} \Delta_y^{P_1} \Delta_y^{P_2} = 0.$$

Таким образом, сильная невырожденная различимость системы слов P_1, P_2 равносильна условию

$$q^{t - rang(L(A(P_1)) \bigcup L(A(P_2)))} = 1,$$

то есть t = rang(L(A(P_1))∪L(A(P_2))).

Лемма 6. Пусть P = ZV входная периодическая последовательность линейного векторного автомата A = (X, $V_n(q)\backslash 0$, F_q, $(B_x)_{x \in X}$, $(C_x)_{x \in X}$) периода ω(P) и V содержит его диагностическую последовательность. Если при некотором s из $V_n(q)\backslash 0$ (W(s, P), ω(P)) = 1, то при к ≥ n все к-граммы последовательности V слабо невырожденно неотличимы относительно автомата A.

Доказательство. По лемме 1 все мультиграммы одинаковой длины слабо неотличимы относительно автомата A. Пусть началом мультиграммы $V^{k(0)}$ является диагностическая последовательность x”(1), x”(2), …, x”(к). Тогда для каждого к найдется s(k) из $V_n(q)\backslash 0$, для которых справедливы равенства

$$A(s_{k(0)}, V^{k(0)}) = A(s_k, V^k).$$

Из диагностичности последовательности x(1), x(2), …, x(к) линейного автомата A = (X, Vn(q)\0, F_q,$(B_x)_{x \in X}$, $(C_x)_{x \in X}$) следует, что ранг системы

$$C_{x”(1)}, C_{x”(2)}B_{x”(1)}, \ldots, C_{x”(к)}B_{x”(к-1)}) \ldots B_{x”(1)}$$

векторов равен n. Поэтому $A(s_{k(0)}, V^{k(0)})$ не является последовательностью, составленной из нулей. Что и требовалось доказать.

Доказательство теоремы 3 очевидно, состоит в прямом применении лемм 1, 5, 6.

Выделим в алфавите X два различных элемента – a и b. Положим $a^к$ = a, a, …, a – слово длины к, состоящее из элементов, равных a. Аналогично $b^к$. Обозначим через $V^*_n(q)$ пространство линейных функций на $V_n(q)$, через B^*_x – линейное преобразование $V^*_n(q)$, сопряженное к B_x, $x \in X$. Через $\chi(x)$ обозначим минимальные многочлены вектора C_x относительно линейного преобразования B^*_x. Из теоремы 3 можно получить следствие 2.

Следствие 2. Пусть P = ZV – входная периодическая последовательность автомата $A = (X, V_n(q)\backslash 0, GF(q), (B_x)_{x\in X}, (C_x)_{x\in X})$ простого периода $\omega(P)$, а V содержит мультиграммы a^t и b^t, причем $\deg \chi(a) = n$, $(\chi(a), \chi(b)) = 1$ и $t \geq \text{degH.O.K.}(\chi(a), \chi(b))$. Тогда при любом s из $V_n(q)\backslash 0$ период $W(s, P)$ кратен $\omega(P)$.

Доказательство. Используем утверждения теоремы 3 и леммы 5. Для доказательства следствия 2 нам достаточно доказать, что, во-первых, V содержит диагностическую последовательность и, во-вторых, система мультиграмм a^t и b^t сильно невырожденно различима, то есть (по лемме 5)

$$\text{rang}(L(A(a^t)) \cup L(A(b^t))) = t.$$

Первое утверждение очевидно, так как из $\deg \chi(a) = n$ следует, что a^t – диагностическая последовательность для A. Второе утверждение сформулируем и докажем в виде отдельной леммы.

Лемма 7. Пусть $t \geq \text{degH.O.K.}(\chi(a), \chi(b))$. Тогда для мультиграмм a^t и b^t условие

$$\text{rang}(L(A(a^к)) \cup L(A(b^t))) = t. \qquad (19)$$

равносильно условию $(\chi(a), \chi(b)) = 1$.

Доказательство. Имеем

$$\text{rang}(L(A(a^t)) \cup L(A(b^t))) = \dim L(A(a^к)) + \dim L(A(b^t)) - \dim(L(A(a^к)) \cap L(A(b^t))).$$

Очевидно,

$$\dim L(A(a^к)) = t - \deg \chi(a), \quad \dim L(A(b^t)) = t - \deg \chi(b),$$
$$\dim(L(A(a^к)) \cap L(A(b^t))) = t - \text{degH.O.K.}(\chi(a), \chi(b)).$$

Требуемое условие (19) равносильно условию

$$t - \deg \chi(a) + t - \deg \chi(b) - t + \text{degH.O.K.}(\chi(a), \chi(b)) = t$$

или

$$\deg \chi(a) + \deg \chi(b) = \text{degH.O.K.}(\chi(a), \chi(b)),$$

которое, в свою очередь эквивалентно тому, что

$$(\chi(a), \chi(b)) = 1.$$

Лемма 7, а вместе с ней и следствие 2 доказаны.

17.4. Период внешнего функционирования автономного последовательного соединения автоматов

Пусть $A_1 = (S_1, У_1, h, \lambda)$ – приведенный полноцикловый автомат с множеством состояний S_1, $|S_1| > 1$, выходным алфавитом $У_1$, $|У_1| > 1$, функцией перехода h и выхода λ и $A_2 = (X, S_2, Y_2, h, f)$, $Y_1 = X$ – перестановочный автомат с частичными функциями переходов $(h_x)_{x\in X}$ и частичными функциями выхода $(f_x)_{x\in X}$. Напомним, что последовательным соединением автоматов A_1, A_2 называют автономный автомат $A_1 \to A_2 = (S_1 \times S_2, Y_2, h^{1,2}, f^{1,2})$, у которого $h^{1,2}(s(1), s(2)) = (hs(1), h_{\lambda(s(1))}s(2))$, $f^{1,2}(s(1), s(2)) = f_{\lambda(s(1))}s(2)$, $(s(1), s(2)) \in S_1 \times S_2$.

Наряду с последовательным соединением $A_1 \to A_2$ введенных автоматов мы будем рассматривать так называемое обобщенное последовательное соединение $A_1 \Rightarrow A_2$ автоматов A_1, A_2, отличающееся от $A_1 \to A_2$ функцией выхода. При обобщенном соединении любое отображение $S_1 \times S_2 \to Y$ может быть функцией выхода автомата $A_1 \Rightarrow A_2$.

Очевидно, построенный автомат $A = A_1 \Rightarrow A_2$ является перестановочным автоматом; длины циклов графа переходов автомата A кратны числу $|S_1|$. Обозначим через $W(s(1), s(2))$ период выходной последовательности $A(s(1), s(2))$, соответствующий начальному состоянию $(s(1), s(2)) \in S_1 \times S_2$ автомата A. Положим $W(A)$ – наименьшее общее кратное периодов $W(s(1), s(2))$ взятое по всем $(s(1), s(2)) \in S_1 \times S_2$. Эта величина называется *периодом внешнего функционирования автомата* A**.**

Пусть $L_1, L_2, \ldots, L_t$ – связные компоненты (циклы) автомата A и $|L_j|$, $j \in \{1, \ldots, t\}$ – их длины. Очевидно, периоды выходных последовательностей автомата A от начальных состояний, содержащихся в одном цикле, совпадают, в связи с чем можно говорить о периоде выходных последовательностей состояний цикла L_j, $j \in \{1, \ldots, t\}$ или, более кратко, о выходном периоде W_j цикла L_j. Известно, что период (длина) W_j цикла L_j совпадает с числом классов неотличимых состояний связной компоненты L_j, $j \in \{1, \ldots, t\}$. Поэтому

$$W(A) = \underset{j\in\{1,\ldots,t\}}{H.O.K.} W_j = H.O.K.\frac{|L_j|}{|N_j|},$$

где $|N_j|$ – мощность классов неотличимых состояний цикла L_j.

Для получения оценки снизу периода W(A) внешнего функционирования автомата A введем необходимые обозначения и докажем вспомогательные леммы.

Пусть A_v, $v \in \{1, \ldots, \Gamma\}$ – подавтомат автомата A, состоящий из v-го класса $L_{v1}, L_{v2}, \ldots, L_{vt(v)}$ неотличимых связных компонент (циклов) автомата A и $N(A_v)$ мощность его классов неотличимых состояний, $W(A_v)$, $v \in \{1, \ldots, \Gamma\}$ – число его классов неотличимых состояний. Очевидно,

$$W(A_v) = W(L_{vj}),\ j \in \{1, \ldots, t(v)\},$$
$$W(A) = \underset{v \in \{1,\ldots,\Gamma\}}{H.O.K.} W(A_v) \quad .$$

Лемма 8. Пусть $d \mid |S_1|$. Тогда

$$\frac{d}{(d, W(A_v)} \mid N(A_v),\ v \in \{1, \ldots, \Gamma\}.$$

Доказательство. Положим $L_{vj} = dk_{vj}$. Имеем

$$\sum_{j \in \{1,\ldots,T_v\}} |L_{vj}| = W(A_v) \cdot N(A_v) = dk_{vj}.$$

Откуда и вытекает данное утверждение.

Лемма 9. Пусть P – простое число, α – целое число, $\alpha \geq 1$, $P^\alpha \mid |S_1|$, (P^α, $W(A) = P^\beta$, $0 \leq \beta \leq \alpha$. Тогда мощность любого класса к-неотличимых состояний ($к \in \{1, 2, \ldots\}$) перестановочного автомата A кратна $P^{\alpha-\beta}$.

Доказательство. Так как каждый класс к-неотличимых состояний автомата A представляет собой объединение некоторых классов (к+1)-неотличимых состояний, а $N(A_v)$, $v \in \{1, \ldots, \Gamma\}$ являются мощностями его классов неотличимых состояний, то для доказательства леммы достаточно показать, что $P^{\alpha-\beta} \mid N(A_v)$ при любом $v \in \{1, \ldots, \Gamma\}$. По лемме 8

$$\frac{d}{(d, W(A_v)} \mid N(A_v),\ v \in \{1, \ldots, \Gamma\}.$$

Заметим, что из условия (P^α, $W(A) = P^\beta$, $0 \leq \beta \leq \alpha$ вытекает равенство

$$(P^\alpha, W(A_v)) = P^{\beta(v)},\ v \in \{1, \ldots, \Gamma\}$$

при некоторых $\beta(v) \leq \beta$ и, следовательно, величина $\dfrac{P^\alpha}{(P^\alpha, W(A_v)} = P^{\alpha-\beta(v)}$ делит $N(A_v)$, $v \in \{1, \ldots, \Gamma\}$. Но тогда и тем более $P^{\alpha-\beta} \mid N(A_v)$, $v \in \{1, \ldots, \Gamma\}$, что и требовалось доказать.

Из леммы 9 непосредственно вытекают такие утверждения.

Следствие 3. Пусть $|S_1| = P_1^{\alpha(1)}P_2^{\alpha(2)}\ldots P_n^{\alpha(n)}$, P_j, – простые числа, α_j, $j\in\{1, \ldots, n\}$ – целые положительные числа, и для автомата $A = A_1 \Rightarrow A_2$

$$(|S_1|, W(A)) = P_1^{\beta(1)}P_2^{\beta(2)}\ldots P_n^{\beta(n)}, \quad \beta(j) \geq 0, j\in\{1, \ldots, n\}.$$

Тогда мощность любого класса к-неотличимых состояний автомата А кратна числу

$$P_1^{\alpha(1)-\beta(1)}P_2^{\alpha(2)-\beta(2)}\ldots P_n^{\alpha(n)-\beta(n)}.$$

Следствие 4. Пусть общий наибольший делитель мощностей некоторых классов к-неотличимых состояний автомата $A = A_1 \Rightarrow A_2$ равен единице. Тогда период внешнего функционирования автомата А кратен $|S_1|$.

17.5. Периоды выходных последовательностей перестановочного автомата без потери информации при заданных периодических входных последовательностях

Ниже в данном пункте рассматриваются перестановочные автоматы и чисто периодические их входные последовательности. Напомним необходимые нам понятия [16]. Состояние s автомата А называется *состоянием с потерей информации*, если найдутся *разные сравнимые слова* R = x(1), x(2), …, x(k), T = x`(1), x`(2), …, x`(k) из X*, при которых

$$A(s, R) = A(s, T), h(s, R) = h(s, T),$$

в противном случае состояние s называется *состоянием без потери информации*. Автомат А называется автоматом с потерей информации, если у него найдется состояние с потерей информации, в противном случае он называется *автоматом без потери информации*.

Через ω(s, P) обозначим период последовательности состояний $A_M(s, P)$ автомата А при входной чисто периодической последовательности P и начальном состоянии s. Обозначим через N_y, $y\in Y$ множество всех состояний $s\in S$ автомата А, для каждого из которых существует элемент $x\in X$, x = x(s), удовлетворяющий равенству

$$f_x s = y.$$

Очевидно, $|N_y| \leq |S|$ при любом $y\in Y$, а если А является автоматом Мура, то

$$\sum_{y\in Y} |N_y| = |S|,$$

что в общем случае для автоматов Мили не справедливо.

Для входной последовательности P автомата A и его состояния $s \in S$ введем параметр N(A(s, P)), положив

$$N(A(s, P)) = \min\{|N_y|\},$$

где минимум берется по всем выходным символам $y \in Y$ автомата A, встречающимся в выходной последовательности A(s, P).

Определение 4. Грубым периодом последовательности состояний $A_M(s, P)$ перестановочного автомата A при входной чисто периодической последовательности P = x(1), x(2), ... периода $\omega = \omega(P)$ и начальном состоянии $s \in S$ называется число $\Omega(s, P) = C \cdot \omega$, где $C = C(s, P) > 0$ – минимальное целое, для которого

$$(h_{x(\omega)}\, h_{x(\omega-1)} \ldots h_{x(1)})^C = s,$$

то есть C = C(s, P) – длина цикла подстановки $h_{x(\omega)}h_{x(\omega-1)}\ldots h_{x(1)}$, содержащего состояние s.

Теорема 4. Справедливы следующие утверждения.

1. Если перестановочный автомат A – автомат с потерей информации, то для любого $\varepsilon > 0$ существуют входная чисто периодическая последовательность P периода $\omega(P)$ и состояние s автомата A, для которых

$$\frac{W(s,P)}{\omega(P)} < \varepsilon .$$

2. Если перестановочный автомат A – без потери информации, то для любой входной чисто периодической последовательности P = x(1), x(2), ... периода $\omega(P)$ и любого начального состояния $s \in S$ автомата A

$$\frac{W(s,P)}{\omega(P)} \geq \frac{W(s,P)}{\Omega(s,P)} \geq \frac{1}{N(A(s,P))} .$$

Доказательство. Докажем сначала первое утверждение теоремы. Пусть автомат A с потерей информации, то есть существуют $s \in S$ и слова R, T, $R \neq T$,

$$R = x(1), x(2), \ldots, x(k);\ T = x`(1), x`(2), \ldots, x`(k);\ k \geq 1;\ x_j, x`_j \in X,$$
$$j \in \{1, ..., k\},$$

для которых справедливы равенства

$$A(s, R) = A(s, T),\ h(s, R) = h(s, T) = s`,\ s` \in S.$$

Так как A – перестановочный автомат, то существует входное слово

$$M = x``(1), x``(2), \ldots, x``(n), x``_j \in X,\quad j \in \{1, ..., n\},$$

для которого

$$h_{x``(n)}h_{x``(n-1)}\ldots h_{x``(1)}s` = s.$$

Рассмотрим последовательность P вида

$$P = \underbrace{RMRM...RM}_{L} TM \underbrace{RMRM...RM}_{L} TM...,$$

период ω(P) которой, очевидно, является делителем числа L·(k+n)+k+n = (L+1)(k+n). Возьмем в качестве L+1 простое число $p > \frac{k+n}{\varepsilon}$. Из условия R ≠ T следует, что ω(P) не является делителем числа k+n и, следовательно, ω(P) кратно p, так как ω(P) делит p · (k+n). Кроме того, из построения последовательности P и выбора s∈S вытекает, что W(s, P) делит k+n. Таким образом, можно заключить:

$$\frac{W(s,P)}{\omega(P)} \le \frac{k+n}{\omega(P)} \le \frac{k+n}{p} < \varepsilon,$$

что и требовалось доказать в первом утверждении теоремы 4.

Докажем второе утверждение теоремы 4. Очевидно, что W = W(s, P) и ω(P) являются делителями грубого периода Ω(s, P) последовательности состояний A_M(s, P) автомата A, поэтому, в частности

$$\frac{W(s,P)}{\omega(P)} \ge \frac{W(s,P)}{\Omega(s,P)}.$$

Пусть

$$\frac{\Omega(s,P)}{W(s,P)} = L(s,P) = L.$$

Положим A_M(s, P) = $s_1, s_2, ..., s_n, ...$, где $s_{n+1} = h_{x(n)}...h_{x(1)}s$ и $s_1 = s$. Для доказательства требуемого утверждения теперь достаточно показать, что для любого j∈{0, 1, ..., W–1} все L состояний вида s_{j+1+kW}, k∈{0, 1, ..., L–1} различны. Действительно, если это так, то L ≤ $|N_y|$ для любого y, содержащегося в последовательности A(s, P), и, следовательно,

$$L \le N(A(s, P)).$$

Поэтому

$$\frac{W(s,P)}{\omega(P)} \ge \frac{W(s,P)}{\Omega(s,P)} = \frac{1}{L}.$$

Покажем теперь, что при любом j∈{0, 1, ..., ω–1} указанные выше L состояний различны. Предположим противное, то есть пусть, например, для j = 0 существуют целые числа k(1), k(2), 0 ≤ k(1) < L–1, k(1) < k(2) ≤ L–1, для которых

$$s_{1+k(1)W} = s_{1+k(2)W}.$$

Для последовательности P = x(1), x(2), ... введем вспомогательные последовательности P^t = x(t), x(t+1), ..., P^1 = P.

Имеем

$$A(s_{1+k(1)W}, P^{k(1)W+1}) = A(s_{1+k(2)W}, P^{k(2)W+1}),$$

так как $W = W(s, P)$ – период последовательности $A(s, P)$.

Положим $s^* = s_{1+k(1)W} = s_{1+k(2)W}$, $\Omega^{ext}(s^*, P^{k(1)W+1}) = C_1 \cdot \omega$, $\Omega^{ext}(s^*, P^{k(2)W+1}) = C_1 \cdot \omega$ – грубые периоды последовательностей $A_M(s^*, P^{k(1)W+1})$, $A_M(s^*, P^{k(2)W+1})$, $H = \text{Н.О.К.}(C_1 \cdot \omega, C_1 \cdot \omega)$, где $\omega = \omega(P) = \omega(P^{k(1)W+1}) = \omega(P^{k(2)W+1})$. Тогда

$$h_{x(k(1)W+H)} \ldots h_{x(k(1)W+2)} h_{x(k(1)W+1)}\, s^* = h_{x(k(2)W+H)} \ldots h_{x(k(2)W+2)} h_{x(k(2)W+1)}\, s^*.$$

Так как автомат A без потери информации, то из этого равенства получаем

$$P^{(k(1)W+1)} = P^{(k(2)W+1)}$$

и, следовательно, $(k(2) - k(1))W \equiv 0 \bmod(\omega(P))$. Учитывая это сравнение, равенство состояний $s_{1+k(1)W}$, $s_{1+k(2)W}$ и перестановочность автомата A, получаем

$$s = h_{x(k(2)-k(1))W)} \ldots h_{x(2)} h_{x(1)} s\ .$$

Из определения величины $\Omega(s,P)$ и того факта, что $\omega(P)$ делит $(k(2) - k(1))W$, следует, что $\Omega(s, P)$ делит $(k(1) - k(2))W$. Последнее условие противоречит тому, что $k(2) - k(1) < L$. Утверждение 2 теоремы 4 полностью доказано.

Следствие 5. Пусть A – перестановочный автомат без потери информации. Тогда для любой входной чисто периодической последовательности P периода $\omega(P)$ и любого состояния s автомата A выполнены неравенства

$$\Omega(s, P) \geq W(s, P) \geq \frac{\Omega(s, P)}{N(A(s, P))} \geq \frac{\omega(P)}{N(A(s, P))}\ ,$$

в частности,

$$|S| \cdot \omega(P) \geq W(s, P) \geq \frac{\omega(P)}{|S|}\ .$$

Доказательство. Верхняя оценка $W(s, P)$ очевидна, а нижняя оценка периода $W(s, P)$ справедлива согласно лемме 2.

Говорят, что *граф автомата* $A = (X, S, Y, (h_x)_{x \in X}, (f_x)_{x \in X})$ *не имеет параллельных дуг*, если при любом $s \in S$

$$h_x s \neq h_{x`} s$$

для каждой пары различных элементов x, x` из X.

Следствие 6 (В. А. Башев). Пусть $A = (X, S, Y, h, f)$ – перестановочный автомат и его граф без параллельных дуг, P – его входная периодическая последовательность периода $\omega(P)$, $s \in S$ – его начальное состояние. Тогда период $\omega(s, P)$ последовательности состояний $A_M(s, P)$ автомата A кратен периоду $\omega(P)$. Если автомат A не являет-

ся автоматом без параллельных дуг, то найдется его начальное состояние $s \in S$ и входная периодическая последовательность P некоторого периода $\omega(P)$, при которых период последовательности состояний $A_M(s, P)$ не кратен $\omega(P)$.

Доказательство. Используем утверждение теоремы 4. В качестве вспомогательного автомата выберем автомат Медведева A_M, соответствующий автомату A = (X, S, Y, h, f). Автомат A_M имеет вид A_M = (X, S, S, h, E), где S является его множеством состояний и выходным алфавитом. Функция выхода E такова, что E(s, x) = s при каждом s из S и x из X. Для автомата A_M ранее введенные множества N_y, $y \in Y$ одноэлементны, поэтому параметр $N(A(s,P))$ равен единице. По утверждению 2 теоремы 4 получаем

$$\Omega(s,P) \geq W(s,P) \geq \Omega(s,P),$$

то есть $\Omega(s,P) = W(s,P)$. Обратно, если граф автомата A имеет параллельные дуги, то автомат A_M = (X, S, S, h, E) является автоматом с потерей информации. Тогда искомые параметры: состояние s и периодическая входная последовательность P найдутся согласно утверждению 1 теоремы 4. Доказательство полученного ранее В. А. Башевым утверждения завершено.

Пусть P – фиксированная чисто периодическая последовательность символов некоторого алфавита X, $|X| > 1$ периода $\omega(P)$ и s_1 – фиксированный элемент некоторого множества S. Следующая теорема отвечает на вопрос о достижимости приведенных в следствии 6 верхней и нижней оценок $\Omega(s,P) \geq W(s,P) \geq \frac{\Omega(s,P)}{N(A(s,P))}$ периода W(s, P) выходной последовательности A(s, P) автомата A.

Теорема 5. В классе перестановочных автоматов Мура A = (X, S, Y, h, λ) без потери информации с входным алфавитом X и множеством состояний S оценки

$$\Omega(s_1,P) \geq W(s_1,P) \geq \frac{\Omega(s_1,P)}{N(A(s_1,P))}$$

периодов $W(s_1, P)$ выходных последовательностей состояний A(s, P) не могут быть улучшены.

Доказательство. Проведем сначала доказательство утверждения теоремы 5 относительно нижней оценки. Пусть A – некоторый перестановочный автомат Мура без потери информации. Рассмотрим отношение

$$\frac{\Omega(s_1,P)}{W(s_1,P)} = L(s_1,P) = L.$$

Исследуем сначала случай, когда $W(s_1, P) = 1$. Если $L = 1$, то все доказано. В случае $L \geq 2$, как следует из доказательства леммы 2, первые L членов последовательности состояний $A_M(s_1, P)$ автомата A различны, поэтому $N(A(s_1, P)) > 1$ и мы можем построить новый автомат

$$A' = (X, S, Y`, h, \lambda`),$$

отличающийся от A выходным алфавитом Y`, который мы определяем соотношением

$$Y` = Y \cup \{z\},$$

где $z \notin Y$ – некоторый новый символ. Функцию выхода $\lambda`$ определяем равенствами

$$\lambda'(s) = \lambda(s),$$

в двух случаях: 1) если s находится среди состояний последовательности $A_M(s_1, P)$; 2) если $s \notin N_y$ для каждого y из выходной последовательности $A(s_1, P)$ автомата A. Далее полагаем

$$\lambda`(s) = z,$$

если в последовательности состояний $A_M(s_1, P)$ не содержится s и $s \in N_y$ для некоторого y из последовательности $A(s_1,P)$. Ясно, что A` является перестановочным автоматом без потери информации, для которого достигается доказываемая нижняя оценка.

Рассмотрим теперь случай $W(s_1, P) > 1$. При $L = N(A(s_1, P))$ все доказано. Допустим, что $L < N(A(s_1, P))$. Пусть $P = x(1), x(2), ..., x(k), ...$ и

$$A_M(s_1, P) = s_1, s_2, ..., s_k, ...; \; s_{k+1} = h_{x(k)}h_{x(k-1)}...h_{x(1)}s_1, \; k \in \{0, 1, 2, ...\}.$$

Выберем $k \in \{0, 1, ..., W(s_1, P)-1\}$ так, чтобы

$$s_k \in N_y, \; |N_y| = N(A(s_1, P)).$$

Определим новый автомат A` условиями: A` отличается от A только выходным алфавитом $Y` = Y \cup z$, где z – некоторый символ, $z \notin Y$, и выходной функцией $\lambda`$, определенной условиями

$$\lambda`(s) = \lambda(s),$$

если s находится в наборе состояний $(s_{1+k+jW}: j \in \{0, 1, ..., L-1\})$, $W = W(s_1,P)$ или $s \notin N$ для каждого y из выходной последовательности $A(s_1, P)$ автомата A. В противном случае полагаем

$$\lambda`(s) = z.$$

Непосредственно проверяется, что A` – перестановочный автомат без потери информации, для которого

$$W(s_1, P) = \frac{\Omega(s_1, P)}{N(A(s_1, P))}.$$

Перейдем теперь к доказательству достижимости верхней оценки периода $W(s_1, P)$. Рассмотрим произвольный перестановочный автомат Мура A без потери информации, для которого отображение $\lambda: S \to Y$, осуществляемое функцией выхода λ, сюръективно. Предположим, что $|Y| = |S|$. Тогда отображение λ взаимно однозначно. Из доказательства леммы утверждения 2 теоремы 4

$$\frac{\Omega(s_1, P)}{W(s_1, P)} = L = 1,$$

и, следовательно, в этом случае утверждение теоремы 5 относительно верхней оценки доказано.

Пусть теперь $|Y| < |S|$. Если $W(s_1, P) = \Omega(s_1,P)$, то теорема 5 верна; в противном случае определим новый автомат A`, отличающийся от A выходным алфавитом $Y` = Y \cup z$, $z \notin Y$ и выходной функцией $\lambda`$, удовлетворяющей условиям:

$$\lambda`(s_1) = z,\ \lambda`(s) = \lambda(s),\ s \in S,\ s \neq s_1.$$

Очевидно, A` – перестановочный автомат без потери информации, для которого

$$W(s_1, P) = \Omega(s_1, P).$$

Теорема 5 полностью доказана.

17.6. Периоды выходных последовательностей последовательного соединения автономного автомата с перестановочным автоматом без потери информации

Рассмотрим приложения полученных результатов в пункте 17.5 к задаче оценки периодов выходных последовательностей и мощностей классов неотличимых состояний перестановочных автоматов, представимых последовательным соединением приведенного автономного автомата с неавтономным перестановочным автоматом без потери информации. Для последовательного соединения автоматов используем обозначения пункта 17.4. Пусть $A_1 = (S_1, У_1, h, \lambda)$ – приведенный полноцикловый автомат с множеством состояний S_1, $|S_1| > 1$, выходным алфавитом $У_1$, $|У_1| > 1$, а $A_2 = (X, S_2, Y_2, h, f)$, $Y_1 = X$ – перестановочный автомат без потери информации. Напомним, что функция выхода автономного последовательного соединения $C = A_1 \to A_2 = (S_1 \times S_2, Y_2, h^{1,2}, f^{1,2})$ автоматов A_1, A_2 определена функцией выхода автомата A_2.

Для $s(1) \in S_1$, $s(2) \in S_2$ обозначим через $W(s(1), s(2))$ период выходной последовательности автомата $C = A_1 \to A_2$, соответствующей

его начальному состоянию (s(1), s(2)), а через $A_1(s(1))$ – выходную последовательность автомата A_1, отвечающую начальному состоянию $s(1) \in S_1$. Из приведенных в пункте 5 результатов непосредственно вытекает теорема 3.

Теорема 6. В указанных выше условиях

$$W((s(1), s(2)) \geq \frac{|S_1|}{N(C(t,s))},$$

где $N(C(t,s))$ – множество минимальной мощности в совокупности множеств N_y, по всем y из последовательности C(s(1), s(2)).

Напомним и введем обозначения:

– L(s(1), s(2)) – связная компонента графа перехода автомата C, содержащая состояние (s(1), s(2));

– C(s(1), s(2)) – выходная последовательность автомата C, отвечающая его начальному состоянию (s(1), s(2));

– W(s(1), s(2)) – период выходной последовательности (s(1), s(2));

– $A_1(s(1))$ – выходная последовательность автомата A_1 при начальном состоянии $s(1) \in S_1$;

– $\omega(A_1(s(1)))$ – период выходной последовательности $A_1(s(1))$ автомата A_1 при начальном состоянии $s(1) \in S_1$;

– $W(s(2), A_1(s(1)))$ – период выходной последовательности автомата A_2, отвечающей входной периодической последовательности A(s(1)) и начальному состоянию s(2);

– $\Omega(s(2), A_1(s(1)))$ – грубый период последовательности состояний перестановочного автомата A_2 для входной периодической последовательности $A_1(s(1))$ и начального состояния $s(2) \in S_2$.

Теорема 7. Мощности классов неотличимых состояний автомата $C = A_1 \to A_2$ ограничены сверху величиной $|S_1| \cdot \max|\{|N_y|\}_{y \in Y}$.

Доказательство. Очевидны следующие равенства:

$$\omega(A_1(s(1))) = |S_1|,$$

$$W(s(1), s(2)) = W(s(2), A_1(s(1))),$$

$$|L(t, s)| = \Omega(s(2), A_1(s(1))).$$

Так как автомат A без потери информации, то из этих равенств следует

$$W(s(1),s(2)) \geq \frac{L(s(1), s(2))}{\max\{|N_y|\}_{y \in Y}}.$$

С другой стороны, W(s(1), s(2)) есть число классов неотличимых состояний связной компоненты автомата C, содержащей состо-

яние (s(1), s(2)). Поэтому, если d(s(1), s(2)) – мощность классов неотличимых состояний этой компоненты, то

$$d(s(1),s(2)) = \frac{|L(s(1),s(2))|}{W(s(1),s(2))} \le \frac{|L(s(1),s(2))| \cdot \max\{|N_y|\}_{y\in Y}}{|L(s(1),s(2))|},$$

то есть

$$d(s_1, s_2) \le \max\{|N_y|\}_{y\in Y}.$$

Теперь утверждение теоремы 4 следует из того, что каждый класс неотличимых состояний автомата C представляет собой объединение некоторых классов неотличимых состояний его связных компонент, причем число связных компонент автомата C не превосходит $|S_1|$.

Теорема 8. Пусть $|S_1| > \max\{|N_y|\}_{y\in Y}$. Тогда

$$(W(s(1),s(2)),|S_1|) \ne 1$$

для любого состояния (s(1), s(2)) автомата C.

Доказательство. Пусть

$$(W(s(1),s(2)),|S_1|) = 1.$$

Тогда, пользуясь тем, что $|L(s(1), s(2)) = C\cdot|S_1|$ для некоторого целого $C = C(s(1), s(2))$, из соотношения

$$d(s(1),s(2)) = \frac{|L(s(1),s(2))|}{W(s(1),s(2))} \le \max_{y\in Y} |N_y|$$

получаем

$$|S_1| \le \max\{|N_y|\}_{y\in Y},$$

что противоречит условию теоремы 8.

Следствие 7. Пусть $|S_1|$ – простое число и $|S_1| > \max\{|N_y|\}_{y\in Y}$. Тогда:

1) для любого состояния $(s(1), s(2))\in S_1\times S_2$ периоды W(s(1), s(2)) выходных последовательностей C(s(1), s(2)) автомата $C = A_1 \to A_2$ кратны $|S_1|$;

2) мощности классов неотличимых состояний автомата $C = B \Rightarrow A$ ограничены сверху величиной $|S_2|$.

Доказательство. Утверждение 1 непосредственно вытекает из теоремы 8. Будем доказывать утверждение 2 следствия. Пусть $L_j = D_j \cdot |S_1|$, $j\in\{1, 2, ..., m\}$ – мощности связных компонент графа перехода автомата C. Тогда мощности классов неотличимых состояний этих связных компонент имеют вид k_j, где k_j делят $|D_j|$, $j\in\{1, 2, ..., m\}$. Следовательно, так как

$$\sum_{j=1}^{m} k_j \le \sum_{j=1}^{m} D_j = |S_2|,$$

то мощности классов неотличимых состояний ограничены сверху величиной $|S_2|$.

Замечание. При получении вышеприведенных результатов перестановочность автомата A использовалась для доказательства наличия входного слова M = x``(1), x``(2), …, x``(n) переводящего приемник $h_{x(k)}h_{x(k-1)}\ldots h_{x(1)}s$ состояния $s \in S$ в состояние s. В связи с чем аналогичные результаты видимо можно получить и для сильно связных автоматов A. При этом необходимо учесть специфику возможной небиективности преобразований вида $h_{x(k)}h_{x(k-1)}\ldots h_{x(1)}$ автомата A, в частности, необходима корректировка понятия грубого периода последовательности состояний автомата A при его начальном состоянии и входной периодической последовательности.

Глава 18. КЛАССЫ АВТОМАТОВ С ГАРАНТИРОВАННЫМИ ПЕРИОДАМИ ВЫХОДНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

Доказаны нижние оценки периодов выходных последовательностей для автономных полноцикловых автоматов с заданным классом функций выхода и класса неавтономных автоматов, выходные последовательности которых имеют вид

$y_1, y_2, ..., y_j, ..., y_j = \varphi(x_j, x_{j+1}, ..., x_{j+L-1})$, $L \geq 2$,

$\varphi: X^L \to Y$, X – входной алфавит, Y – выходной алфавит,

$x_j \in X$, $y_j \in Y$, $j \in \{1, 2, ...\}$.

Приведены и другие классы автоматов с гарантированными периодами выходных последовательностей.

В частности, для заданной периодической входной последовательности узла усложнения поточных криптосхем, функционально представляющих собой устройство нерегулярной выборки, оценен период выходной последовательности.

18.1. Необходимость построения автоматов с гарантированными периодами выходных последовательностей

Известно, что в науке и технике и, в частности, в различных системах обеспечения безопасности широко применяются генераторы псевдослучайных последовательностей.

Так, например, эти генераторы используются в синхронных поточных криптосхемах [14].

Одно из основных требований состоит в том, что последовательность, вырабатываемая генератором, должна иметь большой период.

Ряд современных генераторов содержит разнообразные узлы выборки, предназначенные для усложнения промежуточных последовательностей генератора.

Функционирование некоторых узлов выборки допускает их общее описание в виде математического понятия обобщенного узла выборки (ОУВ) введенного в данном параграфе.

Основные результаты работы состоят в указании классов автоматов гарантированным периодом выходной последовательности.

18.2. Кодирующее устройство с конечной памятью

Пусть X, Y – конечные множества, $|X| \geq 2$, $|Y| \geq 2$, $\varphi: X^L \to Y$, $L \in \{2, 3, ...\}$. Рассматриваемая задача состоит в получении оценок снизу периода W последовательности $y_1, y_2, ..., y_j, ...$,

$$y_j = \varphi(x_j, x_{j+1}, ..., x_{j+L-1}), j \in \{1, 2, ...\}$$

для заданной периодической последовательности $P = x_1, x_2, ...$ периода ω. Устройство перерабатывающую входную последовательность по указанному закону называют кодирующим устройством с конечной памятью и без обратной связи [44].

Для решения задачи напомним и введем необходимые нам понятия.

Под периодической последовательностью ниже понимается чисто периодическая последовательность, а под ее периодом – наименьший период.

Говорят, что функция $\varphi: X^L \to Y$, $L \in \{2, 3, ...\}$ имеет запрет, если существует $k \in \{1, 2, ...\}$ и набор $y_1, y_2, ..., y_k$, для которого система уравнений

$$\varphi(x_1, x_2, ..., x_L) = y_1$$
$$\varphi(x_2, x_3, ..., x_{L+1}) = y_2$$
$$.....$$
$$\varphi(x_k, x_{k+1}, ..., x_{k+L-1}) = y_k$$

относительно неизвестных $x_j \in X$, $j \in \{1, ..., k+L-1\}$ несовместна [31]. В противном случае говорят, что функция φ не имеет запрета. Функцию φ называют сильно k-равновероятной, если при любом наборе $y_1, y_2, ..., y_k$ из Y^k приведенная выше система уравнений имеет ровно

$$\frac{|X|^{k+L-1}}{|Y|^k}$$

решений. Если функция сильно k-равновероятна при любом k, то ее называют сильно равновероятной. В работе [31], теореме 1 доказано, что *двоичная функция не имеет запрета тогда и только тогда, если она сильно равновероятна.* Данное утверждение справедливо и для рассматриваемых в данной работе произвольных функций $\varphi: X^L \to Y$, $L \in \{2, 3, ...\}$. Доказательство этого общего факта проводится аналогично доказательству теоремы 1 работы [31].

Далее под периодической последовательностью понимается чисто периодическая последовательность. Для последовательности $P = x_1, x_2, ...$ обозначим последовательность $x_j, x_{j+1}, ...$ через P^j. Тогда P

представляется в виде $P = (x_1, x_2, ..., x_{j-1})$, P^j – конкатенации слов $x_1, x_2, ..., x_{j-1}$ и P^j. Отметим, что в этих обозначениях последовательность P записывается в виде P^1, $P = P^1$. Начальное подслово $x_1, x_2, ..., x_t$ длины t последовательности $P = x_1, x_2, ...$ обозначим через $P]_t$. Так, в частности, $P^j]_t = x_j, x_{j+1}, ..., x_{j+t-1}$.

Определение 1. Степенью различимости $R = R(P)$ периодической последовательности $P = x_1, x_2, ...$ периода ω назовем минимальное число R, при котором R-гаммы $P^j]_{j+R-1}$, $j \in \{1, ..., \omega\}$ последовательности $P = P^1$ попарно различны, то есть

$$|\{P^j]_{j+R-1}, j \in \{1, ..., \omega\}\}| = \omega.$$

Теорема 1. Пусть $L \geq 2$, $\varphi: X^L \to Y$ – сильно k-равновероятная функция, $k+L-1 \geq R(P)$, где R(P) – степень различимости периодической последовательности $P = x_1, x_2, ...$ периода ω. Тогда справедлива следующая оценка периода W последовательности $y_1, y_2, ..., y_j, ..., y_j = \varphi(x_j, x_{j+1}, ..., x_{j+L-1})$, $j \in \{1, 2, ...\}$

$$W \geq \frac{\omega |Y|^k}{|X|^{k+L-1}}.$$

Доказательство. Пусть $WC = \omega$ при некоторм $C \geq 2$. Тогда

$$y_j = \varphi(x_{j+CW}, x_{j+1+CW}, ..., x_{j+L-1+CW})$$

при любых $j \in \{1, 2, ...\}$, $C \in \{0, 1, ...\}$. Из условий теоремы следует, что C слов длины $k+L-1$ вида $(x_{1+tW}, x_{2+tW}, ..., x_{k+L-1+W})$, $t \in \{0, ..., C-1\}$ попарно различны, и они являются решениями системы уравнений

$$\varphi(x_j, x_{j+1}, ..., x_{j+L-1}) = y_j, j \in \{1, ..., k\}.$$

Так как функция φ сильно k-равновероятна, то число решений данной системы для ее правой части $y_1, y_2, ..., y_k$ равно $\frac{|X|^{k+L-1}}{|Y|^k}$, откуда получаем

$$C = \frac{\omega}{W} \leq \frac{|X|^{k+L-1}}{|Y|^k}.$$

Следовательно,

$$W \geq \frac{\omega |Y|^k}{|X|^{k+L-1}}.$$

Следствие 1. Пусть $L \geq 2$, $\varphi: X^L \to Y$ – сильно равновероятная функция, $|X| = |Y|$, $P = x_1, x_2, ...$ – периодическая последовательность периода $\omega \geq D$. Тогда справедлива следующая оценка периода W последовательности $y_1, y_2, ..., y_j, ..., y_j = \varphi(x_j, x_{j+1}, ..., x_{j+L-1})$, $j \in \{1, 2, ...\}$

$$W \geq \frac{D}{|X|^{L-1}}.$$

Отличительной особенностью последнего утверждения относительно известных утверждений о гарантировании периодов выходных последовательностей автоматов является то обстоятельство, что условиями следствия гарантируется период W рассматриваемого автомата при неизвестном точном значении периода ω входной последовательности.

Утверждение 1. Пусть $P = x_1, x_2, \ldots$ – линейная рекуррентная последовательность максимального периода над полем F_2 из двух элементов, φ – сюръективное отображение $(F_2)^m$ в Y, $|Y| \geq 2$, $m < n$, а $\varphi^{-1}(y)$ – множество решений уравнения $\varphi(x_1, x_2, \ldots, x_m) = y$ относительно неизвестных $x_j \in F_2$, $j \in \{1, \ldots, m\}$, и $\varphi(0, 0, \ldots, 0) = y`$. Если величины

$$\{|\varphi^{-1}(y)| \cdot 2^{n-m},\ y \in Y \setminus \{y`\},\ |\varphi^{-1}(y`)| \cdot (2^{n-m}-1)\}$$

в совокупности взаимно просты, то период W последовательности $y_1, y_2, \ldots, y_j, \ldots$, $y_j = \varphi(x_j, x_{j+1}, \ldots, x_{j+L-1})$, $j \in \{1, 2, \ldots\}$ равен 2^n-1.

Доказательство. Сначала заметим, что задача оценки W сводится к задаче оценки периода выходной последовательности автономного полноцикловаго автомата A = (S, Y, T, Φ), состояниями которого являются следующие ω-граммы последовательности P:

$$s_1 = x_1, x_2, \ldots, x_\omega$$
$$s_2 = x_2, x_3, \ldots, x_\omega, x_1$$
$$\ldots\ldots\ldots\ldots$$
$$s_j = x_j, \ldots, x_\omega, x_1, x_2, \ldots, x_{j-1}$$
$$\ldots\ldots\ldots\ldots$$
$$s_\omega = x_\omega, x_1, \ldots, x_{\omega-1}.$$

Здесь $\omega = 2^n-1$, так как $P = x_1, x_2, \ldots$ – линейная рекуррентная последовательность максимального периода над полем F_2. Функция переходов T автомата A определена отображением: $s_j \to s_{j+1}$, $j \in \{1, \ldots, \omega-1\}$, $s_\omega \to s_1$; функция выходов Φ определена так:

$$\Phi(s_j) = \varphi(x_j, \ldots, x_{j+m-1}),\ j \in \{1, \ldots, \omega\}.$$

Напомним, что автомат называется связным, если для произвольных различных состояний s, s` в его графе переходов существует путь из s в s`, либо существует путь из s` в s. Автомат называют перестановочным, если его частичные функции переходов осуществляют биекции его множества состояний. Несложно показывается, что связный перестановочный автомат является и сильно связ-

ным: для любой упорядоченной пары различных состояний s, s` в его графе переходов существует путь из s в s`.

В лемме 1 работы [2] доказано, что если общий наибольший делитель мощностей классов 1-неотличимых состояний перестановочного связного автомата равен единице, то автомат является приведенным [16].

Очевидно, рассматриваемый автомат A является связным перестановочным автоматом. Величины

$$\{ |\varphi^{-1}(y)|\cdot 2^{n-m},\ y\in Y\backslash\{y`\},\ |\varphi^{-1}(y`)|\cdot(2^{n-m}-1)\}$$

являются мощностями его классов 1-неотличимых состояний. Эти числа взаимно просты по условию. Следовательно, полноцикловый автомат A является приведенным автоматом (у него нет различных неотличимых состояний). Этот факт, очевидно, равносилен тому, что периоды его выходных последовательностей равны $\omega = 2^n-1$, что и требовалось доказать.

18.3. Полноцикловый автомат

В данном пункте предметом изучения будут полноцикловые автоматы вида $A = (S, Y, \delta, \lambda)$, $|S| = \omega$, $\omega \geq 2$, δ: $S\to S$. Функции выхода λ будут принадлежать некоторому классу функций. Пусть F: $S\to Y`$ – произвольное фиксированное сюръективное отображение S в некоторый алфавит Y`, $|Y`| \geq 2$.

Изучаемый *первый класс* $\lambda(F, m, L)$, $L\in\{1, 2, ...\}$, $m\in\{0, 1, ...\}$ выходных функций λ: $S\to Y$ полноцикловых автоматов определим так. Это множество всех функций λ: $S\to Y$, для которых из равенств

$$F(s) = F(s`)$$
$$\lambda(s) = \lambda(s`)$$
$$\lambda(\delta s) = \lambda(\delta s`)$$
$$.....$$
$$\lambda(\delta^m s) = \lambda(\delta^m s`)$$

вытекает равенство

$$F(\delta^{m+L}s) = F(\delta^{m+L}s`).$$

Обозначим через $A(s_1) = Q = y_1, y_2, ...$ выходную последовательность автомата $A = (S, Y, \delta, \lambda)$, отвечающую его начальному состоянию $s_1\in S$ ($y_j = \lambda(\delta^{j-1}s_1,\ j\in\{1, 2, ...\}$), а через W обозначим период этой последовательности. Введем вспомогательный автомат A`(S, Y`, δ, F). Напомним, что δ – заданное ранее полноцикловое преобра-

зование S. Через $A`(s_1) = Q` = y`_1, y`_2, ...$ обозначим выходную последовательность автомата A` для $s_1 \in S$, а через ω` – ее период.

Теорема 2. Пусть $\lambda \in \lambda(F, m, L)$, $m \geq 0$, $L \geq 1$, $|Y`| \geq 2$, $\omega` \geq d$,

$$\alpha = \max \text{НОК}(\alpha_1, \alpha_2, ..., \alpha_{L+m}),$$

где максимум наименьшего общего кратного берется по всем возможным значениям $\alpha_j \in \{1, ..., |Y`|\}$, $j \in \{1, ..., L+m\}$.

Тогда

$$W \geq \frac{d}{\alpha(L+m)}.$$

Доказательство. Доказательство основано на приводимых ниже леммах.

Лемма 1. Пусть ω` – период последовательности

$$Q` = y`_1, y`_2, ..., y`_j \in Y`;$$

r_j^L – период выборочной последовательности шага L, $L \geq 1$

$$y`_j, y`_{j+L}, y`_{j+2L}, ...$$

R(L) – период последовательности L-грамм

$$y^\wedge_1, y^\wedge_2, y^\wedge_3, ..., y^\wedge_j = y`_{(j-1)L+1}, y`_{(j-1)L+2}, ..., y`_{jL}, j \in \{1, 2, ...\}.$$

Тогда

$$\text{НОК}(\omega`, L) = L \cdot R(L),$$

где $R(L) = \text{НОК}(r_1^L, r_2^L, ..., r_L^L)$.

Доказательство. Ясно, что $R(L) = \text{НОК}(r_1^L, r_2^L, ..., r_L^L)$, $\omega` | LR(L)$, $L \mid LR(L)$, откуда вытекает,

$$\text{НОК}(\omega`, L) | L \cdot R(L).$$

С другой стороны,

$$\omega` | \frac{1}{L}(HOK(\omega`, L)),$$

следовательно,

$$\omega` \cdot L | (HOK(\omega`, L)).$$

Доказательство завершено.

Лемма 2. Пусть $\lambda \in \lambda(F, m, L)$, $m \geq 0$, $L \geq 1$, $|Y`| \geq 2$,

$$(\omega`, L+m) = k, \text{НОК}(k, W) = L,$$

r_j^L – период подпоследовательности $y`_j, y`_{j+L}, y`_{j+2L}, ...$ последовательности $y`_j, y`_{j+1}, y`_{j+2}, ...$; $y`_j = \lambda\delta^{j-1}s_1$. Тогда $r_j^L | \omega`$, все элементы $y`_j, y`_{j+L}, ..., y`_M$ различны ($M = j+(r_j^L - 1)L$), $r_j^L \leq |Y`|$, $r_j^L = r_{j+k}^L$, $j \in \{1, 2, ...\}$,

$$HOK(\omega`, L) = L \cdot \text{НОК}(r_j^L)_{j \in \{1, ..., k\}}.$$

Доказательство. Для любых целых $j \geq 1$, $k \geq 0$ имеем

$$\lambda(s_j) = \lambda(s_{j+kW})$$

$$\lambda(s_{j+1}) = \lambda(s_{j+1+kW})$$
$$.....$$
$$\lambda(s_{j+m}) = \lambda(s_{j+m+kW}).$$

Для каждого $j(0) \in \{1, 2, ...\}$ через $C(j(0))$ обозначим произвольное натуральное число, при котором

$$F(s_{j(0)}) = F(s_{j(0)+LC(j(0))}).$$

Тогда из определения множества $\lambda(F, m, L)$ вытекает

$$F(sj(0)+L+m) = F(sj(0)+LC(j(0))+L+m),$$

и итеративно получаем для любого целого $c \geq 0$

$$F(s_{j(0)+c(L+m)}) = F(s_{j(0)+LC(j(0))+c(L+m)}).$$

Используя $(\omega`, L+m) = k$, для любого целого $j \geq 0$ легко получить

$$F(s_{j(0)+jk}) = F(s_{j(0)+jk+LC(j(0))}).$$

Для $\varepsilon \in \{1, ..., k\}$ положим

$$m(\varepsilon) = \min(T(\varepsilon), T(\varepsilon + k), T(\varepsilon + 2k), ...),$$

где $T(\varepsilon+pk)$ есть минимальное натуральное число, при котором

$$F(s_{\varepsilon+pk}) = F(s_{\varepsilon+pk+LT(\varepsilon+pk)}).$$

Из доказанного выше имеем

$$F(s_{\varepsilon+pk}) = F(s_{\varepsilon+pk+Lm(\varepsilon)}),\ \varepsilon \in \{1, ..., k\},\ p \in \{0, 1, ...\}.$$

Используя это равенство и определение периода $r^L_{\varepsilon+pk}$ последовательности

$$F(s_{\varepsilon+pk}), F(s_{\varepsilon+pk+L}), ..., F(s_{\varepsilon+pk+jL}), ...,$$

получаем $r^L_{\varepsilon+pk} \mid m(\varepsilon)$. Из определения величины $m(\varepsilon)$ имеем

$$m(\varepsilon) \leq T(\varepsilon+pk),\ p \in \{0, 1, ...\}.$$

Очевидно,

$$T(\varepsilon+pk) \leq |Y`|,\ T(\varepsilon+pk) \leq r^L_{\varepsilon+pk},\ p \in \{0, 1, ...\}.$$

Следовательно,

$$m(\varepsilon) = r^L_{\varepsilon+pk},\ p \in \{0, 1, ...\},\ m(\varepsilon) \mid \omega`,\ m(\varepsilon) \leq |Y`|.$$

Используя лемму 1 и указанную связь величин $r^L_{\varepsilon+pk}$, $m(\varepsilon)$, получаем

$$НОК(\omega`, L) = L \cdot НОК(r^L_j)_{j \in \{1,...,L)} = L \cdot НОК(m(\varepsilon))_{\varepsilon \in \{1, .., k)}.$$

Лемма доказана.

Перейдем теперь к *доказательству теоремы 2.* По лемме 2 имеем

$$D \leq \omega` \leq НОК(\omega`, L) = L \cdot НОК(r^L_j)_{j \in \{1,...,k)} \leq k \cdot W \cdot \alpha \leq (L+m) \cdot W \cdot \alpha.$$

Откуда

$$W \geq \frac{d}{\alpha(L+m)}.$$

Доказательство теоремы завершено.

Из доказательств леммы 2 и теоремы 2 непосредственно вытекает

Теорема 3. При выполнении условий леммы 2

$$W \geq \frac{\omega`}{k\alpha^*}.$$

Здесь

$$\alpha^* = \max\text{НОК}(\alpha_1, \alpha_2, ..., \alpha_k),$$

где максимум берется по всем $\alpha_j \in \{1, ..., |Y`|\}$, $\alpha_j$ – делители $\omega`$, $j \in \{1, ..., k\}$.

Следствие 2. При выполнении условий леммы 2 и дополнительных условий: $\omega` = |S|$, $k = 1$ справедливы соотношения

$$|S| = W \cdot r_1^W,\ r_1^W = r_j^W,\ j \in \{1, 2, ...\},\ r_1^W \leq |Y`|.$$

Перейдем к рассмотрению второго класса выходных функций полноциклового автомата $A = (S, Y, \delta, \lambda)$, $|S| = \omega$, $\omega \geq 2$.

Пусть $Y``$ – некоторый алфавит, $Y` \subseteq Y``$, $\varphi: Y` \times Y` \to Y``$ – отображение, обладающее свойством: при любом $y`_1 \in Y`$ и любых $y`_2$, $y`_3$ из $Y`$, $y`_2 \neq y`_3$

$$\varphi(y`_1, y`_2) \neq \varphi(y`_1, y`_3),$$

то есть φ представимо в виде

$$\varphi(y`_1, y`_2) = \phi_{y`_1}(y`_2),$$

где $(\phi_{y`_1})_{y`_1 \in Y`}$ – инъективные отображения $Y`$ в $Y``$.

Будем говорить, что *периодическая последовательность*

$$y`_1, y`_2, ..., y`_j, ..., y`_j \in Y`$$

удовлетворяет введенному отображению φ, если для любого j

$$\varphi(y`_1, y`_2) = \varphi(y`_j, y`_{j+1}).$$

Очевидно, что такая последовательность на своем периоде r содержит ровно r различных элементов из $Y`$.

Среди всех периодических последовательностей элементов $Y`$, удовлетворяющих $\varphi$, выберем k периодических последовательностей так, чтобы наименьшее общее кратное их периодов было максимальным. Обозначим эту величину через $\alpha`(k)$, а через $\alpha`(Y`)$ обозначим наименьшее общее кратное периодов всех периодических последовательностей элементов $Y`$, удовлетворяющих φ.

Пусть, как и ранее, F: S→Y`, |Y`| ≥ 2. Второй изучаемый класс λ(φ, F, m, L) выходных функций полноциклового автомата A = (S, Y, δ, λ), |S| = ω, ω ≥ 2 определим так. Это функции λ: S→Y, для которых из условия

$$\lambda(s) = \lambda(s`)$$
$$\lambda(\delta s) = \lambda(\delta s`)$$
$$\dots\dots\dots\dots\dots$$
$$\lambda(\delta^m s) = \lambda(\delta^m s`)$$

вытекает равенство

$$\varphi(F(s), F(s`)) = \varphi(F(\delta^{m+L}s), F(\delta^{m+L}s`)).$$

Теорема 4. Пусть W – период выходной последовательности y_1, y_2, ... полноциклового автомата A = (S, Y, δ, λ), |S| = ω, ω ≥ 2, λ∈λ(φ, F, m, L); ω` – период выходной последовательности $y`_1$, $y`_2$, ... автомата A` = (S, Y, δ, F); k = (L+m, ω`). Тогда

1) для любых c(1), c(2)∈{0, 1, ...}

$$\varphi(y`_j, y`_{j+Wc(1)}) = \varphi(y`_{j+kc(2)}, y`_{j+k(c(2)+Wc(1))});$$

2) $W \ge \frac{\omega`}{k\alpha`(k)} \ge \frac{\omega`}{(L+m)\alpha`(Y`)}$.

Доказательство. Положим N=НОК(k,W). Аналогично доказательству леммы 2 легко показывается, что при c(1), c(2) справедливо равенство

$$\varphi(y`_j, y`_{j+c(1)W}) = \varphi(y`_{j+kc(2)}, y`_{j+kc(2)+Wc(1)}),$$

и, следовательно, для любого j

$$\varphi(y`_j, y`_{j+N}) = \varphi(y`_{j+N}, y`_{j+2N}).$$

Очевидно, последовательность

$$y`_j, y`_{j+N}, \dots, y`_{j+cN}, \dots$$

удовлетворяет φ и, по определению величины α`(k),

$$HOK(r_j^N)_{j\in\{1,\dots k\}} \le \alpha`(k).$$

Используя лемму 2, получаем

$$\text{НОК}(\omega`, N) = N \cdot HOK(r_j^N)_{j\in\{1,\dots k\}} \le N\cdot\alpha`(k) \le N\cdot\alpha`(Y`)$$

и

$$\omega` \le \text{НОК}(\omega`, N) \le N\alpha`(k) \le N\alpha`(Y`).$$

Следовательно,

$$W \ge \frac{\omega`}{k\alpha`(k)} \ge \frac{\omega`}{(L+m)\alpha`(Y`)}.$$

Доказательство теоремы завершено.

Приведем *одно из возможных применений* утверждения теоремы 4. Пусть P = x(1), x(2), ... – периодическая последовательность

периода ω, x(j)∈X, Y` = {$\Pi_x$: x∈X} – множество подстановок некоторой степени. Мы пишем, что {$\Pi_x$: x∈X} – множество, в частности, $\Pi_x \neq \Pi_{x`}$ при x ≠ x`. Будем предполагать также, что подстановки из Y` коммутируют: $\Pi_x\Pi_{x`} = \Pi_{x`}\Pi_x$, x, x`∈X. Положим

$s_j = x(j), x(j+1), ..., x(\omega), x(\omega+1), ..., x(\omega+j-1)$; $S = \{s_1, s_2, ..., s_\omega\}$;

$\Phi_1(s_j) = \Pi_{x(j)} \cdot \Pi_{x(j+1)} \cdot ... \cdot \Pi_{x(j+L-1)}$; T: $s_j \to s_{j+1}$, j∈{1, ..., ω–1}, $s_\omega \to s_1$,

где L ≥ 2, (L, ω) = 1. Таким образом, нами определен автомат A = (S, Y, T, Φ_1), где Y = <{Π_x: x∈X}> – группа, порожденная подстановками {Π_x: x∈X}.

Возможное применение теоремы 4 состоит в возможности оценки периода W последовательности

$$\Phi_1(s_1), \Phi_1(s_2), ... = y_1, y_2, ...$$

Очевидно, что из условия

$$\Pi_{x(j)} \cdot \Pi_{x(j+1)} \cdot ... \cdot \Pi_{x(j+L-1)} = \Pi_{x(p)} \cdot \Pi_{x(p+1)} \cdot ... \cdot \Pi_{x(p+L-1)},$$

$$\Pi_{x(j+1)} \cdot \Pi_{x(j+2)} \cdot ... \cdot \Pi_{x(j+L)} = \Pi_{x(p+1)} \cdot \Pi_{x(p+2)} \cdot ... \cdot \Pi_{x(p+L)}$$

следует

$$\Pi_{x(j)}\Pi^{-1}_{x(p)} = \Pi_{x(j+L)}\Pi^{-1}_{x(p+L)}.$$

Положим

$$F(s_j) = \Pi_{x(j)}, j\in\{1, ..., \omega\}; \quad \varphi(\Pi_x, \Pi_{x`}) = \Pi_x\Pi^{-1}_{x`}.$$

Таким образом, $\Phi_1 \in \lambda(\varphi, F, 1, L-1)$. Заметим, что

$$\omega` = \omega, (L, \omega`) = k = 1, N = НОК(k, W) = W.$$

По теореме 4 получаем

$$\Pi_{x(j)}\Pi^{-1}_{x(j+W)} = \Pi_{x(j+c)}\Pi^{-1}_{x(j+W+c)} = \Pi, \quad c\in\{0, 1, ...\},$$

где Π – некоторая подстановка.

Пусть r_j^W – период последовательности

$$\Pi_{x(j)}, \Pi_{x(j+W)}, \Pi_{x(j+2W)}, ..., j\in\{1, 2, ...\}.$$

Очевидно, что $r_j^W | \omega$. Заметим, что

$$(\Pi_{x(j)} \cdot \Pi_{x(j+1)} \cdot ... \cdot \Pi_{x(j+L-1)})(\Pi_{x(j+W)} \cdot \Pi_{x(j+1+W)} \cdot ... \cdot \Pi_{x(j+L-1+W)})^{-1} = E,$$

где E – тождественная подстановка. Откуда получаем: $\Pi^L = E$. Следовательно, $r_j^W | L$. Так как (ω, L) = 1, то $r_j^W = 1$. По лемме 2

$$НОК(\omega, W) = \omega r_1^W = W.$$

Таким образом, определено значение W, а именно: W = ω. Случай (L, ω) = d ≠ 1, d ≠ L рассматривается аналогично с помощью рассмотрения d-грамм последовательности P = x(1), x(2), ... в качестве нового алфавита X.

Практически доказан более общий результат, формулировка которого не вызывает затруднений. Дело в том, что была использо-

вана лишь абелевость группы $<\{\Pi_x: x\in X\}>$ и ее операция $(\cdot)$ в этой конечной группе. Таким образом, из приведенного результата легко непосредственно вытекает следующее утверждение. Пусть P = x(1), x(2), ... – периодическая последовательность элементов конечного поля (+) – аддитивная операция поля, ω – период последовательности P. Тогда период последовательности

$$\Phi_1(s_1), \Phi_1(s_2), ...,$$

где

$$\Phi_1(s_j) = x(j)+x(j+1)+...+ x(j+L-1), j\in\{1, 2, ...\}, (L, \omega) = 1, L \geq 2,$$

равен ω.

18.4. Обратимый автомат

Назовем автомат A = (X, S, Y, h, f), |X| = |Y|, h: X×S→S, f: S×X→Y *обратимым*, если ограничения f_s: {s}×X→Y отображения f биективны при любом s∈S.

Теорема 5. Пусть A = (X, S, Y, h, f), |X| = |Y| – обратимый автомат, ω – период его входной последовательности P, T = kω – период периодической последовательности состояний $A_M(s, P)$, отвечающей входу P и начальному состоянию s, W – период выходной последовательности A(s, P) автомата A. Тогда

$$W \geq \frac{k\omega}{|S|}.$$

Доказательство. Рассмотрим вспомогательный автомат A^{-1} = (Y, S, X, h^, f^), который назовем обратным к автомату A. Здесь У, X – соответственно входной и выходной алфавит автомата A^{-1}:

$$h^(y, s) = h(s, f_s^{-1}(y)),\ f^(s, y) = f_s^{-1}(y),\ s\in S,\ y\in Y.$$

Обратный автомат является обратимым автоматом и обладает свойством: если

$$A(s, x_1, x_2, ..., x_c) = y_1, y_2, ..., y_c,\ c\in\{1, 2, ...\},$$

то

$$A^{-1}(s, y_1, y_2, ..., y_c) = x_1, x_2, ..., x_c,$$

$$A_M(s, x_1, x_2, ..., x_c) = A_M^{-1}(s, y_1, y_2, ...y_c).$$

Рассмотрим последовательности P, $A_M(s, P)$, A(s, P) периодов ω, T, W соответственно. Для произвольного автомата A справедливо

W|НОК(ω,T). Следовательно, используя условие T = kω, имеем W|kω. Поэтому период T последовательности $A_M^{-1}(s, A(s,P))$ = = A_M(s, P) кратен W с коэффициентом кратности k` ≤ |S|, то есть T = k`W, откуда следует утверждение теоремы

$$W = \frac{k\omega}{k`} \geq \frac{k\omega}{|S|}.$$

18.5. Обобщенный узел выборки

Через X обозначим некий алфавит, x∈X, а через X^{∞} – множество всех бесконечных последовательностей алфавита X. Нас будут интересовать периодические последовательности из X^{∞}. Множество всех *чисто периодических последовательностей* из X^{∞} обозначим через $X^{\infty}_{п}$.

Определение 2. Обобщенным узлом выборки шага H (ОУВ шага H), H∈{1, 2, ...} с параметром (k_1, k_2, ..., k_m; H), m ≤H, k_j∈{1, 2, ..., H}, $k_1 < k_2 <, ..., < k_m$ назовем устройство, реализующее отображение φ: $X^{\infty} \rightarrow X^{\infty}$ вида

φ(x_1, x_2, ...) = x(k_1), x(k_2), ..., x(k_m), x(H+k_1), x(H+k_2), ..., x(H+k_m), ..., (jH+k_1), x(jH+k_2), ..., x(jH+k_m), ...

Далее мы сохраняем обозначение φ для его ограничения на начальных словах x(1), x(2), ..., x(L) бесконечной последовательности x(1), x(2), ...

Для введенного устройства ОУВ рассмотрим вектор (ε(1), ε(2), ..., ε(H)) из F_2^H, F_2 = {0, 1}, где ε_j = 1, j∈{1, ..., H} тогда и только тогда, когда j∈{k_1, k_2, ..., k_m}. Очевидно, такой вектор однозначно определяет ОУВ с параметром (k_1, k_2, ..., k_m; H). Рассмотрим *вспомогательную* двоичную последовательность

ε(1), ε(2), ..., ε(H), ε(1), ε(2), ..., ε(H), ε(1), ε(2), ..., ε(H), ... (20)

Элементы данной последовательности повторяются через H шагов. Поэтому период этой последовательности является делителем величины H. Далее мы рассматриваем только так называемые *«приведенные» ОУВ шага H, то есть ОУВ, для которых период последовательности* (20) *совпадает с H.*

Теорема 6. Пусть x(1), x(2), ... – периодическая входная последовательность периода ω устройства ОУВ с параметром. Тогда период W выходной последовательности ОУВ φ((x(1), x(2), ...) = x`(1), x`(2), ... является делителем величины

$$\frac{HOK(\omega, H)}{H} m .$$

Если дополнительно (H, ω) = 1, то период W кратен ω, W = cω, где c | m.

Если выполнено еще одно дополнительное условие: ω > 3H–2, то W = mω.

Доказательство. Для заданного ОУВ рассмотрим двух компонентную последовательность

$$\begin{matrix} x(1), x(2), \ldots \\ \varepsilon(1), \varepsilon(2), \ldots \end{matrix}, \qquad (21)$$

где ε(1), ε(2), ... – вспомогательная периодическая последовательность периода H, соответствующая параметру (k_1, k_2, ..., k_m; H). Напомним, что здесь для j ≤ m:

ε(j) = 1 при j∈{k_1, k_2, ..., k_m} и ε(j) = 0 в противном случае.

Период последовательности (21) равен N = НОК(ω, H), так как мы рассматриваем приведенный обобщенный узел выборки. В связи с чем для отображения φ, соответствующего ОУВ, при любом K

φ(x(1), x(2), ..., x(N)) = φ(x(1+KN), x(2), ..., x(N+KN).

При этом число элементов |φ(x(1), x(2), ..., x(N))| в выходном слове φ(x(1), x(2), ..., x(N)) ОУВ равно величине

$$\frac{H.O.K.(\omega, N)}{H} m .$$

Поэтому период W выходной последовательности ОУВ

ОУВ(x(1), x(2), ...) = x`(1), x`(2), ...

делит величину

$$\frac{H.O.K.(\omega, N)}{H} m .$$

Предположим теперь, что выполнено первое дополнительное условие теоремы: (H, ω) = 1. Имеем W|ωH. Выборочная последовательность x(k_1), x(k_1+H), x(k_1+2H), ... последовательности x(1), x(2), ... совпадает с выборочной последовательностью x`(1), x`(1+m), x`(1+2m), ... выходной последовательности φ(x(1), x(2), ...) ОУВ и период первой из них есть ω, так как (ω, H) = 1. В связи с чем период второй последовательности равен ω. Следовательно, период W последовательности φ(x(1), x(2), ...) кратен ω, то есть W = cω, c∈{1, 2, ..., m}, c|m.

Для завершения доказательства теоремы осталось показать, что при выполнении всех ее условий в случае $m \geq 2$ обязательно $c = m$. Пусть $m \geq 2$. Имеем

$$x`(j) = x`(j+cm),\ j \in \{1, 2, ...\}.$$

Возможны два случая:

1) $m | c\omega$, $c\omega = qm$;
2) m не делит $c\omega$, $c\omega = qm+R$, $0 < R < m$.

Предположим сначала, что имеет место второй случай. Рассмотрим индексы j вида $j = c`m+R`$, $1 \leq R` \leq m$, $c \in \{0, 1, ...\}$, а $c\omega$ представим в виде $c\omega = qm+R$, $R < m$, $R \neq 0$. Для любого $c`$ имеем основное равенство

$$x`(c`m+R`) = x`(c`m+R`+qm+R).$$

Для записи последнего равенства в обозначениях исходной последовательности используем следующие вспомогательные обозначения:

$$\varepsilon(R`+R, m) = 0, \text{ если } R`+R \leq m,$$
$$\varepsilon(R`+R, m) = 1, \text{ если } R`+R > m;$$

величина $k(R`+R, m)$ определена равенством

$$m\varepsilon(R`+R, m)+ k(R`+R, m) = R`+R.$$

Заметим, что $1 \leq k(R`+R, m) \leq m$.

По определению последовательности $\varphi(x(1), x(2), ...)$ основное равенство можно записать в виде

$$x(c`H+k_{R`}) = x(c`H+qH+H\varepsilon(R`+R, m)+ k(R`+R, m)).$$

Так как $(H, \omega) = 1$, то отсюда вытекает следующая система равенств

$$x(k_{R`}+j) = x(qH+H\varepsilon(R`+R, m)+ k(R`+R, m)+j,\ j \in \{0, 1, ...\}. \quad (22)$$

Следовательно,

$$\omega \mid qH+H\varepsilon(R`+R, m)+ k(R`+R, m) - k_{R`}$$

при любом $R` \in \{1, ..., m\}$. В частности, для произвольных r, r` из {1, ..., m}, $m \geq 2$ имеем

$$\omega \mid (H\varepsilon(r+R, m)+ k(r+R, m) - k_r - (H\varepsilon(r`+R, m)+ k(r`+R, m) - k_{r`})).$$

По условию, $\omega > 3H-2$, поэтому при любых r, r` из {1, ..., m} из этого факта следует

$$H\varepsilon(r+R, m)+k(r+R, m) - k_r = H\varepsilon(r`+R, m)+ k(r`+R, m) - k_{r`}.$$

В частности, имеем систему равенств

$$H\varepsilon(R+1, m)+ k(R+1 ,m) - k_1 = H\varepsilon(R+j, m)+ k(R+j, m) - k_j,\ j \in \{1, ..., m\}.$$

Обозначим последнюю величину через t. Из данной системы равенств вытекает, что период вспомогательной последовательности

$\varepsilon(1), \varepsilon(2), ...,$ соответствующей параметру $(k_1, k_2, ..., k_m; H)$ ОУВ, делит t, причем $\varepsilon(R+1, m)=0$, так как $R < m$. Поэтому $t = k(R+1, m) - k_1$, откуда

$$t < H.$$

Следовательно, рассматриваемый обобщенный узел выборки не является приведенным. Полученное противоречие говорит о том, что возможен только первый случай: $m|c\omega$, то есть $R = 0$. Из системы равенств (22) получаем, что при любом j

$$x(k_R+j) = x(qH+k_R+j), \quad R\in\{1, ..., m\}.$$

Поэтому период $W = c\omega$ делит величину qH, но $(\omega, H) = 1$, откуда получаем $\omega|q$. Используя эти факты и равенство $c\omega = qm$, где $c \le m$, получаем $c = m$. Доказательство теоремы завершено.

Глава 19. КЛАССЫ АВТОМАТОВ С ГАРАНТИРОВАННЫМИ ПАРАМЕТРАМИ ПОДПЕРИОДА ВЫХОДНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

Введено понятие подпериода периодической последовательности, отражающее наличие в последовательности подряд повторяющихся мультиграмм. Доказаны оценки параметров подпериодов выходных последовательностей для автоматов Медведева и класса неавтономных автоматов, выходные последовательности которых имеют вид: $y_1, y_2, ..., y_j, ..., y_j = \varphi(x_j, x_{j+1}, ..., x_{j+L-1})$, $L \geq 2$, $\varphi: X^L \to Y$, X – входной алфавит,Y – выходной алфавит, $x_j \in X$, $y_j \in Y$, $j \in \{1, 2, ...\}$.

Как ранее отмечалось, в науке и технике (и, в частности, в различных системах обеспечения безопасности) широко применяются генераторы псевдослучайных последовательностей [14]. Так, например, эти генераторы используются в синхронных поточных криптосхемах.

Одно из требований к этим генераторам состоит в том, что последовательность вырабатываемая генератором должна иметь большой период.

Другое, не менее важное, требование состоит в том, что в управляющей гамме должны отсутствовать простые аналитические зависимости между близко расположенными знаками. В числе теоретико-автоматных терминов этой главы был приведен вариант одной возможной формализации качественного понятия простых аналитических зависимостей между близко расположенными знаками последовательности, состоящей в введении понятия подпериода изучаемой последовательности, отражающего наличие в последовательности подряд идущих повторяющихся мультиграмм.

Доказываются оценки параметров подпериодов выходных последовательностей для автоматов Медведева, класса неавтономных автоматов, моделируемых так называемыми кодирующими устройствами с конечной памятью [7], и класса обратимых автоматов. (Основные результаты, описанные в данной главе, были сформулированы в [7].)

19.1. Основные обозначения и понятие подпериода последовательности

Напомним необходимые нам понятия:

– $A = (X, S, Y, h, f)$ – конечный автомат с $|X| \geq 2$, $|Y| \geq 2$.

– $A_M(s, P) = s_1, s_2, \ldots, s_j, \ldots$ – последовательность состояний автомата A, отвечающая его входной последовательности P и начальному состоянию $s = s_1$ из S;

– для входного слова $P = x(1), x(2), \ldots, x(j) \ldots,$ и начального состояния $s \in S$ автомата $s_j = h_{x(j-1)} \ldots h_{x(1)} s_1$, $y_j = f_j\, h_{x(j-1)} \ldots h_{x(1)} s_1$;

– $A = (X, S, Y, h, E) = (X, S, Y, (h_x)_{x \in X}, E)$ – автомат Медведева, $Y = S$, выходная функция $E: S \to S$ является тождественным отображением S в S. Выходная последовательность такого автомата совпадает с его последовательностью состояний.

Под периодической последовательностью элементов конечного алфавита Y в данном разделе понимается чисто периодическая последовательность $y_1, y_2, \ldots, y_j, \ldots$: существует d, при котором $y_j = y_{j+d}$, $j \in \{1, 2, \ldots\}$. Под периодом последовательности понимается ее минимальный период.

Для периодической последовательности $Q = y_1, y_2, \ldots, y_j, \ldots$ положим $Q^j = y_j, y_{j+1}, y_{j+2}, \ldots$, в частности, $Q^1 = Q$. Через $Q^j]_m$ обозначим m-грамму

$$y_j, y_{j+1}, \ldots, y_{j+m-1},$$

стоящую в Q на j-м месте.

Определение 1. Периодическая последовательность $Q = y_1, y_2, \ldots$ элементов конечного алфавита Y, $|Y| \geq 2$ периода W имеет подпериод t кратности k, если найдется $j \in \{1, \ldots, W\}$, при котором слово $Q^j]_W = y_j, y_{j+1}, \ldots, y_{j+W-1}$ представимо в виде следующей конкатенации слов

$$Q^j]_W = \overline{y}, \overline{y}, \ldots, \overline{y}, \overline{\overline{y}},$$

где $\overline{y} \in Y^t$, $\overline{y} = y_j, y_{j+1}, \ldots, y_{j+t-1}$, $\overline{\overline{y}} \in Y^{W-kt}$, $\overline{\overline{y}} = y_{j+kt}, y_{j+kt+1}, \ldots, y_{j+W-1}$, причем $k \geq 2$, а $\overline{\overline{y}}$ возможно и пустое слово, $Y^0 = \varnothing$.

Возвращаясь к требованиям к генераторам псевдослучайных последовательностей, следует отметить, что представляют интерес оценки не величины t подпериода кратности k, а оценки величины kt, адекватно отражающей длину перекрытий в поточных шифрах [13]. Отметим также, что получение оценок вида $kt \leq C$ может быть использовано для получения оценки подпериода t заданной последовательности $t \leq \frac{C}{k} \leq \frac{C}{2}$.

Обращаем внимание на то обстоятельство, что подпериод и его кратность заданной периодической последовательности определены неоднозначно. Очевидно и обобщение данного понятия на случай

смешанно периодических последовательностей и на случай непериодических последовательностей.

19.2. Автомат Медведева

Определение 2. Состояние s автомата A = (X, S, Y, h, f) называется внутренне автономным состоянием относительно множества $M \subseteq X^t$, если при любом $j \in \{1, ..., t\}$ для любой пары слов P = x(1), x(2), ..., x(t), P` = x`(1), x`(2), ..., x`(t) из M

$$h_{x(j)}h_{x(j-1)}...h_{x(1)}s = h_{x`(j)}h_{x`(j-1)}...h_{x`(1)}s.$$

Через $A\langle s\rangle = (X, S_s, Y, h, f)$ обозначим связную компоненту автомата A, порожденную состоянием $s \in S$.

Теорема 1. Пусть A = (X, S, Y, h, E) – автомат Медведева, A(s, P) = Q = $y_1, y_2, ...$ – периодическая выходная последовательность автомата A периода W и подпериода t кратности k, отвечающая начальному состоянию $s \in S$ и входной периодической последовательности P = x(1), x(2), ... периода ω. Тогда найдутся $s` \in S_s$ и $j \in \{1, ..., \omega\}$, при которых:

1) состояние s` внутренне автономно относительно следующего множества t-грамм

$$\left\{ P^{j+\nu t+\left[\frac{\nu}{k}\right]H}]_t \ , \nu \in \{0,1,...\} \right\},$$

где $\left[\frac{\nu}{k}\right]$ – целая часть числа $\frac{\nu}{k}$, H = W–kt;

2) состояние s` внутренне автономно относительно последовательностей $P^j]_{(k-1)t}$ и $P^{j+t}]_{(k-1)t}$.

Доказательство теоремы проведем с помощью вспомогательного утверждения, представляющего самостоятельный интерес. Обозначим через $M_t(P^1)$ – множество t-грамм последовательности P^1 вида

$$P^j]_t = x(j), x(j+1), ..., x(j+t-1), j \in \{1, 2,...\},$$

аналогично для $A(s, P^1) = Q^1 = y_1, y_2, ...$

$$M_t(Q^1) = \{Q^j]_t, j \in \{1, 2, ...\}.$$

Пусть $\sigma = \sigma(P^1, s, t)$ – бинарное отношение на $M_t(P^1) \times M_t(Q^1)$:

$$(x`(1), x`(2), ..., x`(t))\sigma(y`_1, y`_2, ..., y`_t)$$

тогда и только тогда, когда существует $j \in \{1, 2, ...\}$, при котором

$$(x(j), x(j+1), ..., x(j+t-1))=(x`(1), x`(2), ..., x`(t)),$$

$$(y_j, y_{j+1}, ..., y_{j+t-1}) = (y`_1, y`_2, ..., y`_t).$$

Через $\sigma^{-1}(y`_1, y`_2, ..., y`_t)$ обозначим прообраз элемента $(y`_1, y`_2, ..., y`_t)$ отношения σ.

Рассмотрим еще одно бинарное отношение $\sigma_{A<s>}$ на $X^t \times Y^t$, положив

$$(x`(1), x`(2), ..., x`(t))\ \sigma_{A<s>}(y`_1, y`_2, ..., y`_t),$$

тогда и только тогда, когда найдется $s` \in S_s$, при котором

$$A(s`, x`(1), x`(2), ..., x`(t)) = y`_1, y`_2, ..., y`_t.$$

Определение 1. Множество слов $M \subseteq X^t$ назовем неотличимым множеством слов относительно A<s>, если найдется слово $(y`_1, y`_2, ..., y`_t) \in Y^t$, при котором

$$M \subseteq \sigma^{-1}_{A<s>}(y`_1, y`_2, ..., y`_t).$$

Лемма 1. Пусть $P^1 = x(1), x(2), ...$ – периодическая входная последовательность периода ω автомата A; $A(s, P^1) = Q^1 = y_1, y_2, ...$ – периодическая выходная последовательность периода $W = kt+H$ и подпериода t кратности k. Тогда найдется $j \in \{1, 2, ..., W\}$, при котором:

1) множество t-грамм

$$M(s, P^1) = \left\{ P^{j+\nu t+\left[\frac{\nu}{k}\right]H}]_t \ , \nu \in \{0,1,...\} \right\}$$

неотличимо относительно A<s>, в частности, следующее множество слов неотличимо относительно A<s>:

$$\left\{ P^{j+cd+\left[\frac{cn(1)}{k}\right]H}]_t \ , c \in \{0,1,...\} \right\},$$

где $d=(t,\omega)$, а натуральное число n(1) определяется из условия: найдется натуральное число n(2), при котором $tn(1) - \omega n(2) = d$;

2) слова $P^j]_{(k-1)t}$ и $P^{j+t}]_{(k-1)t}$ неотличимы относительно A<s>.

Доказательство. Выберем j, при котором

$$Q^j]_W = \bar{\bar{y}}, \bar{\bar{y}}, ..., \bar{\bar{y}}, \bar{\bar{y}},$$

где $\bar{y} \in Y^t$, $\bar{y} = y_j, y_{j+1}, ..., y_{j+t-1}$, $\bar{\bar{y}} \in Y^H$, $\bar{\bar{y}} = y_{j+kt}, y_{j+kt+1}, ..., y_{j+W-1}$. Тогда при любом $\nu \in \{0, 1, ...\}$

$$Q^j]_t = Q^{j+\nu t+\left[\frac{\nu}{k}\right]H}]_t .$$

Следовательно,

$$P^{j+\nu t+\left[\frac{\nu}{k}\right]H}]_t \sigma \bar{y} .$$

Воспользовавшись включением

$$\sigma^{-1}(y_i, y_{i+1}, ..., y_{i+t-1}) \subseteq \sigma^{-1}_{A<s>}(y_i, y_{i+1}, ..., y_{i+t-1}),\ i \in \{1, 2, ...\},$$

заключаем, что множество слов $M(s, P^1)$ неотличимо относительно $A<s>$. Полагая теперь $\nu = cn(1)$, $c \in \{0, 1, ...\}$, заключаем, что множество

$$\left\{ P^{j+\nu t+\left[\frac{\nu}{k}\right]H}]_t \ ,\nu = cn(1),\ c \in \{0,1,...\} \right\} = \left\{ P^{j+cd+\left[\frac{cn(1)}{k}\right]H}]_t \ ,\ c \in \{0,1,...\} \right\},$$

являясь подмножеством множества $M(s, P^1)$ также неотличимо относительно $A<s>$.

Пункт 2 леммы доказывается аналогично.

Утверждение теоремы 1 непосредственно вытекает из определений 2, 3 и леммы 1.

Говорят, что автомат A не имеет *параллельных дуг на контурах*, если для всех состояний s графа переходов автомата A, лежащих на контурах графа, выполняется неравенство

$$h(x, s) \neq h(x`, s)$$

при любых x, x` из X, $x \neq x`$.

Назовем *степенью различимости R(P) периодической последовательности* $P = x(1), x(2), ...$ минимальное число r, такое, что все r-граммы последовательности P, взятые на ее периоде, различны.

Следствие 1. Пусть $A = (X, S, Y, h, E)$ – автомат Медведева; $A(s, P) = Q = y_1, y_2, ...$ – периодическая выходная последовательность автомата A периода W и подпериода t кратности k, отвечающая начальному состоянию $s \in S$ и входной периодической последовательности $P = x(1), x(2), ...$ периода ω, $t < \omega$; автомат $A<s>$ не имеет параллельных дуг на контурах. Тогда

$$Kt \leq 2R(P).$$

Доказательство. По теореме 1 найдутся $j \in \{1, ..., \omega\}$ и $s` \in S_s$, которое внутренне автономно относительно (k–1)t-грамм $P^j]_{(k-1)t}$ и $P^{j+t}]_{(k-1)t}$. Так как $A<s>$ не имеет параллельных дуг на контурах, то

$$P^j]_{(k-1)t-1} = P^{j+t}]_{(k-1)t-1}.$$

По условию $t < \omega$, поэтому

$$(k-1)t-1 < R(P).$$

В частности, при k = 2

$$t \leq R(P) \text{ и } kt \leq 2R(P).$$

При $k \geq 3$

$$kt-2 < 2(k-1)t-2 < 2R(P),$$

или

$$kt \leq 2R(P).$$

Следствие доказано.

Рассмотрим один из возможных примеров применения следствия 1. Пусть автомат A_1 моделирует получение линейной рекуррентной последовательности максимального периода $q^n - 1$ над полем из q элементов, а перестановочный автомат A_2 моделирует функционирование регистра сдвига с обратной связью [13. – С. 208]. Рассмотрим последовательное соединение $B = A_1 \rightarrow A_2$ (рис. 17).

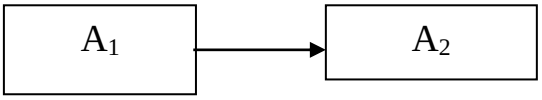

Рис. 17

автоматов A_1 и A_2. Если $Q = s_1, s_2, \ldots$ – последовательность состояний автомата A_2, отвечающая некоторому начальному состоянию автомата B, имеющая подпериод t кратности k, то по следствию 1 заключаем: либо t кратно $q^n - 1$, либо $kt \le 2n$, в частности, $t \le n$.

19.3. Кодирующее устройство с конечной памятью (проходная линия задержки с функцией усложнения)

Пусть X, Y – конечные множества, $|X| \ge 2$, $|Y| \ge 2$, $\varphi: X^L \rightarrow Y$, $L \in \{2, 3, \ldots\}$. Рассматриваемая задача состоит в получении оценок параметров подпериода W последовательности $y_1, y_2, \ldots, y_j, \ldots$,

$$y_j = \varphi(x_j, x_{j+1}, \ldots, x_{j+L-1}),\ j \in \{1, 2, \ldots\}$$

для заданной периодической последовательности $P = x_1, x_2, \ldots$ со степенью различимости R(P). Устройство, перерабатывающее входную последовательность по указанному закону, называют кодирующим устройством с конечной памятью и без обратной связи [20].

Функцию φ называют *сильно k-равновероятной* [31], если при любом наборе $y_1, y_2, \ldots, y_k$ из Y^k система уравнений

$$\varphi(x_1, x_2, \ldots, x_L) = y_1$$
$$\varphi(x_2, x_3, \ldots, x_{L+1}) = y_2$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$
$$\varphi(x_k, x_{k+1}, \ldots, x_{k+L-1}) = y_k$$

имеет ровно $\frac{|X|^{k+L-1}}{|Y|^k}$ решений. Если функция сильно k-равновероятна при любом k, то ее называют сильно равновероятной.

Теорема 1. Пусть $L \geq 2$, $\varphi: X^L \to Y$ – сильно k-равновероятная функция, $k+L-1 \geq R(P)$, где $R(P)$ – степень различимости периодической последовательности $P = x_1, x_2, \ldots$ периода ω. Тогда при $k \leq t$ справедлива следующая оценка кратности $k(0)$

$$k(0) \leq \frac{|X|^{k+L-1}}{|Y|^k}$$

подпериода t последовательности $y_1, y_2, \ldots, y_j, \ldots, y_j = \varphi(x_j, x_{j+1}, \ldots, x_{j+L-1})$, $j \in \{1, 2, \ldots\}$.

Доказательство. Пусть W – период последовательность $Q = Q1 = y_1, y_2, \ldots, y_j, \ldots$ По условию найдется $j \in \{1, \ldots, W\}$, при котором

$$Q^j]_W = \overline{\overline{y}, \overline{y}, \ldots, \overline{y}, \overline{\overline{y}}},$$

где $\overline{y} \in Y^t$, $\overline{y} = y_j, y_{j+1}, \ldots, y_{j+t-1}$, $\overline{\overline{y}} \in Y^{W-tk(0)}$, причем $k \geq 2$. Очевидно, слова вида

$$P^{j+ct}]_{k+L-1},\ c \in \{0,1,\ldots,k(0)-1\}$$

длины $k+L-1$ являются решениями системы уравнений

$$\varphi(x_1, x_2, \ldots, x_L) = y_j$$
$$\varphi(x_2, x_3, \ldots, x_{L+1}) = y_{j+1}$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$
$$\varphi(x_k, x_{k+1}, \ldots, x_{k+L-1}) = y_{j+k-1}$$

при $k \leq t$, причем указанные слова различны в силу условий теоремы: $k+L-1 \geq R(P)$, кроме того, $W|\omega$. Число решений выписанной системы уравнений относительно $x_i \in X$ равно величине $\frac{|X|^{k+L-1}}{|Y|^k}$, так как функция φ сильно k-равновероятна. В связи с указанными обстоятельствами должно выполняться неравенство

$$k(0) \leq \frac{|X|^{k+L-1}}{|Y|^k}.$$

Замечание 1. При использовании доказанной теоремы полезно иметь в виду, что сильно k-равновероятная функция является и сильно k`-равновероятной при любом $k` \leq k$. Утверждение данной теоремы при $t > k > R(P)-L+1$ дает верхнюю оценку $k(0)$, при известной нижней оценке $R(P)-L+1$ подпериода t последовательности $Q = y_1, y_2, \ldots, y_j, \ldots, y_j = \varphi(x_j, x_{j+1}, \ldots, x_{j+L-1})$, $j \in \{1, 2, \ldots\}$. Из нее вытекает, что при $k = t$ и

$$k(0) > \frac{|X|^{t+L-1}}{|Y|^t}$$

справедлива верхняя оценка $t < R(P)–L+1$ подпериода t последовательности Q.

Рассмотрим частный класс проходных линий задержек с функцией усложнения. Для $m \geq 2$, $L \geq 2$ обозначим через $\lambda(m, L)$ множество всех отображений $\lambda: X^L \to Y$, для которых из равенств

$$x_1 = x`_1$$
$$\lambda(x_1, x_2, ..., x_L) = \lambda(x`_1, x`_2, ..., x`_L)$$
$$\lambda(x_2, x_3, ..., x_L, x_{L+1}) = \lambda(x`_2, x`_3, ..., x`_L, x`_{L+1})$$
$$.....$$
$$\lambda(x_{m-1}, x_m, ..., x_{m+L-2}) = \lambda(x`_{m-1}, x`_m, ..., x`_{m+L-2})$$

для $(x_{m-1}, x_m, ..., x_{m+L-2}) \in X^{m+L-2}$, $(x`_{m-1}, x`_m, ..., x`_{m+L-2}) \in X^{m+L-2}$ вытекает

$$x_{m+L-2} = x`_{m+L-2}.$$

Заметим, что при $m = 3$, $(L, \omega) = 1$, а

$$y_j = \lambda(x_j, x_{j+1}, ..., x_{j+L-1}) = \delta_{x(j)} \cdot \delta_{x(j+1)} \cdot ... \cdot \delta_{x(j+L-1)},$$

где $\{\delta_x: S \to S, x \in X\}$ совокупность биекций множества S, выборочная последовательность $y_1, y_{1+L}, ...$ представляет собой последовательность шифрующих преобразований поточной шифрсистемы [14. – С. 243].

Теорема 3. Пусть $\lambda \in \lambda(m, L)$, $m \geq 2$, $L \geq 2$, $L` = m+L–3$, $R = R(P(L))$ – степень различимости выборочной последовательности

$$P(L) = x_{1+L`}, x_{1+2L`}, ..., x_{1+iL`}, ...$$

периодической последовательности $P = P^1 = x_1, x_2, ...$ периода ω элементов алфавита X, $|X| \geq 2$, t – подпериод последовательности

$$Q = y_1, y_2, ..., y_j = \lambda(x_j, x_{j+1}, ..., x_{j+L-1})$$

кратности $k(0)$, $k(0) \geq |X|+1$, а W – ее период, причем $(L`, \omega) = 1$. Тогда

$$tk(0) \leq |X|t + L`(R–1),$$

в частности,

$$t \leq L`(R–1).$$

Доказательство. По условию найдется $j \in \{1, ..., W\}$, при котором $Q^j]_W$ имеет вид

$$Q^j]_W = \overline{\overline{y}, \overline{y}, ..., \overline{y}, \overline{\overline{y}}},$$

где $\overline{y} \in Y^t$, $\overline{y} = y_j, y_{j+1}, ..., y_{j+t-1}$, $\overline{\overline{y}} \in Y^{W-tk(0)}$. Так как $k(0) \geq |X|+1$, то найдутся $c(1), c(2)$, $0 \leq c(1) < c(2) \leq |X|$, для которых

$$x_{j+tc(1)} = x_{j+tc(2)}.$$

Предположим, что утверждение теоремы не выполняется, то есть

$$tk(0) \geq |X|t+L`(R-1)+1.$$

Тогда при M = R–1 имеем

$$j+tc(2)+ML` \leq j+t(k(0)-1)+t-1.$$

Так как $\lambda \in \lambda(m, L)$, то из этих фактов следует

$$x_{j+tc(1)+cL`} = x_{j+tc(2)+cL`}$$

при любом $c \in \{0, ..., M\}$. Заметим, что по условию $(L`, \omega) = 1$, в связи с чем (M+1)-граммы $P(L`)^{j+tc(1)}]_{M+1}$, $P(L`)^{j+tc(2)}]_{M+1}$ принадлежат последовательности P(L`). Используя теперь равенство M+1 = R, заключаем

$$P(L`)^{j+tc(1)}]_{M+1} = P(L`)^{j+tc(2)}]_{M+1},$$

и периоды этих последовательностей равны ω, откуда вытекает, что $\omega | t(c(2) - c(1))$, причем

$$t(c(2) - c(1)) \leq t|X| < tk(0) \leq W.$$

С другой стороны, как легко видеть, что $W|\omega$. Полученное противоречие завершает доказательство теоремы.

Замечание 2. Для линейной рекуррентной последовательности $P = x_1, x_2, ...$ максимального периода q^n-1 при $L` = m+L-3$, $(L`, q^n-1) = 1$ справедливо равенство $R(P(L`)) = n$. При фиксации t утверждение теоремы 3 дает верхнюю оценку величины tk(0), а вместе с ней и оценку k(0). Фиксируя же нижнюю оценку c(0) величины k(o), мы получаем верхнюю оценку подпериода t. Последняя ситуация представляет интерес при применении методов анализа поточных шифрсистем, основанных на перекрытиях последовательностей номеров шифрующих преобразований [13. – С. 243].

19.4. Обратимые автоматы

Напомним, что автомат A = (X, S, Y, h, f), |X| = |Y|, $h: X \times S \to S$, $f: S \times X \to Y$ является *обратимым*, если ограничения f_s: $\{s\} \times X \to Y$ отображения f биективны при любом $s \in S$.

Теорема 5. Пусть A = (X, S, Y, h, f), |X| = |Y| – обратимый автомат, ω – период его входной последовательности P, t – подпериод кратности k(0) периодической выходной последовательности A(s, P), отвечающей входу P и начальному состоянию s, причем $t < \frac{\omega}{|S|}$. Тогда либо t меньше степени различимости R(P) последовательности P, либо $k(0) \leq |S|$.

Доказательство. Пусть W – период последовательности A(s, P) = $Q^1 = y_1, y_2, ...$ Положим $s = s_1$, $P = P^1 = x_1, x_2, ...$, $A_M(s_1, P^1) = s_1, s_2, ...$ –

последовательность состояний автомата, отвечающая начальному состоянию s_1 и входной последовательности P.

По условию, найдется j, при котором

$$Q^j]_W = \bar{\bar{y}},\bar{\bar{y}},\ldots,\bar{\bar{y}},\bar{\bar{\bar{y}}},$$

где $\bar{\bar{y}} \in Y^t$, $\bar{\bar{y}} = y_j, y_{j+1}, \ldots, y_{j+t-1}$, $\bar{\bar{\bar{y}}} \in Y^{W-tk(0)}$.

Предположим, что $t \geq R(P)$, $k(0) > |S|$. В наборе состояний

$$(s_{j+kt}, k \in \{0, 1, \ldots, k(0)\})$$

в силу $k(0) > |S|$ найдутся одинаковые состояния. Пусть это будут состояния $s_{j+tr(1)}$, $s_{j+tr(2)}$, $r(2) > r(1)$, причем $r(2) - r(1) \leq |S|$. Тогда начальные отрезки длины t выходных последовательностей

$$A(s_{j+tr(1)}, P^{j+tr(1)}), A(s_{j+tr(2)}, P^{j+tr(2)})$$

совпадают. Из этих фактов и определения обратимого автомата следует равенство начальных отрезков длины t последовательностей

$$P^{j+tr(1)}, P^{j+tr(2)},$$

а так как, по предположению, $t \geq R(P)$, то

$$P^{j+tr(1)} = P^{j+tr(2)}.$$

Следовательно, $\omega | t(r(2) - r(1))$, откуда вытекает

$$\omega \leq t|S|,$$

что противоречит условию теоремы.

Глава 20. О ПЕРИОДИЧНОСТИ ПОСЛЕДОВАТЕЛЬНОСТИ СОСТОЯНИЙ АВТОМАТА, ОТВЕЧАЮЩЕЙ ЕГО НАЧАЛЬНОМУ СОСТОЯНИЮ И ВХОДНОЙ ПЕРИОДИЧЕСКОЙ ПОСЛЕДОВАТЕЛЬНОСТИ. ПРИБЛИЖЕННЫЕ ПЕРИОДЫ ПОСЛЕДОВАТЕЛЬНОСТИ СОСТОЯНИЙ АВТОМАТА

Для интуитивного понятия почти периодичности последовательности элементов конечного алфавита введена его формализация – мера приближенного периода этой последовательности. Получена нижняя оценка меры приближенного периода последовательности состояний автомата, отвечающей его начальному состоянию и входной периодической последовательности. На основании этой оценки для автоматов, моделирующих функционирование регистров сдвига, получены оценки снизу мер приближенных периодов их выходных последовательностей.

20.1. Введение, вспомогательные обозначения, понятия и результаты

Напомним, что основным результатом по оценке снизу периодов выходных последовательностей конечных автоматов, отвечающих их начальным состояниям и входным периодическим последовательностям является теорема 2.2. работы [33], состоящая в том, что минимальный период W выходной последовательности автомата не превосходит величины $k\omega$, где k – число состояний автомата, а ω – минимальный период входной последовательности. В [13] и [20] приведены утверждения, суть которых состоит в том, что W является делителем числа $k`\omega$ при некотором $k` \le k$.

Известно, что в связи с необходимой простотой реализации шифров и достижения высоких скоростей шифрования наибольшее распространение получили поточные многоалфавитные шифры. При реализации таких шифров выделяют два блока: управляющий блок и шифрующий блок. Управляющий блок вырабатывает последовательность номеров шифрующих преобразований – управляющую гамму. Шифрующий блок осуществляет алгоритм зашифрования. Качество шифрующего блока в значительной степени зависит от качества управляющей гаммы. Одно из важнейших требований к управляющему блоку состоит в том, что период управляющей гам-

мы должен превышать максимально возможную длину открытых сообщений, подлежащих шифрованию.

В связи с большой сложностью проблемы нижней оценки периодов выходных последовательностей конечных автоматов при заданных начальном состоянии и входной периодической последовательности естественным подходом к ее удовлетворительному решению является выделение тех или иных классов автоматов в качестве объектов исследований. Например, ряд работ посвящен вопросам периодичности выходных последовательностей линейных автономных автоматов, в частности, в этом классе выделяются работы, в которых указываются способы построения линейных рекуррентных последовательностей максимального периода в разнообразных алгебраических структурах. В настоящей работе используется другой подход к решению поставленной проблемы, заключающейся в предварительном решении промежуточной задачи – оценки снизу периода последовательности состояний автомата, отвечающей его начальному состоянию и входной периодической последовательности. Эта задача решается в работе в более общей постановке, а именно речь идет об оценке характеристик почти периодичности последовательностей состояний конечных автоматов.

Для периодической последовательности $\mathfrak{I}$ периода ω элементов конечного алфавита X вводится понятие меры $\mu(\mathfrak{I}, d)$ приближенного периода d. Качественно $\mu(\mathfrak{I}, d)$ трактуется как минимальная часть знаков последовательности $\mathfrak{I}$, которые необходимо изменить для получения из $\mathfrak{I}$ последовательности периода d.

Основным результатом является теорема 1, дающая нижние оценки мер приближенных периодов последовательности состояний автомата, отвечающей его начальному состоянию и входной периодической последовательности. Следствие 1 дает нижние оценки периодов этих последовательностей. В следствии 2 указываются нижние оценки мер приближенных периодов выходной последовательности регистра сдвига, отвечающей его начальному состоянию и входной периодической последовательности. Используются результаты, опубликованные в [8].

Положим:

- $A = (X, S, Y, h, f)$ – конечный автомат, $|X| \geq 2$, $|Y| \geq 2$;
- N – множество натуральных чисел, $N \cup o = N_o$;
- X* – множество всех слов в алфавите X;

– X_n^∞ – множество всех смешанно-периодических последовательностей в алфавите X. Последовательность $\mathfrak{I}$ из X_n^∞ называется чисто-периодической, если длина L ее предпериода равна нулю. Под периодом последовательности $\mathfrak{I}$ здесь и далее будет пониматься ее минимальный период.

– $X_{n,W}^\infty$ – множество всех последовательностей из X_n^∞ периода W;

– AM(s,$\mathfrak{I}$) = s1, s2, …, sj, … – последовательность состояний автомата A;

– для $\mathfrak{I}$ = x1, x2, …, xj, … и s∈S

$$s_j = h_{x_{j-1}} \ldots h_{x_1} s,\ y_j = f_{x_j} s_j,\ s_1 = s;$$

– ρ($\mathfrak{I}$, $\mathfrak{I}$`) – расстояние Хемминга между словами $\mathfrak{I}$, $\mathfrak{I}$` одинаковой длины из X*;

– ρk($\mathfrak{I}$, $\mathfrak{I}$`) – расстояние Хемминга между начальными словами длины k последовательностей $\mathfrak{I}$, $\mathfrak{I}$` из X_n^∞;

– (ω, ω`) – наибольший общий делитель чисел ω, ω`;

– [ω, ω`] – наименьшее общее кратное чисел ω, ω`;

– D| ω – D делит ω;

– ∃ – знак существует.

Для $\mathfrak{I}$ = $x_1, x_2, \ldots, x_j, \ldots$ из $X_п^\infty$ положим:

$$\mathfrak{I}^j = x_j, x_{j+1}, \ldots; \mathfrak{I}^1 = \mathfrak{I}; \mathfrak{I}^j]_k = x_j, x_{j+1}, \ldots, x_{j+k-1};$$

$$COD(\mathfrak{I}) = \{x \in X: \exists\, j \in N, x_j = x\}.$$

Последнюю величину мы называем *содержанием последовательности* $\mathfrak{I}$**.** Если понимать под последовательностью $\mathfrak{I}$ элементов алфавита X отображение $\mathfrak{I}$: N→X, то содержание $\mathfrak{I}$ равно образу множества N.

Пусть $\mathfrak{I}$, $\mathfrak{I}$` – произвольные последовательности из $X_n^\infty$ с длинами подходов L, L` и периодами ω, ω` соответственно. Легко доказывается следующее утверждение.

Утверждение 1. При k→∞ предел

$$\lim \frac{1}{k} \rho_k(\mathfrak{I}, \mathfrak{I}`)$$

существует и равен величине

$$\mu(\mathfrak{I}, \mathfrak{I}`) = \frac{1}{[\omega, \omega`]} \rho_{[\omega,\omega`]}(\mathfrak{I}^{\max(L,L`)+1}, \mathfrak{I}`^{\max(L,L`)+1}).$$

Данное утверждение является частным случаем следствия 1 работы [11].

Определение 1. Приближенным периодом последовательности $\mathfrak{I} \in I_n^\infty$ называется любое число W из N. Величина $\mu(\mathfrak{I}, W) = \inf\mu(\mathfrak{I}, \mathfrak{I}`)$, где нижняя грань берется по всем последовательностям $\mathfrak{I}` \in X_{n,W}^\infty$, называется мерой приближенного периода W (мерой приближения приближенного периода W) последовательности $\mathfrak{I}$.

Из утверждения 1 следует, что величина $\mu(\mathfrak{I},\mathfrak{I}`)$ определена периодическими частями $\mathfrak{I}^k$, $\mathfrak{I}`^k$ последовательностей $\mathfrak{I}$, $\mathfrak{I}`$ при $k \geq \max(L, L`)+1$. Мощность множества всех чисто периодических последовательностей периода W элементов алфавита X конечна. Поэтому $\inf\mu(\mathfrak{I}, \mathfrak{I}`) = \min\mu(\mathfrak{I}, \mathfrak{I}`)$.

Пусть N` – конечное подмножество N.

Определение 2. Наилучшей мерой приближения приближенных периодов из множества N` последовательности $\mathfrak{I}$ называется величина $\min\mu(\mathfrak{I}, W`)$, где минимум берется по всем $W` \in N`$.

Определение 3. Наилучшим приближенным периодом W среди периодов из N` последовательности $\mathfrak{I}$ называется минимальное число $W \in N`$, при котором

$$\mu(\mathfrak{I}, W) = \min\mu(\mathfrak{I}, W`), W` \in N`.$$

Определение 4. Наилучшей приближенной последовательностью НПП($\mathfrak{I}$, $\bigcup_{W` \in N`} X_{n,W`}^\infty$) из множества $\bigcup_{W` \in N`} X_{n,W`}^\infty$ к последовательности $\mathfrak{I}$ называется произвольная последовательность $\mathfrak{I}` \in \bigcup_{W` \in N`} X_{n,W`}^\infty$, для которой

$$\mu(\mathfrak{I}, \mathfrak{I}`) = \min_{W` \in N`} (\mathfrak{I}, W`).$$

Для формулировки приводимых ниже вспомогательных утверждений введем дополнительные обозначения.

Для чисто периодической последовательности $\mathfrak{I} = x_1, x_2, \ldots$ из $X_{n,\omega}^\infty$, D| ω и $j \in \overline{1,D}$ обозначим через $\nu_j(x)$ – частоту встречаемости символа x слове

$$x_j, x_{j+D}, \ldots, x_{j+TD}, T = (\frac{\omega}{D} - 1),$$

а через X(j) – множество всех $x \in X$, для которых $\nu_j(x) = \max_{i \in X} \nu_j(x)$. Отметим, что $|X(j)| \geq 1$.

Через $\Re(\mathfrak{I}, D)$ *обозначим множество всех последовательностей* $\mathfrak{I}`` = x``_1, x``_2, \ldots$ *вида:*

$$x``_j = x``_{j+D}, \ j \in N,$$

$$x``_k \in X(k),\ k \in \overline{1,D}.$$

Последние соотношения определяют $\mathfrak{I}``$ однозначно лишь в случае $|X(k)| = 1$, $k \in \overline{1,D}$. Очевидно, что $COD(\mathfrak{I}``) \subseteq COD(\mathfrak{I})$ для любой последовательности $\mathfrak{I}``$ из $\Re(\mathfrak{I}, D)$, а период каждой последовательности из $\Re(\mathfrak{I}, D)$ является делителем числа D.

Лемма 1. Для $\mathfrak{I} \in X^{\infty}_{n,\omega}$, $\mathfrak{I}` \in X^{\infty}_{n,\omega`}$, $D = (\omega, \omega`)$ величина $\mu(\mathfrak{I}, \mathfrak{I}``)$ не зависит от выбора $\mathfrak{I}``$ из $\Re(\mathfrak{I}, D)$ и

1) $\mu(\mathfrak{I},\mathfrak{I}``) \le \mu(\mathfrak{I},\mathfrak{I}`)$,

2) $\mu(\mathfrak{I},\mathfrak{I}``) \le \mu(\mathfrak{I},\omega`)$.

Доказательство. Из утверждения 1 следует, что для доказательства леммы 1 достаточно доказать ее для чисто-периодических последовательностей $\mathfrak{I}$, $\mathfrak{I}`$. Пусть $\mathfrak{I}$, $\mathfrak{I}`$ – чисто-периодические последовательности.

При $(\omega,\omega`) = \omega$ утверждение леммы очевидно, так как множество $\Re(\mathfrak{I}, D)$ состоит из последовательности $\mathfrak{I}`` = \mathfrak{I}$.

Пусть $(\omega, \omega`) = D \ne \omega$, $\mathfrak{I} = x_1, x_2, \ldots$, $\mathfrak{I}` = x`_1, x`_2, \ldots$ По утверждению 1 имеем

$$\mu(\mathfrak{I}, \mathfrak{I}`) = \frac{1}{[\omega,\omega`]}\rho_{[\omega,\omega`]}(\mathfrak{I},\mathfrak{I}`) = \frac{1}{[\omega,\omega`]}\sum_{j=1}^{[\omega,\omega`]}\rho(x_j, x`_j) =$$

$$= \frac{1}{[\omega,\omega`]}\sum_{j=1}^{\omega`}\ \sum_{k=0}^{\frac{[\omega,\omega`]}{\omega`}-1}\rho(x`_j, x_{j+k\omega`}).$$

Заметим, что $\frac{[\omega,\omega`]}{\omega`} - 1 = \frac{\omega}{D} - 1$, а слова $x_j, x_{j+\omega`}, \ldots, x_{j+C\omega`}, x_j, x_{j+D}, \ldots, x_{j+CD}$, где $C = \frac{\omega}{D} - 1$, получаются друг из друга перестановкой символов, в связи с чем справедливо равенство

$$\sum_{k=0}^{\frac{\omega}{D}-1}\rho(x`_j, x_{j+k\omega`}) = \sum_{k=0}^{\frac{\omega}{D}-1}\rho(x`_j, x_{j+kD}).$$

Поэтому

$$\mu(\mathfrak{I}, \mathfrak{I}`) = \frac{1}{[\omega,\omega`]}\sum_{j=1}^{\omega`}\ \sum_{k=0}^{\frac{\omega}{D}-1}\rho(x`_j, x_{j+kD}) = \frac{1}{[\omega,\omega`]}\sum_{j=1}^{D}\ \sum_{m=0}^{\frac{\omega`}{D}-1}\ \sum_{k=0}^{\frac{\omega}{D}-1}\rho(x`_{j+mD}, x_{j+kD}).$$

Для произвольной последовательности $\mathfrak{I}`` = x_1``, x_2``, \ldots$ из $\Re(\mathfrak{I}, D)$ имеем

$$\mu(\mathfrak{I}, \mathfrak{I}``) = \frac{\rho_{\omega}(\mathfrak{I}, \mathfrak{I}``)}{\omega} =$$

$$= \frac{\rho_{[\omega,\omega`]}(\mathfrak{I}, \mathfrak{I}``)}{[\omega,\omega`]} = \frac{1}{[\omega,\omega`]} \sum_{j=1}^{\omega`} \sum_{k=0}^{\frac{\omega}{D}-1} \rho(x_{j}``, x_{j+kD}) =$$

$$= \frac{1}{[\omega,\omega`]} \sum_{j=1}^{D} \sum_{m=0}^{\frac{\omega`}{D}-1} \sum_{k=0}^{\frac{\omega}{D}-1} \rho(x_{j+mD}``, x_{j+kD}).$$

Из этого равенства, во-первых, вытекает независимость значения $\mu(\mathfrak{I}, \mathfrak{I}``)$ от выбора $\mathfrak{I}``$ из $\Re(\mathfrak{I}, D)$ и, во-вторых, то, что при любых $j \in \overline{1,D}$, $m \in 0, \overline{\frac{\omega`}{D}-1}$ справедливо неравенство

$$\sum_{k=0}^{\frac{\omega}{D}-1} \rho(x_{j+md}``, x_{j+kD}) \le \sum_{k=0}^{\frac{\omega}{D}-1} \rho(x`_{j+md}, x_{j+kD}).$$

Следовательно, $\mu(\mathfrak{I}, \mathfrak{I}``) \le \mu(\mathfrak{I}, \mathfrak{I}`)$. Откуда получаем неравенство $\mu(\mathfrak{I}, \mathfrak{I}``) \le \mu(\mathfrak{I}, \omega`)$. Лемма 1 доказана.

Утверждение 2. Пусть $\mathfrak{I} \in X^{\infty}_{n,\omega}$, $\omega` \in N$. Наилучшая мера приближения $\min\limits_{d`: d` | \omega`} \mu(\mathfrak{I}, d`)$ приближенных периодов из множества $\{d`: d`|\omega`\}$ последовательности $\mathfrak{I}$ равна величине $\mu(\mathfrak{I}, \mathfrak{I}``)$, где $\mathfrak{I}`` \in \Re(\mathfrak{I}, D)$ при $D = (\omega, \omega`)$.

Доказательство. Пусть $\min\limits_{d`: d` | \omega`} \mu(\mathfrak{I}, d`) = \mu(\mathfrak{I}, d`_{o})$, а $\mathfrak{I}` = НПП(\mathfrak{I}, X^{\infty}_{n,d`_{o}})$ – наилучшая приближенная последовательность из множества $X^{\infty}_{n,d`_{o}}$ к последовательности $\mathfrak{I}$. Тогда $\mu(\mathfrak{I}, \mathfrak{I}`) = \mu(\mathfrak{I}, d`_{o})$.

По лемме 1 заключаем, что найдется $\mathfrak{I}`` \in \Re(\mathfrak{I}, D_{o})$, периода $d``$, $d``|D_{o}$, $D_{o} = (d`_{o}, \omega)$, для которой $\mu(\mathfrak{I}, \mathfrak{I}``) \le \mu(\mathfrak{I}, \mathfrak{I}`)$. Так как $D_{o}|\omega`$, то $d``|\omega`$. Из определения $\mu(\mathfrak{I}, d`_{o})$ и предыдущего неравенства получаем

$$\mu(\mathfrak{I}, \mathfrak{I}``) = \mu(\mathfrak{I}, d`_{o}) = \mu(\mathfrak{I}, \mathfrak{I}`).$$

Очевидно, что $\mu(\mathfrak{I}, d`_{o})$ является наилучшей мерой приближения приближенных периодов и из множества $\{d`: d`|D\}$ последовательности $\mathfrak{I}$.

Откуда вытекает, что $\mathfrak{I}`` \in \Re(\mathfrak{I}, D)$.

20.2. Нижние оценки мер приближенных периодов последовательностей состояний автомата, отвечающих его начальным состояниям и входным смешанно-периодическим последовательностям

Пусть $\Im = x_1, x_2, \ldots$ – входная смешанно-периодическая последовательность автомата $A = (X, S, Y, h, f)$, а α – бинарное отношение эквивалентности на СОД($\Im$) удовлетворяющее условию: произвольные элементы $x, x`$ из разных классов эквивалентности таковы, что частичные функции переходов $h_x, h_{x`}$ автомата A не имеют общих переходов, то есть $h_x s \neq h_{x`} s$ при любом $s \in S$. Класс эквивалентности отношения α, содержащий элемент x, обозначим через $\alpha(x)$.

Теорема 1. Пусть $\Im = x_1, x_2, \ldots$ – входная смешанно-периодическая последовательность автомата A, $\alpha(\Im) = \alpha(x_1), \alpha(x_2), \ldots$ – соответствующая ей последовательность периода $\omega(\alpha)$ классов эквивалентности отношения α на СОД($\Im$); $A_M(s, \Im)$ – последовательность состояний автомата A, отвечающая его начальному состоянию $s \in S$ и входной последовательности $\Im$; $\tau`$ – приближенный период последовательности $A_M(s, \Im)$ с мерой приближения $\mu(A_M(s, \Im), \tau`)$, причем $(\tau`, \omega(\alpha)) = t \neq \omega(\alpha)$. Тогда

$$\mu(A_M(s, \Im), \tau`) \geq \frac{1}{2} \min_{d:d|t} \mu(\alpha(\Im), d).$$

Доказательство. Пусть $НПП(A_M(s, \Im), X^{\infty}_{n,\tau`}) = s`_1, s`_2, \ldots$ – наилучшая приближенная последовательность периода $\tau`$ из множества $X^{\infty}_{n,\tau`}$ к последовательности $A_M(s, \Im) = s_1, s_2, \ldots$ периода τ, $s = s_1$. Определим вспомогательные последовательности

$$(A_M(s, \Im))_2 = s_1s_2, s_2s_3, \ldots, s_js_{j+1}, \ldots,$$

$$(НПП\,(A_M(s, \Im), X^{\infty}_{n,\tau`}))_2 = s`_1s`_2, s`_2s`_3, \ldots, s`_js`_{j+1}, \ldots$$

Очевидно, периоды этих последовательностей равны $\tau, \tau`$ соответственно. Непосредственно проверяется, что

$$\mu((A_M(s, \Im))_2, \tau`) \leq \mu((A_M(s, \Im))_2, (НПП(A_M(s, \Im), X^{\infty}_{n,\tau`}))_2) \leq$$

$$\leq 2\mu(A_M(s, \Im), НПП(A_M(s, \Im), X^{\infty}_{n,\tau`})) = 2\mu(A_M(s, \Im), \tau`).$$

По утверждению 2 найдется последовательность $Q``$ периода $d_o``$ из $\Re(A_M(s, \Im)_2, D)$, $D = (\tau, \tau`)$, для которой $d_o``|D$ и выполняются соотношения

$$\mu((A_M(s, \Im)_2, d_o``) = \mu((A_M(s, \Im)_2, Q``) \leq \mu((A_M(s, \Im)_2, \tau`),$$

Отметим, что СОД(Q``)$\subseteq$СОД(($A_M(s, \Im)_2$)).

На множестве СОД(($A_M(s, \Im)_2$)) определим функцию F. Для ss` из СОД($A_M(s, \Im)_2$) положим F(ss`) = $\alpha(x)$, если $\delta_x s = s`$. Рассмотрим последовательности

$$F((\ A_M(s, \Im)_2)) = F(s_1s_2), F(s_2s_3), \ldots, F(s_js_{j+1}), \ldots,$$

$$F(Q``) = \alpha(x_1``), \alpha(x_2``), ...$$

Очевидно, что $F((A_M(s, \Im)_2)) = \alpha(\Im)$. Напомним, что период последовательности $\alpha(\Im)$ равен $\omega(\alpha)$. Обозначим через $\omega``(\alpha)$ период последовательности F(Q``). Ясно, что $\omega``(\alpha)|d_o``$. Так как $(\omega(\alpha), \tau`) = t \neq \omega(\alpha)$, то $(\omega(\alpha), \omega``(\alpha)) = d$, где d|t.

Очевидно, что

$$\mu(\alpha(\Im), F(Q``) \leq \mu((\ A_M(s, \Im))_2), Q``).$$

Используя утверждение 2, получаем

$$\min_{d:d|t} \mu(\alpha(\Im), d) \leq \mu(\alpha(\Im), F(Q``).$$

Следовательно,

$$\min_{d:d|t} \mu(\alpha(\Im), d) \leq \mu((A_M(s, \Im))_2), \tau`) \leq 2\mu(A_M(s, \Im), \tau`),$$

что и требовалось доказать.

Эффективность теоремы 1 (рамки ее применения) определены условием $\omega(\alpha) > 1$. Таким образом, для нахождения нижней оценки меры приближенного периода последовательности $A_M(s, \Im)$ состояний автомата A с помощью теоремы 1 необходимо предварительно построить какое либо бинарное отношение типа α. В ряде случаев удобно сначала пытаться строить бинарное отношение эквивалентности σ^* на СОД($\Im$) следующим образом. Определяем бинарное отношение σ на СОД($\Im$): x находится в отношении σ с x` тогда и только тогда, если найдется $s \in S$, при котором $h_x s = h_{x`} s$. В качестве σ^* берем транзитивное замыкание отношения σ. Для повышения эффективности теоремы 1 удобно предварительно определить компоненту связности A_s автомата A, содержащую начальное состояние s, а затем проверять выполнение условий теоремы для автомата A_s.

Следствие 1. Пусть $\Im = x_1, x_2, \ldots$ – входная смешанно-периодическая последовательность автомата A, $\alpha(\Im) = \alpha(x_1), \alpha(x_2), \ldots$ – соответствующая ей последовательность периода $\omega(\alpha)$ классов эквивалентности отношения α на СОД($\Im$). Тогда период τ последовательности $A_M(s, \Im)$ состояний автомата A, отвечающей его начальному состоянию $s \in S$ и входной последовательности $\Im$, кратен $\omega(\alpha)$.

Доказательство. Предположим, что $(\tau, \omega(\alpha)) = t \neq \omega(\alpha)$. В качестве приближенного периода $\tau`$ последовательности $A_M(s, \Im)$ рассмотрим период τ последовательности $A_M(s, \Im)$. Тогда по теореме 1

$$\mu(A_M(s, \Im), \tau) \geq \frac{1}{2} \min_{d:d|t} \mu(\alpha(\Im), d) .$$

Так как $t \neq \omega(\alpha)$, то очевидно, что правая часть неравенства больше нуля. Поэтому $\mu(A_M(s, \Im), \tau) > 0$, что противоречит тому, что τ – период последовательности $A_M(s, \Im)$. Таким образом, τ кратен величине $\omega(\alpha)$.

Утверждение следствия 1 позволяет строить автоматы и с гарантированными периодами последовательностей состояний, отвечающих их начальным состояниям и входным смешанно-периодическим последовательностям. Так, в частности, выбор частичных функций переходов автомата так, чтобы они попарно не имели общих переходов, гарантирует кратность периода последовательности его состояний величине периода входной последовательности при любом его начальном состоянии. Этот факт ранее был доказан В. А. Башевым.

Следующие две леммы, представляющие и самостоятельный интерес, являются вспомогательным инструментом для доказательства иной (чем в теореме 1) нижней оценки меры приближенного периода последовательности состояний автомата, отвечающей его начальному состоянию и входной смешанно-периодической последовательности.

Лемма 2. Пусть $\Im \in X^{\infty}_{n,\omega}$, $\Im` \in X^{\infty}_{n,\omega`}$, $(\omega, \omega`) = d$; L, L` – предпериоды последовательностей $\Im$, $\Im`$, соответственно; $M = \max (L, L`)$. Тогда

$$\mu(\Im, \Im`) = \mu(\Im^{M+j}, \Im`^{M+j}) = \mu(\Im^{M+j+cd}, \Im`^{M+j}),$$

где $j \in N$, $c \in N_o$.

Доказательство. Так как $(\omega, \omega`) = d$, то найдутся натуральные числа $k_1$, $k_2$, при которых $k_2\omega` - k_1\omega = d$. По утверждению 1 имеем

$$\mu(\Im, \Im`) = \frac{1}{[\omega, \omega`]} \rho_{[\omega,\omega`]}(\Im^{M+1}, \Im`^{M+1}).$$

Очевидно, что при любом $j \in N$ и $c \in N_o$ справедливы равенства

$$\frac{1}{[\omega, \omega`]} \rho_{[\omega,\omega`]}(\Im^{M+1}, \Im`^{M+1}) = \frac{1}{[\omega, \omega`]} \rho_{[\omega,\omega`]}(\Im^{M+j}, \Im`^{M+j}) =$$

$$= \frac{1}{[\omega, \omega`]} \rho_{[\omega,\omega`]}(\Im^{M+j+ck_2\omega`}, \Im`^{M+j}) = \frac{1}{[\omega, \omega`]} \rho_{[\omega,\omega`]}(\Im^{M+j+ck_1\omega+cd}, \Im`^{M+j}) =$$

$$= \frac{1}{[\omega, \omega`]} \rho_{[\omega,\omega`]}(\Im^{M+j+cd}, \Im`^{M+j}).$$

Несложно доказывается следующая лемма 3.

Лемма 3. Для любых $\Im, \Im`, \Im`` \in X_n^\infty$ справедливо неравенство

$$\mu(\Im,\Im`)+\mu(\Im`, \Im``) \geq \mu(\Im, \Im``).$$

На множестве всех чисто-периодических последовательностей функция μ является метрикой.

Теорема 2. Пусть Пусть $\Im = x_1, x_2, \ldots$ – входная смешанно-периодическая последовательность автомата A, $\alpha(\Im) = \alpha(x_1), \alpha(x_2), \ldots$ – соответствующая ей последовательность периода $\omega(\alpha)$ классов эквивалентности бинарного отношения α на СОД($\Im$); $A_M(s, \Im)$ – последовательность периода τ состояний автомата A, отвечающая его начальному состоянию $s \in S$ и входной последовательности $\Im$; $\tau`$ – приближенный период последовательности $A_M(s, \Im)$ с мерой приближения $\mu(A_M(s, \Im), \tau`)$, причем $(\tau`, \tau)) = d \neq \omega(\alpha)$. Тогда при любом $j \in N$

$$\frac{1}{4}\mu(\alpha(\Im)^j, \alpha(\Im)^{j+cd}) \leq \mu(A_M(s, \Im), \tau`).$$

Доказательство. Пусть $НПП(A_M(s, \Im), X_{n,\tau`}^\infty) = s_1`, s_2`, \ldots$ – наилучшая приближенная последовательность из множества последовательностей периода $\tau`$ к последовательности $A_M(s, \Im) = s_1, s_2, \ldots$ Обозначим через V – максимальную длину из длин подходов последовательностей $НПП(A_M(s, \Im), X_{n,\tau`}^\infty)$ и $A_M(s, \Im)$. Тогда последовательности $(НПП(A_M(s, \Im), X_{n,\tau`}^\infty))^{V+1}$, $(A_M(s, \Im))^{V+1}$ – чисто периодические и первая последовательность является наилучшей приближенной последовательностью из множества последовательностей периода $\tau`$ ко второй последовательности. Пользуясь леммой 2 для $j \in N$, $c \in N_o$, получаем

$$\mu(A_M(s,\Im), \tau`) = \mu((A_M(s, \Im))^{V+1}, \tau`) = \mu((A_M(s,\Im))^{V+1},$$
$$(НПП(A_M(s, \Im), X_{n,\tau`}^\infty))^{V+1}) =$$
$$= \mu((A_M(s, \Im))^{V+j+cd}, (НПП(A_M(s, \Im), X_{n,\tau`}^\infty))^{V+j}).$$

Для c и c` из N_o по лемме 3 имеем

$$\mu((A_M(s, \Im))^{V+j+cd}, (A_M(s, \Im))^{V+j+c`d})) \leq 2\mu(A_M(s, \Im)), \tau`).$$

Для последовательностей

$$(A_M(s, \Im))^{V+j+cd} = s_{V+j+cd}, s_{V+j+cd+1}, \ldots, (A_M(s,\Im))^{V+j+c`d}) = s_{V+j+c`d},$$
$$s_{V+j+c`d+1}, \ldots$$

построим вспомогательные последовательности:

$$((A_M(s, \Im))^{V+j+cd})_2 = s_{V+j+cd}s_{V+j+cd+1}, s_{V+j+cd+1}s_{V+j+cd+2}, \ldots;$$

$$((A_M(s, \Im))^{V+j+c`d})_2 = s_{V+j+c`d}s_{V+j+c`d+1}, s_{V+j+c`d+1}s_{V+j+c`d+2}, \ldots$$

и функцию F на СОД$(((A_M(s, \Im))^{V+j+cd})_2)$, положив

$$F(s_k, s_{k+1}) = \alpha(x),$$

если $f_x s_k = s_{k+1}$. Из законов функционирования автомата A следует, что последовательности

$$F((A_M(s, \Im))^{V+j+cd})_2 = F(s_{V+j+cd}s_{V+j+cd+1}), F(s_{V+j+cd+1}s_{V+j+cd+2}), \ldots$$

$$F((A_M(s, \Im))^{V+j+c`d})_2 = F(s_{V+j+c`d}s_{V+j+c`d+1}), F(s_{V+j+c`d+1}s_{V+j+c`d+2}), \ldots$$

равны, соответственно, последовательностям

$$\alpha(\Im)^{V+j+cd} = \alpha(x_{1+j+cd}), \alpha(x_{2+j+cd}), \ldots$$

$$\alpha(\Im)^{V+j+c`d} = \alpha(x_{1+j+c`d}), \alpha(x_{2+j+c`d}), \ldots$$

Очевидно, что

$$\mu(F((A_M(s, \Im))^{V+j+cd})_2, F((A_M(s, \Im))^{V+j+c`d})_2) \le$$
$$\le \mu(((A_M(s, \Im))^{V+j+cd})_2, ((A_M(s, \Im))^{V+j+c`d})_2) \le$$
$$\le 2\mu((A_M(s, \Im))^{V+j+cd}, (A_M(s, \Im))^{V+j+c`d}).$$

Из полученных оценок вытекает, что

$$\mu(\alpha(\Im)^{V+j+cd}, \alpha(\Im)^{V+j+c`d}) \le 2\mu((A_M(s, \Im))^{V+j+cd}, (A_M(s, \Im))^{V+j+c`d}) \le$$
$$\le 4\mu(A_M(s, \Im)), \tau`).$$

Доказательство закончено.

Теорему 2 можно использовать и для оценки периода τ последовательности $A_M(s, \Im)$ состояний автомата A. Анализ доказательств теорем 1, 2 показывает, что данные в них оценки меры $\mu(A_M(s, \Im), \tau`)$ приближенного периода $\tau`$ последовательности $A_M(s, \Im)$ несравнимы. На практике для получения оптимальной оценки следует использовать утверждения обеих теорем.

20.3. Нижние оценки мер приближенных периодов выходных последовательностей регистров сдвига, отвечающих его начальным состояниям и входным смешанно-периодическим последовательностям

Рассмотрим регистр сдвига, то есть автомат $A = R(\varphi, X) = (X, S, Y, (h_x)_{x\in X}, (f_x)_{x\in X})$ вида:

$$S = X^n, Y = X; \text{ для } x \in X \text{ и } x(n), x(n-1), \ldots, x(1) \in X^n$$

$$h_x(x(n), x(n-1), \ldots, x(1)) = (\varphi(x, x(n), x(n-1), \ldots, x(1)), x(n),$$
$$x(n-1), \ldots, x(2)),$$

где φ – функция: $X^{n+1} \to X$; $f_x = \lambda$, $x \in X$,

$$\lambda(x(n), x(n-1), \ldots, x(1)) = x(k)$$

для некоторого $k \in \{1, \ldots, n\}$.

Пусть $\mathfrak{I}$ – входная смешанно-периодическая последовательность автомата A = R(φ, X). Период выходной последовательности A(s, $\mathfrak{I}$) автомата R(φ, X) совпадает с периодом его последовательности состояний A_M(s, $\mathfrak{I}$), в связи с чем, следствие 1, теорема 2 дают нижние оценки периода выходной последовательности A(s, $\mathfrak{I}$) автомата R(φ, X).

Рассмотрим вопрос о связях мер приближенных периодов последовательностей A_M(s, $\mathfrak{I}$) и A(s, $\mathfrak{I}$).

Утверждение 3. Для любого $\tau` \in N$ справедливо неравенство

$$n\mu(A(s, \mathfrak{I}), \tau`) \geq \mu(A_M(s, \mathfrak{I}), \tau`) .$$

Доказательство. Без ограничения общности доказательства будем предполагать, что входная последовательность $\mathfrak{I}$ и выходная последовательность регистра сдвига A(s, $\mathfrak{I}$) = x(k), x(k+1), …, x(k+j), … чисто периодические последовательности (см. утверждение 1). Последовательность A_M(s, $\mathfrak{I}$) можно записать в виде:

$A_M(s,\mathfrak{I})=(x(n), x(n–1), ..., x(1)), (x(n+1), x(n), ..., x(2)), …, (x(n+j), ..., x(j+1)), …$ Несовпадение состояний – слов $(x(n+j), ..., x(j+1))$, $(x`(n+j), ..., x`(j+1))$ обуславливается несовпадением их компонент. Для последовательности A(s, $\mathfrak{I}$) = x(k), x(k+1), …, x(k+j), … и чисто периодической последовательности $\mathfrak{I}` = x`(k), x`(k+1), …, x`(k+j), …$ периода $\tau`$ неравенство $x(k+j) \neq x`(k+j)$ для $j \geq k–1$ влечет n неравенств:

$(x(k+j), x(k+j–1), …, x(k+j–n+1)) \neq (x`(k+j), x`(k+j–1), …, x`(k+j–n+1));$

$(x(k+j+1), x(k+j), …, x(k+j–n+2)) \neq (x`(k+j+1), x`(k+j), …, x`(k+j–n+2));$

……..

$(x(k+j+n–1), x(k+j+n–2), …, x(k+j) \neq (x`(k+j+n–1);$
$x`(k+j+n–2), …, x`(k+j)).$

Поэтому для последовательностей A(s, $\mathfrak{I}$) периода τ и $\mathfrak{I}`$ периода $\tau`$ справедливы соотношения

$$n\mu(A(s, \mathfrak{I}), \mathfrak{I}`) = \frac{n}{[\tau,\tau`]}\rho_{[\tau,\tau`]}(A(s, \mathfrak{I}), \mathfrak{I}`) \geq \frac{1}{[\tau,\tau`]}\rho_{[\tau,\tau`]}(A_M(s, \mathfrak{I}),R(\mathfrak{I})) =$$
$$= \mu(A_M(s, \mathfrak{I}), R(\mathfrak{I})),$$

где

$$R(\mathfrak{I}`) = (x`(k), x`(k+1), …, x`(k+n–1)), (x`(k+1), x`(k+2), …, x`(k+n)),…$$

Имеем

$$\mu(A_M(s, \mathfrak{I}), R(\mathfrak{I})) \geq \mu(A_M(s, \mathfrak{I}), \tau`)) .$$

Следовательно, взяв в качестве $\mathfrak{I}`$ наилучшую приближенную последовательность периода $\tau`$ к $A(s, \mathfrak{I})$ получаем требуемое неравенство

$$n\mu\,(A(s, \mathfrak{I}), \tau`) = n\mu(A(s, \mathfrak{I}),\mathfrak{I}`) \geq \mu(A_M(s, \mathfrak{I}),R(\mathfrak{I})) \geq \mu(A_M(s, \mathfrak{I}), \tau`).$$

Из теорем 1, 2 и утверждения 3 вытекает следствие 2.

Следствие 2. Пусть $\mathfrak{I}$ – входная последовательность регистра сдвига $R(\varphi, X)$, $\alpha(\mathfrak{I})$ – соответствующая ей последовательность периода $\alpha(\omega)$ классов эквивалентности бинарного отношения α на СОД($\mathfrak{I}$); $W`$ – приближенный период выходной последовательности $A(s, \mathfrak{I})$ периода W регистра сдвига $R(\varphi, X)$.

1. Если $(W, W`) = d \neq \alpha(\omega)$, то при любых $j \in N$ и $c \in N_o$

$$\frac{1}{4}\mu(\alpha(\mathfrak{I})^j, \alpha(\mathfrak{I})^{j+cd}) \leq \mu(A(s, \mathfrak{I}), W`).$$

2. Если $(\alpha(\omega), W`) = t \neq \alpha(\omega)$ и $d$ – наилучший приближенный период последовательности $\alpha(\mathfrak{I})$ среди приближенных периодов из множества $\{d`: d|`t\}$, то

$$\frac{1}{2n}\mu(\alpha(\mathfrak{I}), d) \leq \mu(A(s, \mathfrak{I}), W`).$$

Глава 21. ПРИБЛИЖЕННЫЕ ПЕРИОДЫ ВЫХОДНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ ПОЛНОЦИКЛОВОГО АВТОМАТА, ПРЕДСТАВИМОГО ПОСЛЕДОВАТЕЛЬНЫМ СОЕДИНЕНИЕМ АВТОНОМНОГО АВТОМАТА С НЕАВТОНОМНЫМ ПЕРЕСТАНОВОЧНЫМ АВТОМАТОМ

Ниже будут получены нижние оценки мер приближенных периодов выходных последовательностей полноциклового автомата, представимого последовательным соединением автономного автомата с неавтономным перестановочным автоматом.

В разделе 20 было введено понятие приближенного периода заданной периодической последовательности и его меры приближения. Приведены оценки снизу мер приближенных периодов для последовательности состояний автомата при заданных начальном состоянии и входной периодической последовательности.

В данной главе объектом изучения являются выходные последовательности полноциклового автомата, представимого последовательным соединением автономного автомата с неавтономным перестановочным автоматом.

Используем обозначения:

– $d \mid D$ – d делит D;
– (a, b) общий наибольший делитель a и b;
– [a, b] – наименьшее общее кратное чисел a и b.

Пусть X – некоторый алфавит, $|X| \geq 2$, $P = x_1, x_2, \ldots$, $P` = x`_1, x`_2, \ldots$ – периодические последовательности элементов алфавита X периодов ω, ω`, соответственно, $\rho_N(P, P`) = \rho(x_1, x_2, \ldots, x_N, x`_1, x`_2, \ldots, x`_N)$ – расстояние в метрике Хэмминга между словами $x_1, x_2, \ldots, x_N$ и $x`_1, x`_2, \ldots, x`_N$ длины N .

Таким образом, $\rho_N(P, P`)$ совпадает с числом таких $j \in \{1, \ldots, N\}$, для которых $x_j \neq x`_j$. Пусть M_ω – множество всех периодических последовательностей элементов из X периода ω.

Определение 1. Будем говорить, что периодическая последовательность P периода ω имеет приближенный период ω` с мерой приближения $\rho_{\omega`}(P)$, если

$$\min \rho_{[\omega,\omega`]}(P, P`) = \rho_{\omega`}(P),$$

где минимум берется по всем P` из M_ω.

21.1. Полноцикловое последовательное соединение автоматов

Пусть $B=(T, Y_B, \delta, \lambda)$ – автономный автомат с множеством состояний T, выходным алфавитом Y_B, функцией переходов δ: $T\to T$ и функцией выхода λ: $T\to Y_B$, $A = (X, S, (h_x)_{x\in X})$ – автомат без выхода с входным алфавитом $X = Y_B$, множеством состояний S, частичными функциями переходов $(h_x)_{x\in X}$, h_x: $S\to S$ для $x\in X$. Рассмотрим автомат $C=(T\times S, Y, \delta_C, \Phi)$, являющийся последовательным соединением $B\to A$ с выходной функцией Φ автономного автомата $B = (T, Y_B, \delta, \lambda)$ с неавтономным автоматом $A = (X, S, (h_x)_{x\in X})$. Он имеет множество состояний $S_C=T\times S$, выходной алфавит Y, функцию перехода $\delta_C(t, s) = (\delta t, h_{\lambda(t)}s)$ и функцию выхода Φ: $T\times S \to Y$.

Через C(t, s) обозначим выходную последовательность автомата A , отвечающую его начальному состоянию $(t, s)\in T\times S$. Пусть $\{d_j\}$ – множество всех таких делителей числа $|S_1|\cdot|S_2|$, которые не являются одновременно делителем числа $|S_1|$, то есть

$$\{d_j\} = \{d_j: d_j \mid |T|\cdot|S|, d_j \text{ не делит } |T|\}.$$

Предположим, что множество $\{d_j\}$ не пустое, то есть $|S| > 1$ и d_0 – минимальный делитель из $\{d_j\}$. Напомним, что автомат называют полноцикловым, если он автономный и его граф переходов состоит из единственного цикла, содержащего все состояния. Автомат называют перестановочным, если его все частичные функции переходов биективны.

Теорема 1. Пусть для автоматов B, A выполнены условия:

1) автомат $C = B\to A$ полноцикловый;

2) существуют $t_0\in T$, и $s_0, s`_0\in S$ и R, $N \in\{1, 2, ..., d_0\}$, для которых

$$\rho_N(C(t_0, s_0), C(t_0, s`_0)) \ge R.$$

Пусть (t, s) – произвольное состояние автомата C и $\tau`$ – приближенный период с мерой $\rho_{\tau`}(C(t, s)) < \frac{R}{2}$ выходной периодической последовательности C(t, s) периода τ автомата C. Тогда $\tau`$ – кратен хотя бы одному из делителей множества $\{d_j\}$.

Доказательство. Сформулируем сначала вспомогательное очевидное утверждение.

Лемма 1. Автомат $C = B\to A$ полноцикловый тогда и только тогда, когда:

A_1 – полноцикловый автомат;

A_2 – перестановочный автомат и подстановка

$$\Pi_1 = h_{x(|T|)}h_{x(|T|-1)}\ldots h_{x(2)}h_{x(1)},$$

построенная с помощью $t \in T$ и выходной последовательности $B(t) = x(1), x(2), \ldots$, автомата B, полноцикловая.

Предположим, что каждое d_j из множества $\{d_j\}$ не делит $\tau`$. Тогда $(\tau`, |T|\cdot|S|) = d$, где $d \mid |T|$.

По определению приближенного периода $\tau`$ последовательности $C(t, s)$ найдется периодическая последовательность $Q = y_1, y_2, \ldots$ элементов алфавита Y периода $\tau`$, для которой

$$\rho_{[\tau,\tau`]}(C(t, s), Q) = \rho_{\tau`}(C(t, s)).$$

Пусть $t = t_1$, $s = s_1$ и

$C_M(t_1, s_1) = (t_1, s_1), (t_2 s_2), \ldots, (t_j, s_j), \ldots$– последовательность состояний автомата A, отвечающая его начальному состоянию (t, s), а

$$Q = Q^1, Q^j = y_j, y_{j+1}, \ldots$$

Несложно показывается, что справедливы равенства

$$\rho_{[\tau,\tau`]}(C(t_1, s_1), Q^1) = \rho_{[\tau,\tau`]}(C(t_j, s_j), Q^j) = \rho_{[\tau,\tau`]}(C(t_{j+cd`}, s_{j+cd`}), Q^j),$$

где $c \in \{0, 1, 2, \ldots\}$, $d' = (\tau, \tau`)$.

Так как $\tau \mid |S_1|\cdot|S_2|$, то $d' \mid d$. В частности по предположению, заключаем $d' \mid |S_1|$. Поэтому из последнего равенства получаем

$$\rho_{\tau`}(C(t, s)) = \rho_{[\tau,\tau`]}(C(t_{j+\nu\cdot|T|}, s_{j+\nu\cdot|S|}), Q^j) = \rho_{[\tau,\tau`]}(C(t_j, \textstyle\prod_j^{\nu} s_j), Q^j),$$

$$\nu \in 0, 1, 2, \ldots\}.$$

Здесь учтена полноцикловость автомата B и положено

$$\Pi_j = h_{x(j-1)}h_{x(j)}\ldots h_{x(1)}h_{x(|T|)}h_{x(|T|-1)}\ldots h_{x(j+1)}h_{x(j)}.$$

Очевидно подстановка Π_j – подобна полноцикловой подстановке Π_1, следовательно, она полноцикловая. Поэтому последние равенства принимают вид

$$\rho_{\tau`}(C(t_1, s_1)) = \rho_{[\tau,\tau`]}(C(t_j, s), Q^j),$$

где s – произвольное состояние из S. Из свойств метрики Хэмминга заключаем: при любом $t \in T$ и любых s, s` из S

$$\rho_{[\tau,\tau`]}(C(t, s), C(t, s`)) \le 2\rho_{\tau`}(C(t_1, s_1)).$$

Предположим сначала, что в качестве $\tau`$ нами было взято τ и мера $\rho_\tau(C(t_1, s_1)) = 0$. Тогда последнее неравенство имеет вид

$$\rho_\tau(C(t, s), C(t, s`)) = 0$$

при любых $t \in T$ и $s, s` \in S$. Последнее противоречит условию теоремы о том, что $R > 0$. Таким образом, в частности доказано, что τ кратно хотя бы одному делителю из $\{d_j\}$. Учитывая это, из последнего неравенства получаем

$$\rho_{d_0}(C(t, s), A(t, s`)) \le 2\rho_{\tau`}(C(t_1, s_1))$$

при любых $t \in T$, $s, s` \in S$.

Напомним, что условие 2 теоремы говорит о том, что $1 \le N \le d_0$ и

$$\rho_N(C(t_0, s_0), C(t_0, s`_0)) \ge R > 0.$$

Следовательно,

$$R \le 2\rho_{\tau`}(C(t_1, s_1)),$$

что противоречит условию теоремы

$$2\rho_{\tau`}(C(t_1, s_1)) < \frac{R}{2}.$$

Таким образом, предположение о том, что для любое d_j из множества $\{d_j\}$ не делит $\tau`$, не выполняется, следовательно, $\tau`$ кратно хотя бы одному из чисел множества $\{d_j\}$. Теорема доказана.

Из доказательства теоремы 1 вытекает следствие 1.

Следствие 1. Пусть $C = B \to A$ – полноцикловый автомат с периодом выходной последовательности равной $|S_1|\cdot|S_2|$, d – произвольный собственный делитель числа $|S_1|\cdot|S_2|$. Если для некоторого $L \le |S_1|\cdot|S_2|$ нашлось $v \in \{1, 2, \ldots, \frac{|S_1|\,|S_2|}{d} - 1\}$ и состояние $(t, s) \in T \times S$, для которого

$$\rho_L(C(t, s), C(\delta_C^{vd}(t, s))) > R \ge 0,$$

то для любой периодической последовательности Q элементов алфавита Y периода $\tau`$, $(\tau`, |T|\cdot|S|) = d$ и любого начального состояния (t, s) автомата C:

$$\rho_{[|T|\cdot|S|],\,\tau`]}(C(t, s), Q) \ge \frac{R}{2}.$$

Следствие 2. При выполнении условий теоремы 1

$$\tau` \ge d_0,$$

в частности, $\tau \ge d_0$.

Следствие 3. Пусть выполнены условия теоремы 1 и дополнительно $|T| = P^\alpha$, $\alpha \ge 1$, $|S| = P$, P – простое число. Тогда $P^{\alpha+1} | \tau`$, в частности, $\tau = P^{\alpha+1}$.

Заметим, что при формулировке теоремы 1 и ее следствий не было использовано конструктивного, явного задания функции Ф. В ряде случаев функция Ф может быть сложной функцией, или же она может быть задана неявным образом, например, алгоритмически.

21.2. Полноцикловое последовательное соединение автономного автомата с перестановочным коммутируемым автоматом

Утверждение теоремы 1 для некоторых классов перестановочных автоматов A и функций Ф допускает следующие уточнения.

Напомним, что $A = (X, S, (h_x)_{x\in X})$ называется коммутируемым автоматом, если при любых $x, x'\in X$ $h_x h_{x'} = h_{x'} h_x$. Выберем произвольное состояние $t_1\in T$ полноциклового автомата $B = (T, Y_B, \delta, \lambda)$, $Y_B = X$. Тогда при $B(t_1) = x(1), x(2), \ldots, x(|T|), \ldots$ подстановка $\Pi = h_{x(|T|)}\ldots h_{x(2)}h_{x(1)}$ не зависит, в силу коммутируемости A_2, от выбора $t\in T$.

Теорема 2. Пусть $C = B\to A$ полноцикловый автомат с выходной функцией $\Phi: T\times S\to Y$, причем A – перестановочный коммутируемый автомат, $\tau`$ – приближенный период с мерой $R$ выходной последовательности $C(t, s)$ периода $\tau$ автомата $C$, $(t, s)\in T\times S$. И пусть $(\tau, \tau`) = D_1\cdot D_2 = d'$, где $D_1 = (d`, |T|)$. Тогда для любых пар состояний автомата C вида: $(t, s), (t, \prod^{\nu\cdot D2} s), \nu\in\{0, 1, 2, \ldots\}$

$$\rho_{[\tau,\tau`]}(C(t, s), C(t, \prod^{\nu\cdot D2} s)) \le 2R.$$

Доказательство. Аналогично началу доказательства теоремы 1 получаем для $c\in\{0, 1, 2, \ldots\}$, $j\in\{1, 2, \ldots\}$, $t = t_1$, $s = s_1$

$$R = \rho_{[\tau,\tau`]}(C(t_{j+cd`}, s_{j+cd`}), Q^j).$$

При $c = \nu\cdot\frac{|T|}{D_1}$, $\nu\in\{0, 1, 2, \ldots\}$ в обозначениях теоремы I имеем

$$R = \rho_{[\tau,\tau`]}(C(t_j, \prod^{j\cdot D2} s_j), Q^j).$$

Откуда, учитывая, в частности, коммутируемость автомата A, полноцикловость B, получаем утверждение теоремы.

Следствие 4. Пусть выполнены условия теоремы 2 и дополнительно

$$\tau` = \tau = D_1D_2, R = 0, D_1 = (\tau, |T|).$$

Тогда при любом $(t, s)\in T\times S$ состояния вида $(t, \prod^{\nu\cdot D2}s)$, $\nu\in\{0, 1, \ldots, \frac{|S|}{D_2}\}$ неотличимы в автомате C, то есть $C(t, \prod^{\nu\cdot D2}s) = C(t, \prod^{\nu`\cdot D2}s)$, $\nu, \nu`\in\{0, 1, \ldots, \frac{|S|}{D_2}\}$.

21.3. Класс функций выхода полноциклового последовательного соединения автономного автомата с перестановочным коммутируемым автоматом

Ниже дается развитие результатов для функций выхода Φ автомата $C = B\to C$ из некоторых классов функций.

Пусть $Y`$, $Y``$ – некоторые новые алфавиты и заданы отображения:

$$\psi: T\to Y`;$$

$$\varphi: S \to Y``;$$
$$F: Y` \times Y`` \to Y,$$

причем при любой паре $(y`, y) \in Y` \times Y$ *уравнение*

$$F(y`, y``) = y$$

однозначно разрешимо относительно $y`` \in Y``$.

Определим вспомогательный автомат Мура $A_\varphi = (X, S, Y``, (h_x)_{x \in X}, \varphi)$ и вспомогательный автономный полноцикловый автомат $A_{\varphi, \Pi} = (S, Y``, \Pi, \varphi)$ функциями выхода φ и функцией перехода Π (подстановка Π определена в начале раздела 2.1.2). Через $A_\varphi(P, s)$ $(A_{\varphi, \Pi}(s))$ будем обозначать выходную последовательность автомата A_φ $(A_{\varphi, \Pi})$, отвечающую его входной последовательности P и начальному состоянию $s \in S$ (отвечающую его начальному состоянию $s \in S$). Напомним, что автомат $A_{\varphi, \Pi}$ называют приведенным, если для его любых различных состояний s, s`

$$A_{\varphi, \Pi}(s) \neq A_{\varphi, \Pi}(s`).$$

Для произвольного делителя D числа $|S|$ и произвольного $s \in S$ и $\nu \in \{0, 1, \ldots\}$ определим меру близости $\rho_{|S_2|}^{(\nu, D)}$ выходных последовательностей $A_{\varphi, \Pi}(s)$, $A_{\varphi, \Pi}(\Pi^{\nu \cdot D} s)$ автомата $A_{\varphi, \Pi}$ при начальных состояниях s и $\Pi^{\nu \cdot D} s$ из S.

$$\rho_{|S_2|}^{(\nu, D)} = \rho_{|S|}(A_{\varphi, \Pi}(s), A_{\varphi, \Pi}(\Pi^{\nu \cdot D} s)).$$

Обозначим через $\rho_{|S|}(D)$ максимальное значение $\rho_{|S_2|}^{(\nu, D)}$, $\nu \in \{0, 1, \ldots\}$.

Легко показывается, что введенные меры близости не зависят от выбора $s \in S$.

Теорема 3. Пусть $C = B \to A$ – полноцикловый автомат, A – коммутируемый автомат, функция выхода Φ автомата C имеет вид либо

1) $\Phi(t, s) = F(\psi t, \varphi s)$, ψ, φ, F – введены ранее,

либо

2) $\Phi(t, s) = \varphi(s)$.

Пусть $\tau`$– приближенный период с мерой R, выходной последовательности C(t, s) периода $\tau$, автомата C, отвечающей его начальному состоянию $(t, s) \in T \times S$, причем $(\tau, \tau`) = D_1 D_2 = d'$, где $D_1 = (d`, |T|)$.

Тогда

$$[\tau, \tau`] \cdot \rho_{|S|}(D_2) \leq 2|S| \cdot R,$$

где параметр $\rho_{|S2|}(D_2)$ введен перед теоремой 3.

Доказательство. По определению τ` и R найдется последовательность Q = $\overline{y_1}, \overline{y_2}$, … элементов из Y периода τ`, для которой

$$\rho_{[\tau,\tau`]}(C(t, s), Q) = R.$$

Пусть $t = t_1$, $s = s_1$ и $(t_1, s_1),(t_2, s_2)$, …, (t_j, s_j), ... – последовательность состояний автомата C, отвечающая его начальному состоянию (t_1, s_1). Аналогично началу доказательства теоремы 1 получаем для $c \in \{0, 1, 2, ...\}$, $j \in \{1, 2, \ldots\}$

$$R = R = \rho_{[\tau, \tau`]}(C(t_{j+cd`}, s_{j+cd`}), Q^j).$$

При $c = \frac{|T|}{D_1} \cdot \nu$, $\nu \in \{0, 1, 2, \ldots\}$, в обозначениях доказательства теоремы I, имеем

$$R = \rho_{[\tau, \tau`]}(C(t_j, \Pi_j^{\nu D_2} s_j), Q^j).$$

Из этого равенства получаем при $L = [[\tau, \tau`], |T|\cdot|S|]$

$$R \cdot \frac{L}{[\tau, \tau`]} = \rho_L(C(t_1, \Pi_1^{\nu D_2} s_1), Q^1),$$

откуда следует

$$\rho_L(C(t_1, \Pi_1^{\nu_1 D_2} s_1), C(t_1, \Pi_1^{\nu_2 D_2} s_1)) \le 2R\frac{L}{[\tau, \tau`]},\ \nu_1, \nu_2 \in \{0, 1, 2, \ldots\}.$$

Положим $B(t_1) = P = x_1, x_2, \ldots, x_{|T|}, \ldots$ Используя структуру функции Φ, характеризующую однозначную разрешимость уравнения F(y`, y``) = y относительно y`` либо то, что Φ = φ, из последнего неравенства получаем

$$R_{L,\nu} = \rho_L(A_\varphi(P, s_1), A_\varphi(P, \Pi_1^{\nu \cdot D_2} s_1)) \le 2R\frac{L}{[\tau, \tau`]}.$$

Рассмотрим выборочные подпоследовательности

$$A_{\varphi, \Pi}(s_j), A_{\varphi, \Pi}(\Pi^{\nu \cdot D_2} s_j), j \in \{1, 2, \ldots\},$$

соответственно, последовательностей $A_\varphi(P, s_1)$, $A_\varphi(P, \Pi_1^{\nu \cdot D_2} s_1)$. Здесь в обозначениях учтена коммутируемость автомата A ($\Pi_j = \Pi$).

Имеем

$$R_{L,\nu} = \sum_{j=1}^{|T|} \rho_{\frac{L}{|T|}}(A_{\varphi, \Pi}(s_j), A_{\varphi, \Pi}(\Pi^{\nu \cdot D_2} s_j)).$$

По условию теоремы каждое слагаемое при соответствующем выборе ν принимает одновременно максимальное свое значение $\rho_{|S|}(D_2) \cdot \frac{L}{|T|\,|S|}$. Поэтому

$$\max_\nu R_{L,\nu} = \rho_{|S|}(D_2) \cdot \frac{L \cdot |T|}{|T|\,|S|}.$$

Следовательно,

$$\frac{L}{|S|}\cdot\rho_{|S|}(D_2) \le 2R\frac{L}{[\tau,\tau`]}$$

или

$$\frac{[\tau,\tau`]\cdot\rho_{|S|}(D_2)}{2|S|} \le R,$$

что и требовалось доказать.

Следствие 5. Пусть выполнены условия теоремы 3 и дополнительно к ним $A_{\varphi,\,\Pi}$ – приведенный автомат. Тогда период τ последовательности $C(t, s)$, $(t, s)\in T\times S$ кратен $|S|$.

Теорема 4. Пусть $C = B\to A$ – полноцикловый автомат, A – коммутируемый, автомат $A_{\varphi,\,\Pi}$ приведен, период выходной последовательности B(t) автомата B равен $|T|$ и выполнено одно из следующих двух условий:

1) функция выхода автомата C имеет вид $\Phi(t, s) = \varphi(s)$,
2) функция выхода имеет вид $\Phi(t, s) = F(\psi(t), \varphi(s))$,

где

$$\psi: T\to Y`,\ \varphi: S\to Y``,\ F: Y`\times Y``\to Y,$$

причем уравнение $F(y', y'') = y$ при любой паре $(y', y)\in Y`\times Y$ однозначно разрешимо относительно $y''\in Y``$ и при любой паре $(y'', y)\in Y``\times Y$ однозначно разрешимо относительно $y'\in Y`$. Обозначим через $F_{y'}$ отображение Y``в Y, положив $F_{y'}(y'') = F(y', y'')$, а через $F^{-1}_{y`}$ – обратное к $F_{y`}$ отображение. Положим для $y`_1, y`_2\in Y`$, $\chi_{y`_1 y`_2} = F^{-1}_{y`_1}\cdot F_{y`_2}$ – отображение Y``в Y``и пусть порядки этих отображений при $y`_1, y`_2\in Y`$ взаимно просты с $|S|$.

Тогда период выходной последовательности $C(t, s)$ автомата A с начальным состоянием (t, s) равен $|T||S|$.

Доказательство. Пусть τ – период выходной последовательности $C(t_1, s_1)$ автомата C, а $(t_1, s_1),(t_2, s_2), ..., (t_j, s_j), ...$ – его последовательность состояний. Для любого $c\in\{0, 1, 2, \ldots\}$ имеем

$$C(t_1, s_1) = C(s_{1+c\tau}, s_{1+c\tau})$$

или

$$F(\psi(s_j), \varphi(\Pi^{\nu}s_j)) = F(\psi(sj+c\tau), \varphi(\Pi^{\nu}s_{j+c\tau})) \qquad (23)$$

при выполнение второго условия теоремы и

$$\psi(\Pi^{\nu}s_j) = \varphi(\Pi^{\nu}s_{j+c\tau}),\ \nu\in\{1, ..., |S|\},\ j\in[1, 2\ldots)$$

при выполнении первого условия теоремы. В последнем случае, в силу приведенности автомата $A_{\varphi,\,\Pi}$, получаем $s_j = s_{j+c\tau}$, откуда $\tau = |T|\cdot|S|$, так как автомат C полноцикловый и период последовательности $B(t_1)$ равен $|T|$.

Пусть выполнено второе условие теоремы. Нам достаточно доказать, что при любых j и c $s_j = s_{j+c\tau}$, для чего, в свою очередь, в силу (23) и приведенности автомата $A_{\varphi, \Pi}$ достаточно показать, что

$$\psi(t_j) = \psi(s_{j+c\tau}) \qquad (24)$$

при любых j и c. Допустим противное: нашлись j(0) и c(0), при которых

$$\psi(t_{j(0)}) = y`_1 \neq \psi(s_{j(0)+c(0)\tau}) = y`_2.$$

Для этих j(0), c(0) из (23) получаем

$$\varphi(\Pi^{\nu} s_{j(0)}) = F^{-1}_{y`_1} F_{y`_2} \varphi(\Pi^{\nu} s_{j(0)+c(0)\tau}).$$

Положим $s_{j(0)} = \Pi^{L(0)} s_{j(0)+c(0)\tau}$ и перепишем последние равенства в виде

$$\varphi(\Pi^{L(0)}\Pi^{\nu} s_{j(0)+c(0)\tau}) = \chi_{y`_1 y`_2} \varphi(\Pi^{\nu} s_{j(0)+c(0)\tau})$$

или при любом $s \in S$

$$\varphi(\Pi^{L(0)} s) = \chi_{y`_1 y`_2} \varphi(s),$$

так как $A_{\varphi, \Pi}$ – полноцикловой автомат. Итерируя, получаем при любом k

$$\varphi\Pi^{kL(0)} = (\chi_{y`_1 y`_2})^k \varphi.$$

Пусть k(0) – минимальное k, при котором $(\chi_{y`_1 y`_2})^k \varphi = \varphi$. Через deg будем обозначать порядок рассматриваемых подстановок. Очевидно, что

$$k(0) \mid \deg \chi_{y`_1 y`_2} \text{ и } k(0) \mid \deg \Pi^{L(0)}, \deg \Pi^{L(0)} \mid |S|.$$

Так как по условию $(|S|, \deg \chi_{y`_1 y`_2}) = 1$, то k(0) = 1, откуда имеем

$$\varphi\Pi^{L(0)} = \varphi.$$

Теперь, так как $A_{\varphi, \Pi}$ – приведенный автомат, то $\Pi^{L(0)}$ – тождественная подстановка, откуда следует

$$s_{j(0)} = s_{j(0)+c(0)\tau}.$$

Подставляя эти состояния в уравнения (23) и учитывая однозначную разрешимость этих уравнений, получаем

$$\psi(t_{j(0)}) = \psi(t_{j(0)+c(0)\tau}),$$

то есть получили требуемое уравнение (24). Теорема 4 полностью доказана.

Замечание. Пусть $Y = Y` = Y`` = F_2$ – поле из двух элементов. Тогда для функции F вида F(y`, y``) = y`+y``, отображение $\chi_{y`_1 y`_2}$ имеет порядок 2, если $y`_1 \neq y`_2$, и порядок равен 1, если $y`_1 \neq y`_2$. Следовательно, условие 1 – порядки отображений $\chi_{y`_1 y`_2}$

взаимно просты – в нашем случае принимает вид: число |S| – нечетное.

Пусть теперь Y = Y` = Y`` = G – некоторая группа с операцией (•) и F имеет вид F(y`, y``) = y`•y``. Тогда условие 1 эквивалентно условию (|G|, |S|) = 1.

21.4. Автономное последовательное соединение автоматов со свойством принудительного восстановления состояния второго автомата

Рассмотрим следующее устройство (рис. 18) со свойством восстановления (УСВ), состоящее из автоматов B = (T, Y_1, δ, λ), A = (X, S, Y, $(h_x)_{x\in X}$, $(f_x)_{x\in X}$), Y_1 = X. УСВ:

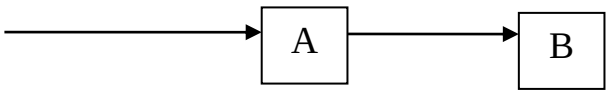

Рис. 18

Если $(t_1, s_1)\in T\times S$ – начальное состояние устройства, то последовательность его состояний $\{(t_j, s_j)\}$, $j\in[1, 2, \ldots)$ имеет вид

$$(t_j, s_j) = \begin{cases} (\delta t_j, h_{\lambda t_j} s_j), & \text{если L не делит j,} \\ (\delta t_j, s_1), & \text{если L делит j,} \end{cases}$$

где L – некоторое фиксированное натуральное число. Выходная последовательность УСВ Q = $y_1, y_2, \ldots$ при его начальном состоянии $(t_1, s_1)\in T\times S$ имеет вид

$$y_j = f_{\lambda(t_j)} s_j .$$

Пусть B – полноцикловый автомат. Тогда последовательность Q – периодическая, с периодом τ, делящим величину L·|T|. Для произвольной периодической последовательности Q` элементов из Y периода τ` положим

$$\mu(Q, Q`) = \frac{\rho_{[\tau,\tau`]}(Q,Q`)}{[\tau,\tau`]}.$$

Заметим, что величина μ является метрикой на множестве периодических последовательностей. Рассмотрим множество M = {τ`: τ не делит τ`} периодических последовательностей элементов алфавита Y периодов, не кратных τ, и величину

$$\min_{Q`\in M}\mu(Q,Q`)\cdot$$

Несложно показывается, что данный минимум достигается на некоторой последовательности Q^ периода τ^ | τ. Доказательство этого факта содержится в [8].

Представляет интерес оценка значения величины μ(Q, Q^). Для получения такой оценки введем необходимые понятия.

Пусть U = (P(1), P(2), …, P(r)) некоторое семейство слов длины L алфавита X, среди которых возможны и одинаковые слова. Обозначим через A(P(j), s) выходное слово длины L автомата A, отвечающее входу $P(j)\in X^L$ и начальному состоянию $s\in S$.

Определение 2. Степенью приближенной автономности состояния s автомата A относительно множества U входных слов назовем величину

$$\min_{\tilde{y}_1,\tilde{y}_2,\ldots,\tilde{y}_L\in Y^L}\ \frac{1}{r\cdot L}\sum_{j=1}^{r}\rho_L(A(P(j),s);\tilde{y}_1,\tilde{y}_2,\ldots\tilde{y}_L)=C(s,U),$$

а набор $y_1^0, y_2^0, \ldots, y_L^0$, на котором достигается данный минимум назовем приближенным выходом автомата A_2 с состояния s относительно U.

Теорема 5. Пусть B – полноцикловый автомат, (L, |T|) = 1, |T| – простое число Q = $y_1, y_2, \ldots$ – выходная последовательность УСВ периода τ, отвечающая начальному состоянию $(t_1, s_1)\in T\times S$; $\overline{y'} = \overline{y_1}, \overline{y_2}, \ldots$ последовательность периода τ` из множества M, для которой $\min_{Q`\in M}\mu(Q, Q`) = \mu(Q, \overline{y'})$. Тогда, если τ` не кратно |T|, то

$$\mu(Q, \overline{y'}) = C(s, (B(t)]_L)_{t\in T}),$$

где $B(t)]_L$ – выходная последовательность длины L автомата B с начального состояния $t\in T$.

Доказательство. Имеем τ | |T|·L и τ` | τ, поэтому τ` | |T|·L. Так как |T| – простое число, то в случае, когда |T| не делит τ`, получаем τ` | L. Учитывая теперь закон функционирования УСВ и факт τ`|L, имеем для $\overline{y'} = \overline{y_1}, \overline{y_2}, \ldots$

$$\mu(Q, \overline{y'}) = \frac{\rho_{|T|\cdot L}{}^{(Q,\tilde{y}')}}{|T|\cdot L} = \frac{1}{|T|\cdot L}\sum_{k=0}^{|T|-1}\rho_L(A(B(t_{kL+1})]_L,s_1);\overline{y_1},\overline{y_2},\ldots\overline{y_L}).$$

Используем теперь условие (L, |T|) = 1, и получаем

$$\mu(Q, \bar{y}') = \frac{1}{|T| \cdot L} \sum_{t` \in T} \rho_L(A(B(t`)]_L, s_1); \bar{y}_1, \bar{y}_2, \ldots \bar{y}_L) \geq C(s_1, (B(t`)]_L)_{t` \in T}).$$

С другой стороны, для приближенного выхода y_1^0, y_2^0, …, $y_L^0 = \hat{y}$ с состояния s_1 относительно набора входных слов $(B(t`)]_L)_{t` \in T}$, можно построить периодическую последовательность $Q^\wedge = \hat{y}, \hat{y}, \ldots$, состоящую из слов $\hat{y}$ периода $d \mid L$, для которой, очевидно, $\mu(Q, Q^\wedge) = C(s_1, (B(t`)]_L)_{t' \in T})$, а по определению, $M(Q, \bar{y}')$,

$$\mu(Q, \bar{y}') \leq \mu(Q, Q^\wedge).$$

Следовательно,

$$\mu(Q, \bar{y}') = C(s, (B(t)]_L)_{t \in T}).$$

Глава 22. G-ИЗОПЕРИОД ВЫХОДНОЙ ПОСЛЕДОВАТЕЛЬНОСТИ АВТОНОМНОГО ПОСЛЕДОВАТЕЛЬНОГО СОЕДИНЕНИЯ АВТОМАТОВ

В главе вводится и изучается понятие изопериода последовательности. Оценивается изопериод выходной последовательности автономного последовательного соединения автоматов.

С одной стороны, приводимые ниже результаты, характеризующие G-изопериоды выходных последовательностей автоматов указанного в заголовке класса, тесно связаны с известной классической проблемой оценки периодов выходных последовательностей конечных автоматов, поставленной в книгах по теории автоматов, например, авторов Н. Е. Кобринского, Б. А. Трахтенброта и В. Б. Кудрявцева, С. В. Алешина, А. С. Подколзина.

С другой стороны, введение и изучение понятия изопериода выходных последовательностей автомата полезно в криптографии. Так, одним из требований к синтезу управляющих блоков многоалфавитных поточных шифров является требование того, что в управляющей гамме должны отсутствовать простые аналитические зависимости между близко расположенными знаками.

Вводится понятие g-изопериода последовательности, обобщающее понятие периода периодической последовательности.

Указывается методика расчета численных параметров g-изопериода для: последовательности состояний и выходной последовательности конечного автомата при заданных входной последовательности и начальном состоянии; для выходной последовательности последовательного соединения полноциклового автомата с неавтономным автоматом. (Ниже используются результаты, которые опубликованы в [5; 37].)

22.1. Основные понятия и предварительные результаты

Напомним некоторые обозначения: (a, b) – общий наибольший делитель чисел a, b; [a, b] – наименьшее общее кратное чисел a, b; НОК(a_j), $j \in \{1, ..., d\}$ – наименьшее общее кратное чисел a_j, $j \in \{1, ..., d\}$; a|b – a делит b; ordg – порядок элемента g группы.

Пусть Y – конечный алфавит, $|Y| \geq 2$, σ – бинарное отношение на Y.

Определение 1. Последовательность $Q = y_1, y_2, \ldots$ элементов алфавита Y называется σ-периодической, если существует натуральное число d, при котором $y_j \sigma y_{j+d}$ для любого $j \in \{1, 2, \ldots\}$. Число d называется σ-периодом последовательности Q.

Если в определении 1 σ – отношение равенства, то $Q = y_1, y_2, \ldots$ – периодическая последовательность и минимальное число d с указанным свойством является ее периодом.

В случае, когда σ – бинарное отношение на эквивалентности на Y, минимальный σ-период последовательности $Q = y_1, y_2, \ldots$ совпадает с периодом последовательности $[y_1], [y_2], \ldots$, где $[y_j]$ – класс эквивалентности, содержащий элемент y_j, $j \in \{1, 2, \ldots\}$. Если σ является отображением Y в Y, то последовательность $Q = y_1, y_2, \ldots$ будем называть *σ-изопериодической*, а минимальное число d – ее *σ-изопериодом*.

Полнотой θ(Q) последовательности $Q = y_1, y_2, \ldots$ назовем максимальное натуральное число k, если таковое существует, при котором каждое слово из Y^k содержится в Q в качестве k-граммы. *Степенью различимости R(Q) периодической последовательности Q* назовем минимальное число R, при котором все R-граммы последовательности Q различны.

Через C(Q) обозначим множество всех элементов $y \in Y$, содержащихся в $Q = y_1, y_2, \ldots$ Множество C(Q) назовем *содержанием последовательности* $Q = y_1, y_2, \ldots$ Отметим, что $\theta(Q) \geq 1$ тогда и только тогда, если C(Q) совпадает с алфавитом Y. Для последовательности $Q = y_1, y_2, \ldots$ через S(C(Q)) обозначим группу всех взаимно однозначных отображений C(Q) в C(Q), через ordσ – порядок отображения $\sigma \in S(C(Q))$.

Положим

$$M(\omega, C(Q)) = \{\sigma \in S(C(Q)): \mathrm{ord}\sigma | \omega\},$$

где ω – фиксированное натуральное число. Обозначим через E тождественное отображение C(Q) в C(Q). Очевидно, $E \in M(\omega, C(Q))$ при любых ω, C(Q).

Обозначим через D^{ω}_{min} минимальный делитель числа ω, отличный от единицы.

Для $\omega \in \{1, 2, \ldots\}$ положим

$$C(\omega, C(Q)) = \max \mathrm{ord}\sigma \text{ по всем } \sigma \in M(\omega, C(Q)).$$

Теорема 1. Пусть $Q = y_1, y_2, \ldots$ – периодическая последовательность элементов конечного алфавита Y периода ω. Если W_η являет-

ся η-изопериодом последовательности Q при некотором отображении η: Y→Y, то:

а) ограничение $\bar{\eta}$-отображения η на C(Q) является биекцией C(Q) в C(Q);

б) $\omega = d \cdot \mathrm{ord}\,\bar{\eta}$, где $d = (W_\eta, \omega)$;

в) $L_j^{\bar{\eta}} \mid \omega$, $j \in \overline{1, m(\bar{\eta})}$, где $L_j^{\bar{\eta}}$ – длина j-го цикла биекции $\bar{\eta}$, $m(\bar{\eta})$ – число циклов подстановки $\bar{\eta}$;

г) $d \geq \dfrac{\omega}{C(\omega, C(Q))}$, в частности, $W_\eta \geq \dfrac{\omega}{C(\omega, C(Q))}$;

д) $W_\eta \geq R(Q)$, где $R(Q)$ – степень различимости последовательности Q;

е) если дополнительно $D_{\min}^{\omega} > |C(Q)|$, то $W_\eta = \omega$, $\bar{\eta} = E$;

ж) d является $\eta^{\kappa(1)}$-изопериодом Q, где к(1) удовлетворяет условию

$$\text{к}(1)W_\eta - \text{к}(2)\omega = d,$$

к(1), к(2) – натуральные числа;

з) W_η – η^h-изопериод выборочной последовательности $y_1, y_{1+h}, \ldots$ шага h последовательности Q при $(h, \omega) = 1$.

Доказательство. Пусть $W = W_\eta$ – η-изопериод последовательности Q.

Тогда

$$y = y_{j+[W,\omega]} = \eta^{\frac{[W,\omega]}{W}}(y_j),\ j \in \{1, 2, \ldots\}.$$

Отсюда заключаем, что $\bar{\eta}$ – биекция C(Q) в C(Q). Обозначим через ω_j период последовательности $y_j, y_{j+d}, y_{j+2d}, \ldots$. Несложно показать, что

$$\omega = d\ \text{НОК}(\omega_j),\ j \in \{1, \ldots, d\}.$$

Очевидно, что ω_j является и периодом последовательности $y_j, y_{j+W}, \ldots$ Следовательно, $\omega_j = L(y_j)$, где $L(y_j)$ – длина цикла подстановки $\bar{\eta}$, содержащего элемент y_j. Заметим также, что число циклов $\bar{\eta}$ не превосходит d. Из указанных фактов вытекает

$$ord\bar{\eta} = HOK(\omega_1, \omega_2, \ldots, \omega_d).$$

Таким образом,

$$\omega = ord\bar{\eta}.$$

Откуда

$$d \geq \frac{\omega}{C(\omega, C(Q))},$$

И, в частности,

$$W \geq \frac{\omega}{C(\omega, C(Q))},$$

откуда следует утверждение е). Утверждения д), ж), и) несложно доказываются стандартными приемами. Теорема доказана.

Рассмотрим частные случаи η-изопериодичности некоторых последовательностей.

Пусть Y = G, где G – некоторая конечная группа.

Определение 2. Последовательность Q = y_1, y_2, ... элементов группы G назовем G-изопериодической слева (справа), если существует элемент g∈G и натуральное и натуральное число W_g, при которых

$$y_{j+W_g} = g y_j \,;\, j \in \{1,2,\ldots\}, \; (y_{j+W_g} = y_j g \,;\, j \in \{1,2,\ldots\}).$$

Минимальное натуральное число W_g, обладающее указанным свойством для данного g, назовем левым (правым) g-изопериодом – g-изопериодической слева (справа) последовательности Q.

Определение 3. Последовательность Q = y_1, y_2, ... элементов группы G назовем двухсторонне G-периодической, если существуют элементы g∈G, h∈G и натуральное число $W_{g,\,h}$, при которых

$$g_{j+W_{g,h}} = g y_j h, \; j \in \{1, 2, \ldots\}.$$

Минимальное число $W_{g,\,h}$, обладающее указанным выше свойством для данных g, h назовем двухсторонним (g, h)-изопериодом последовательности Q, а Q – двухсторонне (g, h)-изопериодической последовательностью.

Из утверждения теоремы 1 непосредственно вытекают следующие следствия.

Следствие 1. Пусть Q = y_1, y_2, ... – периодическая последовательность элементов конечной группы G периода ω. Если W_g – левый (правый) g-изопериод последовательности Q, g∈G, то

а) $\omega = d \cdot ord g$, где $d = (W_g, \omega)$;

б) $W_g \geq d \geq \frac{\omega}{C(\omega, G)}$, где $C(\omega, G) = \max\limits_{g' \in G:\; ord g' \mid \omega} ord g'$;

в) если дополнительно $(|G|, \omega) = 1$, то

$$W_g = \omega, \; g = e,$$

где e – единица группы G.

Следствие 2. Пусть Q = y_1, y_2, ... – периодическая последовательность элементов конечной группы G периода ω. Если $W_{g,\ h}$ – двухсторонний (g, h)-изопериод последовательности Q, то

а) $\omega = d \cdot HOK(L_{g_1}^{g,h},...,L_{g_d}^{g,h})$, где $d = (W_{g,h}, \omega)$, и $L_{g_j}^{g,h}$ – длина биекции $\eta_{g,h} : g' \to gg'h$, g`∈G, содержащей элемент g_j, j∈{1, ..., d};

б) $L_{g_j}^{g,h} | \omega$, $L_{g_j}^{g,h} | HOK(ordg, ordh)$, j∈{1, ..., d};

в) если НОК(ordg,ordh) и ω взаимно просты, $(HOK(ordg, ordh), \omega) = 1$, или (|G|, ω) = 1, то $W_{g,\ h} = \omega$.

Определение 4. Минимальное значение η-изопериодов периодической последовательности Q = y_1, y_2, ... при всех возможных отображениях η Y в Y назовем изопериодом последовательности Q.

Аналогично вводятся понятия левого, правого, двухстороннего G-изопериода периодической последовательности элементов конечной группы G.

Из пункта ж) теоремы 1 вытекает, что изопериод периодической последовательности всегда является делителем ее периода. Условие е) теоремы 1 гарантирует максимальность изопериода W = ω периодической последовательности Q = y_1, y_2, ... периода ω; условие в) следствия 1 гарантирует максимальность левого и правого G-изопериода W = ω периодической последовательности Q = y_1, y_2, ..., y_j∈G периода ω, а условие (|G|, ω) = 1 в пункте в) следствия 2 гарантирует максимальность двухстороннего G-изопериода W = ω последней последовательности.

Пусть A = (S, Y, h, λ) – полноцикловый автомат с множеством состояний S, S, |S| ≥ 2, выходным алфавитом Y, функцией перехода h и функцией выхода λ. При известном периоде ω выходной последовательности A(s) = y_1, y_2, ... автомата A теорема 1 дает оценки ее η-изопериода. В случае Y⊆G, где G – конечная группа, следствия 1, 2 дают дополнительные оценки ее левого, правого (g, h)-изопериода. Так, например, справедливо

Следствие 3. Пусть A = (S, Y, h, λ) – полноцикловый, приведенный автомат, |S| ≥ 2.

1. Если λ: S→Y – сюръективное отображение и минимальный делитель числа |S| больше |Y| ($D^{|S|}_{min} > |Y|$), то изопериод выходной последовательности A(s) = y_1, y_2, ... автомата A максимален и равен |S|.

2. Если $Y \subseteq G$, где G – конечная группа и $(|G|,|S|) = 1$, то левый, правый, двухсторонний G-изопериоды выходной последовательности $A(s) = y_1, y_2, \ldots$ автомата A максимальны и равны |S|.

22.2. Изопериод последовательности внешнего функционирования перестановочного автомата при заданной входной периодической последовательности

Пусть $A = (X, S, Y, (h_x)_{x\in X}, (f_x)_{x\in X})$ – конечный автомат. В данном пункте работы будем предполагать, что автомат A является перестановочным, то есть его частичные функции переходов $(h_x)_{x\in X}$ – биекции S в S. Через $G = \langle (h_x)_{x\in X} \rangle$ обозначим группу автомата A, а через $P = x(1), x(2), \ldots$ – периодическую входную последовательность автомата A периода ω.

Последовательность A(P) отображений $\lambda_j = f_{x(j)}h_{x(j-1)}\ldots h_{x(1)}$ S в Y

$$A(P) = \lambda_1, \lambda_2, \ldots, \lambda_j, \ldots = f_{x(1)}, f_{x(2)}h_{x(1)}, \ldots, f_{x(j)}h_{x(j-1)}\ldots h_{x(1)}, \ldots$$

назовем *последовательностью внешнего функционирования автомата* A при входной последовательности P.

Пусть g – произвольный элемент из симметрической группы подстановок на множестве S, в частности, g может принадлежать G.

Под *g-изопериодом последовательности* A(P) будем понимать минимальное натуральное число W_g, если оно существует, при котором

$$\lambda_j g = \lambda_{j+W_g},\ j \in \{1, 2, \ldots\}.$$

Через A(s, P) будем означать выходное слово автомата A соответствующее входному слову P и начальному состоянию s автомата A.

Для формулировки основного результата данного пункта введем следующее понятие.

Определение 5. Слова P, P` из $X^k$ называются вероятностно неотличимыми в автомате A, если число решений уравнения A(s, P) = Q, относительно $s \in S$ совпадает с числом решений уравнения A(s, P`) = Q , при любом $Q \in Y^k$.

Вероятность $P(Q/P)$ получения выходного слова Q в автомате A при входном слове P и случайном и равновероятном выборе его начального состояния $s \in S$ равна $\frac{N(Q,P)}{|S|}$, где N(Q, P) – число решений относительно $s \in S$ уравнения A(s, P) = Q. Таким образом, P и P`

вероятностно неотличимы в A тогда и только тогда, если $\boldsymbol{P}(Q/P) = \boldsymbol{P}(Q/P`)$ при любом $Q \in Y^k$.

Для последовательности $P = x(1), x(2), \ldots$ обозначим через P^j последовательность $x(j), x(j+1), \ldots$, а через $P^j]_k$ – *начальное слово длины k последовательности* P^j.

Теорема 2. Пусть $W_g = W$ – g-изопериод последовательности внешнего функционирования A(P) перестановочного автомата $A = (X, S, Y, (h_x)_{x\in X}, (f_x)_{x\in X})$ при входной периодической последовательности $P = P^1 = x(1), x(2), \ldots$ периода ω, $(W, \omega) = d$. Тогда при любом $k \in \{1, 2, \ldots\}$ мультиграммы $P^j]_k$ $P^{j+d}]_k$, $j \in \{1, 2, \ldots\}$ последовательности P вероятностно неотличимы в автомате A.

Доказательство. Пусть выполнены условия теоремы. Положим

$$\Pi_j = h_{x(j)}h_{x(j-1)}\ldots h_{x(1)}h_{x(\omega)}h_{x(\omega-1)}\ldots h_{x(j-1)}.$$

Тогда, при натуральных k(1), k(2) таких, что $k(1)W - k(2)\omega = d$, и $c \in \{1, 2, \ldots\}$ имеем

$$f_{x(j)}h_{x(j-1)}\ldots h_{x(1)}g^{ck(1)} = f_{x(j+ck(1)W)}h_{x(j+ck(1)W-1)}\ldots h_{x(1)} = f_{x(j+cd)}h_{x(j+cd-1)}\ldots h_{x(1)}\Pi_\omega^{ck(2)}.$$

Следовательно,

$$f_{x(j)}h_{x(j-1)}\ldots h_{x(1)}g^{k(1)}\Pi_\omega^{-k(2)} = f_{x(j+d)}h_{x(j-1+d)}\ldots h_{x(1)}$$

$$f_{x(j+1)}h_{x(j)}\ldots h_{x(1)}g^{k(1)}\Pi_\omega^{-k(2)} = f_{x(j+1+d)}h_{x(j+d)}\,h_{x(j-1+d)}\ldots h_{x(1)}$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$f_{x(j+k-1)}h_{x(j+k-2)}\ldots h_{x(j)}h_{x(j-1)}\ldots h_{x(1)}g^{k(1)}\Pi_\omega^{-k(2)} = f_{x(j+k-1+d)}h_{x(j+k-2+d)}\ldots h_{x(1)}$$

Откуда непосредственно следует вероятностная неотличимость мультиграмм $P^j]_k$, $P^{j+d}]_k$. Теорема доказана.

Через θ(A, ВН) обозначим максимальное k, если оно существует, при котором каждая пара слов из X^k вероятностно неотличима (ВН) в автомате A.

Следствие 4. Пусть P – входная периодическая последовательность простого периода ω перестановочного автомата A и $\theta(P) > \theta(A, ВН)$, тогда любой g-изопериод последовательности A(P) кратен ω.

22.3. Изопериоды полноциклового автомата, представимого последовательным соединением двух автоматов

Пусть $A_1 = (S_1, Y_1, h, \lambda)$ – автономный автомат, $A_1({}^1s)$ – выходная последовательность автомата A_1 с начального состояния ${}^1s \in S_1$; $A_2 = (X, S_2, (h_x)_{x\in X})$ – неавтономный автомат без выходов, $Y_1 = X$; $A_2({}^2s, P)$ – последовательность состояний автомата A_2, отвечающая

его начальному состоянию ${}^2s \in S_2$ и входной последовательности P. Через $A = A_1 \xrightarrow{\Phi} A_2$ обозначим последовательное соединение автомата $A_1 = (S_1, Y_1, h, \lambda)$ с автоматом $A_2 = (X, S_2, (h_x)_{x \in X})$. Символ Φ обозначает выходную функцию $\Phi: S_1 \times S_2 \to Y$ этого последовательного соединения. Для описания класса рассматриваемых ниже функций Φ введем вспомогательные функции, $\psi: S_1 \to Y`$, $\varphi: S_2 \to Y``$ и $F: Y` \times Y`` \to Y$. Будем считать, что функция F инъективна по последней переменной, в связи с чем удобно использовать обозначение $F_{y`}(y``) = F(y`, y``)$, $(y`, y``) \in Y` \times Y``$ для отображения $F_{y`}$ в Y.

Автомат A_2 назовем *коммутируемым*, если $h_x h_{x`} = h_{x`} h_x$ для любых $x, x` \in X$.

Ниже нам потребуется описание следующего вспомогательного автомата $A_{\varphi, \Pi} = (S2, \Pi, \varphi)$ с функцией выходов φ и функцией переходов $\Pi = h_{x(|S_1|)} h_{x(|S_1|-1)} \ldots h_{x(2)} h_{x(1)}$, где x(1), x(2), ... – выходная последовательность автомата A_1 с некоторого его начального состояния.

Теорема 3. Пусть $A = A_1 \xrightarrow{\Phi} A_2$ – полноцикловый автомат; $\Phi({}^1s, {}^2s) = F(\psi({}^1s), \phi({}^2s))$, $({}^1s, {}^2s) \in S_1 \times S_2$, причем функция F инъективна по последней переменной; A_1 – полноцикловый приведенный автомат; A_2 – коммутируемый автомат; период последовательности состояний $A_2({}^2s, P)$ при $P = A_1({}^1s)$, ${}^1s \in S_1$ кратен величине $|S_1|$; для автомата $A_{\varphi, \Pi} = (S_2, \Pi, \varphi)$ выполняется свойство: при фиксированной биекции σ Y в Y любой η-изопериод выходной последовательности $A_{\varphi, \Pi}({}^2s)$ автомата $A_{\varphi, \Pi}$ равен $|S_2|$ при $\eta \in \{F_{y`}^{-1} \sigma F_{\overline{y`}} : y`, \overline{y`} \in Y`\}$. Тогда σ-изопериод выходной последовательности $A({}^1s, {}^2s)$ автомата A равен $|S_1||S_2|$.

Докажем теорему с помощью следующей леммы.

Лемма 1. Пусть $A = A_1 \xrightarrow{\Phi} A_2$ – полноцикловый автомат; $\Phi({}^1s, {}^2s) = F(\psi({}^1s), \phi({}^2s))$, причем функция F инъективна по последней переменной; A_1 – полноцикловый приведенный автомат; A_2 – коммутируемый автомат. Если W_σ – σ-изопериод выходной последовательности $A({}^1s, {}^2s)$ автомата A и W_σ не кратен периоду $\tau({}^1s_1)$ последовательности состояний $A_2({}^1s_1, A_1({}^1s_2))$ автомата A_2, то найдутся биекции $F_{y`}$, $F_{\overline{y`}}$ алфавита Y`` в Y, при которых выходная последовательность $A_{\phi, \Pi}({}^2s_1)$ автомата $A_{\varphi, \Pi}$ η-изопериодична с η-изопериодом $W_\eta < |S_2|$, где $\eta = F_{y`}^{-1} \sigma F_{\overline{y`}}$.

Доказательство. Пусть W = W_σ – σ-изопериод последовательности $A({}^1s_1, {}^2s_1)$ и $({}^1s_1, {}^2s_1),({}^1s_2, {}^2s_2),\ldots$ – последовательность состояний автомата A. Для любого j∈{1, 2, ...} имеем

$$F(\psi({}^1s_{j+W}),\phi({}^2s_{j+W})) = \sigma F(\psi({}^1s_j),\phi({}^2s_j)).$$

Для j = к+p|S_1|, (к, p)∈{1, 2, ...} получаем

$$F(\psi({}^1s_{\kappa+W}),\phi({}^2s_{\kappa+p|S_1|+W})) = \sigma F(\psi({}^1s_\kappa),\phi({}^2s_{\kappa+p|S_1|})).$$

Из условий леммы следует, что последнее равенство равносильно равенству

$$\phi(\Pi^p\ {}^2s_{\kappa+W}) = F^{-1}_{\psi({}^1s_{\kappa+W})}\sigma F_{\psi({}^1s_\kappa)}(\phi(\Pi^p\ {}^2s_\kappa)).$$

По условию леммы, период W не кратен периоду последовательности состояний ${}^2s_1, {}^1s_2,\ldots$ автомата A_2. Следовательно, найдется к`, при котором ${}^2s_{\kappa'+W} \neq {}^2s_{\kappa'}$. В силу полноцикловости автомата A отображение П – полноцикловое. Выберем натуральное число m = m(к`) исходя из условия:

$${}^2s_{\kappa'+W} = \Pi^m\ {}^2s_{\kappa'},\ 1 \le m < |S_2|.$$

Тогда

$$\phi(\Pi^{p+m}\ {}^2s_\kappa) = F^{-1}_{\psi({}^1s_{\kappa'+W})}\sigma F_{\psi({}^1s_{\kappa'})}(\phi(\Pi^p\ {}^2s_{\kappa'})),\ p\in\{0, 1, 2, \ldots\}.$$

Следовательно, последовательность $A_{\varphi,\Pi}({}^2s_{\kappa`})$ – η-изопериодическая для $\eta = F^{-1}_{\psi({}^1s_{\kappa'+W})}\sigma F_{\psi({}^1s_{\kappa'})}$ и ее η-изопериод W_η удовлетворяет неравенствам

$$W_\eta \le m < |S_2|.$$

Перейдем к доказательству теоремы 3. Из условий теоремы несложно получить, что период последовательности состояний $A_2({}^2s, A_1({}^1s))$ автомата A_2 равен $|S_1||S_2|$. Предположим, что W ≠ $|S_1||S_2|$. Тогда $|S_1||S_2|$ не делит W_σ, так как для периодической последовательности всегда ее σ-изопериод не превосходит ее периода. По лемме 1, найдется $\eta\in\{F^{-1}_{y`}\sigma F_{\overline{y`}} : y`, \overline{y`}\in Y`\}$, при котором выходная последовательность полноциклового автомата $A_{\varphi,\Pi}$ имеет η-изопериод $W_\eta < |S_2|$, что противоречит условиям теоремы 3. Теорема доказана.

Отметим, что при σ = E (E – тождественное отображение Y в Y) условия теоремы 3 гарантируют максимальность периода выходной последовательности автомата A = $A_1 \xrightarrow{\Phi} A_2$.

Из теоремы 3 непосредственно вытекает следующее следствие.

Следствие 5. Пусть A = $A_1 \xrightarrow{\Phi} A_2$ – полноцикловый автомат; $\Phi({}^1s, {}^2s) = F(\psi({}^1s),\phi({}^2s))$, причем функция F(y`, y``) инъективна по по-

следней переменной; A_1 – приведенный автомат; A_2 – коммутируемый автомат; период последовательности состояний $A_2(^2s, P)$ при $P = A_1(^1s)$ кратен $|S_1|$; $D_{\min}^{|S_2|} > |Y``|$, где $D_{\min}^{|S_2|}$ – минимальный делитель числа $|S_2|$, отличный от 1; $A_{\varphi, \Pi}$ – приведенный автомат. Тогда изопериод выходной последовательности автомата $A = A_1 \xrightarrow{\Phi} A_2$ равен $|S_1||S_2|$.

Рассмотрим частный случай последовательного соединения $A = A_1 \xrightarrow{\Phi} A_2$ автономного автомата $A_1 = (S_1, Y_1, h, \lambda)$ и автомата $A_2 = (X, S_2, (h_x)_{x \in X}, \varphi)$ с выходной функцией φ, $Y_1 = X$, в случае, когда $\Phi(^1s, ^2s) = \varphi(^2s)$.

Теорема 4. Пусть $A = A_1 \xrightarrow{\Phi} A_2$ – полноцикловый автомат; A_1 – полноцикловый, приведенный автомат; A_2 – коммутируемый автомат; период последовательности состояний $A_2(^2s, P)$ при $P = A_1(^1s)$ кратен $|S_1|$. Тогда, если W_σ – σ-изопериод выходной последовательности автомата A, причем $W_\sigma < |S_1||S_2|$, то выходная последовательность $A_{\varphi, \Pi}(^2s)$, $^2s \in S_2$, автомата $A_{\varphi, \Pi} = (S_2, Y, \Pi, \varphi)$ σ-изопериодична и ее σ-изопериод меньше $|S_2|$.

Доказательство. Пусть $W = W_\sigma$ – σ-изопериод выходной последовательности $A(^1s_1, ^2s_1)$ автомата A, а

$A_M(^1s_1, ^2s_1) = (^1s_1, ^2s_1), (^1s_2, ^2s_2), \ldots$ – соответствующая ей последовательность состояний автомата A.

Имеем

$$\phi(^2s_{j+W}) = \sigma\phi(^2s_j),\ j \in \{1, 2, \ldots\},$$

$$\phi(\Pi^p(^2s_{j+W})) = \sigma\phi(\Pi^p(^2s_j)),\ j \in \{1, 2, \ldots\},\ p \in \{0, 1, 2, \ldots\},.$$

Так как A_1 – приведенный автомат и период последовательности состояний $A_2(^2s, P)$ при $P = A_1(^1s)$ кратен $|S_1|$, то период последовательности $A_M(^1s_1, ^2s_1)$ равен $|S_1||S_2|$.

По условию, $W < |S_1||S_2|$, поэтому найдется j`, при котором $^2s_{j'} \neq {}^2s_{j'+W'}$ и

$$\phi(\Pi^p(^2s_{j`+W})) = \sigma\phi(\Pi^p(^2s_{j`})),\ p \in \{0, 1, 2, \ldots\}.$$

Из условий теоремы вытекает, что Π – полноцикловое преобразование, следовательно, найдется $m = m(j`)$, $1 < m < |S_2|$, при котором

$$^2s_{j`+W} = \Pi^m(^2s_{j`}).$$

Из предыдущих равенств получаем

$$\phi(\Pi^p\Pi^m(^2s_{j`})) = \sigma\phi(\Pi^p(^2s_{j`})),\ p \in \{0, 1, 2, \ldots\}.$$

Следовательно, σ-изопериод последовательности $A_{\varphi,\,\Pi}({}^2s_j)$, очевидно равный σ-изопериоду последовательности $A_{\varphi,\,\Pi}({}^2s_1)$, не превосходит m и поэтому меньше $|S_2|$. Теорема доказана.

Изложенные результаты позволяют строить автономное последовательное соединение n автоматов, $n \geq 2$, с гарантированными свойствами, указанными в предыдущих теоремах. Действительно, если заданы автономный автомат A_1 и коммутируемые автоматы A_2, ..., A_n, то можно построить сначала автомат $A = A_1 \xrightarrow{\Phi_1} A_2$ с выходной функцией Φ_1, определенной через функции F_1, ψ_1, φ_1, либо только φ_1; далее, беря в качестве исходного полноцикловый автомат A, можно построить автомат $A \xrightarrow{\Phi_2} A_3$, где функция Φ_2 определяется через соответствующие функции F_2, ψ_2, φ_2, либо только через φ_2 и так далее.

22.4. Изопериоды последовательного соединения автоматов с выходным алфавитом-группой

Рассмотрим еще один частный случай изучаемого последовательного соединения $A = A_1 \xrightarrow{\Phi} A_2$ автоматов A_1, A_2 с функцией

$$\Phi({}^1s, {}^2s) = F(\psi({}^1s), \phi({}^2s)),$$

когда Y` = Y`` = Y = G , где G – некоторая конечная группа и

$$F(\psi({}^1s), \phi({}^2s)) = \psi({}^1s) \cdot \phi({}^2s).$$

В этом случае наряду с изучением σ-изопериодичности выходной последовательности $A({}^1s, {}^2s)$ автомата A представляет интерес и изучение ее левых, правых, двухсторонних G-изопериодов (данные понятия введены в пункте 1).

Теорема 5. Пусть $A = A_1 \xrightarrow{\Phi} A_2$ – полноцикловый автомат, Y` = Y`` = Y = G, $|G| > 1$, $\Phi({}^1s, {}^2s) = \psi({}^1s) \cdot \phi({}^2s)$; A_1 – приведенный автомат; A_2 – коммутируемый автомат; период последовательности состояний $A_2({}^2s, P)$ при $P = A_1({}^1s)$ кратен $|S_1|$; левый (правый, двухсторонний) G-изопериод последовательности $A_{\varphi\,,\Pi}({}^2s)$ автомата $A_{\varphi,\,\Pi}$ равен $|S_2|$. Тогда левый (правый, двухсторонний) G-изопериод выходной последовательности автомата A равен $|S_1||S_2|$.

Доказательство этой теоремы проводится аналогично доказательству теоремы 3.

Теорема 6. Пусть $A = A_1 \xrightarrow{\Phi} A_2$ – полноцикловый автомат; A_2 – коммутируемый автомат; Y` = Y`` = Y = G, $|G| > 1$; $\Phi({}^1s, {}^2s) = \psi({}^1s) \cdot \phi({}^2s)$; левый G-изопериод выходной последовательности автономного автомата (S_1, h, Y`, ψ) равен $|S_1|$, а левый

G-изопериод выходной последовательности автомата $A_{\varphi,\,\Pi}(S_2, Y``, \Pi, \varphi)$ равен $|S_2|$. Тогда левый G-изопериод выходной последовательности автомата A равен $|S_1||S_2|$.

Доказательство. Пусть $W = W_g$ – левый g-изопериод выходной последовательности $A({}^1s_1, {}^2s_1)$ автомата A, а $({}^1s_1, {}^2s_1),({}^1s_2, {}^2s_2),\ldots$ – последовательность состояний автомата A, отвечающие его начальному состоянию $({}^1s_1, {}^2s_1)\in S_1\times S_2$.

Тогда

$$\psi({}^1s_{j+W})\phi({}^2s_{j+W}) = g\psi({}^1s_j)\phi({}^2s_j),\ j\in\{1, 2, \ldots\},$$

или

$$(\phi(\Pi^p({}^2s_{\kappa+W})) = (\psi({}^1s_{\kappa+W}))^{-1} g\psi({}^1s_\kappa)\phi(\Pi^p({}^2s_\kappa)),\ \kappa\in\{1, 2, \ldots\},\ p\in\{0, 1, \ldots\}.$$

Покажем, что $\tau({}^2s_1)\ |W$, где $\tau({}^2s_1)$ – период последовательности ${}^2s_1, {}^2s_2,\ldots$, то есть покажем, что

$${}^2s_{\kappa+W} = {}^2s_\kappa,\ \kappa\in\{1, 2, \ldots\}.$$

Из условий теоремы следует, что Π – полноцикловая подстановка, следовательно, для каждого $\kappa\in\{1, 2, \ldots\}$ найдется натуральное число $m = m(\kappa)$, $1 \le m \le |S_2|$, при котором

$${}^2s_\kappa = \Pi^m({}^2s_\kappa).$$

Положив

$$(\psi({}^1s_{\kappa+W}))^{-1} g\psi({}^1s_\kappa) = g_\kappa,$$

имеем

$$\phi(\Pi^p\Pi^m({}^2s_\kappa)) = g_\kappa\phi(\Pi^p({}^2s_\kappa)),\ \kappa\in\{1, 2, \ldots\},\ p\in\{0, 1, 2, \ldots\}.$$

По условию G-изопериод последовательности $(\phi({}^2s_\kappa),\phi(\Pi({}^2s_\kappa)),\ldots$ равен $|S_2|$. Поэтому

$$\Pi^m({}^2s_\kappa) = {}^2s_\kappa,\ g_\kappa = e,\ \kappa\in[1,2,\ldots),$$

где e – единица группы G. Таким образом,

$$\tau({}^2s_1)\ |W_g,$$

а последнее равенство дает

$$\psi({}^1s_{\kappa+W}) = g\psi({}^1s_\kappa).$$

Так как автомат A_1 – полноцикловый, то найдется натуральное число C, для которого

$${}^1s_{\kappa+W} = \delta^C({}^1s_\kappa),\ 1\le C\le|S_1|,\ \kappa\in\{1, 2, \ldots\}.$$

Имеем

$$\psi(\delta^C({}^1s_{\kappa+W})) = g\psi({}^1s_\kappa),\ \kappa\in\{1, 2, \ldots\}.$$

По условию теоремы, левый G-изопериод последовательности $\psi({}^1s_1),\psi({}^1s_2),\ldots$ равен $|S_1|$, следовательно, $C = |S_1|$, то есть

$$^1s_{\kappa+W_g} = {}^1s_\kappa,\ \kappa \in \{1, 2, ...\}.$$

Поэтому $|S_1|$ делит W_g. Итак, $\tau(^2s_1) \mid W_g$, $|S_1| \mid W_g$, следовательно,

$$HOK(|S_1|, \tau(^2s_1)) \mid W_g.$$

Величина $HOK(|S_1|, \tau(^2s_1))$ совпадает с $|S_1||S_2|$ в силу полноцикловости автомата A. Заключаем, что $W_g = |S_1||S_2|$, g = e, e – нейтральный элемент группы G. Теорема доказана.

Рассмотрим еще один частный случай последовательного соединения $A = A_1 \xrightarrow{\Phi} A_2$ автоматов A_1, A_2, когда

$$\Phi(^1s, {}^2s) = \varphi(^2s),\ Y`` = Y = G \neq e.$$

Теорема 7. Пусть $A = A_1 \xrightarrow{\Phi} A_2$ – полноцикловый автомат; $\Phi(^1s, {}^2s) = \varphi(^2s)$, $Y`` = Y = G \neq e$; A_1 – полноцикловый, приведенный автомат; A_2 – коммутируемый автомат; левый G-изопериод выходной последовательности $A_{\varphi, \Pi}(^2s)$ автомата $A_{\varphi, \Pi}$ равен $|S_2|$; период последовательности состояний $A_2(^2s, P)$, $P = A_1(^1s)$ автомата $A_2 = (X, S_2, (h_x)_{x \in X})$ равен $|S_1||S_2|$. Тогда левый G-изопериод выходной последовательности $A(^1s, {}^2s)$ автомата A равен $|S_1||S_2|$.

Доказательство теоремы проводится аналогично доказательству теоремы 4.

Замечание. Утверждение теоремы 7 остается справедливым при замене использованных в ее условии и утверждении левого G-изопериода на правый G-изопериод или на двухсторонний G-изопериод.

Глава 23. ОЦЕНКИ ПАРАМЕТРОВ ОБОБЩЕННОЙ ПЕРИОДИЧНОСТИ ВЫХОДНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ НЕКОТОРЫХ ПОЛНОЦИКЛОВЫХ АВТОМАТОВ С ВЫХОДНЫМ АЛФАВИТОМ, ЯВЛЯЮЩИМСЯ ГРУППОЙ

В данной главе вводятся понятия σ-периода последовательности элементов конечного алфавита и меры приближенного σ-периода. Доказываются оценки введенных параметров для выходных последовательностей некоторых полноцикловых автоматов с выходным алфавитом, являющимся группой.

23.1. Основные понятия, постановка задачи

Напомним необходимые нам основные обозначения:

$a \mid b$ – a делит b;

(a, b) – общий наибольший делитель a и b;

[a, b] – наименьшее общее кратное чисел a, b;

Пусть У – конечный алфавит, $|Y| \geq 2$, σ – бинарное отношение на множестве Y. Используем обозначение: yσy` – y находится в отношении σ с y`.

Определение 1. Последовательность Q = y(1), y(2), ..., y(j), ... элементов алфавита Y называется σ-периодической, если найдется натуральное число d, при котором для любого j

$$y(j)\sigma y(j+d). \qquad (25)$$

Любое такое число d называется σ-периодом последовательности Q.

Последовательность называется периодической, если она удовлетворяет определению 1 для бинарного отношения равенства элементов. Минимальное d в (25) называется ее периодом или минимальным периодом.

Пусть $Y_П$ – множество всех периодических последовательностей элементов алфавита Y. На множестве $Y_П$ можно задать метрику μ, положив для Q = y(1), y(2), ..., y(j), ... и Q` = y`(1), y`(2), ..., y`(j), ... из $Y_П$

$$\mu(Q, Q`) = \lim_{k\to\infty} \frac{1}{k} \rho_k(Q, Q`),$$

где $\rho_k(Q, Q`)$ – расстояние Хэмминга между начальными словами y(1), y(2), ..., y(k), y`(1), y`(2), ..., y`(k)) длины k последовательностей Q, Q`. Данный предел существует и он равен величине

$$\frac{1}{[\omega, \omega`]} \rho_{[\omega,\omega`]}(Q, Q`),$$

где ω, ω` – периоды, соответственно, последовательностей Q, Q`. Расстояние $\mu(Q, Q`)$ между периодическими последовательностями было использовано в [8] для определения меры приближенного периода d исследуемой периодической последовательности, именно за эту меру принималась величина

$$\mu(Q, d) = \min \mu(Q, Q`),$$

где min брался по всем периодическим последовательностям Q` периода d. В свою очередь, расстояние $\mu(Q, Q`)$ легко выводится из определения меры неотличимости инициальных автоматов (в частном случае их автономности), введенного в более ранней работе [10].

Обозначим через $Y(d, \sigma)$ подмножество всех σ-периодических последовательностей с σ-периодом d множества $Y_П$.

Определение 2. Для $Q \in Y_П$, натурального числа d, бинарного отношения σ на Y величина

$$\mu(Q, d, \sigma) = \inf\mu(Q, Q`),$$

где inf берется по всем Q` из $Y(d,\sigma)$, называется мерой приближенного σ-периода d периодической последовательности Q.

Анализируемую последовательность Q = y(1), y(2), ..., y(j), ... можно представить как последовательность к-грамм последовательности, то есть как последовательность элементов из $Y^к$. Такое представление дает дополнительные возможности исследования зависимости символов последовательности с помощью бинарных отношений на $Y^к$.

В [8] были указаны классы автоматов с гарантированной нижней оценкой меры приближенного периода последовательностей состояний при заданной входной периодической последовательности. В случае, когда бинарное отношение σ задано отображением, в [4; 37; 5; 12] приведены оценки снизу σ-периодов выходных последовательностей полноцикловых автоматов и автоматов, представимых в виде последовательного соединения полноциклового автомата с неавтономным автоматом. Естественным продолжением данных работ является получение нижних оценок σ-периодичности выходных последовательностей новых классов автоматов, а также оценок их мер приближенных σ-периодов.

Основные результаты данного раздела ранее сформулированы в параграфе 2 обзорной работы [12].

Пусть X – конечный алфавит, $|X| \geq 2$, $G = \langle (h_x)_{x\in X} \rangle$ – конечная группа (с операцией умножения), порожденная образующими $(h_x)_{x\in X}$. $P = h_{x(1)}, h_{x(2)}, ..., h_{x(j)}, ...$ – периодическая последовательность элементов семейства $(h_x)_{x\in X}$ периода ω. Ниже предполагается, что последовательность P содержит все элементы множества $\{h_x: x\in X\}$. Отметим, что мощность $|X|$ семейства $(h_x)_{x\in X}$ элементов G может не совпадать с мощностью $|\{ h_x: x\in X\}|$ множества $\{h_x: x\in X\}$.

Пусть L, H – натуральные числа, $L \geq 2$, $(\omega, L) = (\omega, H) = 1$. Введем автономный автомат $A = (S, G, \delta, f)$ с множеством состояний

$$S = \{P^1, P^2, ..., P^\omega\},$$

где $P^j = h_{x(j)}, h_{x(j+1)}, ...$ для $j\in\{1, 2, ...\}$, в частности, $P^1 = P$, выходным алфавитом G, функцией перехода $\delta: S\to S$, $\delta(P^j) = P^{j+1}$, $j\in\{1, ..., \omega–1\}$, $\delta(P^\omega) = P^1$, функцией выхода $f: S\to G$, $f(P^j) = h_{x(j+L–1)} \cdot ... \cdot h_{x(j+1)} \cdot h_{x(j)}$. Выходная последовательность $A(P^1)$ автомата A, отвечающая его начальному состоянию P^1 имеет вид

$$A(P^1) = y(1), y(2), ..., y(j), ...,$$

где $y(j) = f(P^j) = h_{x(j+L–1)} \cdot ... \cdot h_{x(j+1)} \cdot h_{x(j)}$.

Через A^H обозначим H-тую степень автомата A:

$$A^H = (S, G, \delta^H, f).$$

Тогда выходная последовательность $A^H(P^1)$ автомата A^H, отвечающая начальному состоянию $P^1\in S$, имеет вид

$$A^H(P^1) = y(1), y(1+H), ..., y(1+jH), ...$$

Решаемая задача состоит в расчете возможных значений σ-периодов выходной последовательности $A^H(P^1)$ автомата A^H, оценки снизу значений мер приближенных σ-периодов для приводимых ниже двух классов бинарных отношений на группе G.

1. Класс стабильных слева (справа) бинарных отношений на конечной группе $G = \langle (h_x)_{x\in X} \rangle$. Напомним, что бинарное отношение $\theta_л$ ($\theta_п$) на G называется стабильным слева (справа), если из отношений

$$g_1\theta_л g_2, (g_1\theta_п g_2), g_1, g_2\in G$$

следует

$$gg_1\theta_л gg_2, (g_1g\theta_л g_2g)$$

для любого $g\in G$.

Стабильное слева и справа бинарное отношение θ на G называется стабильным.

2. Класс автоморфизмов группы G.

23.2. σ-периоды последовательности $A^H(P^1)$ для стабильных слева (справа) бинарных отношений на G

Для стабильного слева бинарного отношение $\theta_л$ на G определим вспомогательное бинарное отношение $\hat{}\theta_л$ на множестве $\{h_x: x\in X\}$, соответствующему набору $(h_x)_{x\in X}$ образующих группы G. Положим $h_x\hat{}\theta_л h_{x`}$ тогда и только тогда, если существуют $g, g`\in G$, при которых

$$g\theta_л\, g`,\ gh_x\theta_л g`h_{x`}.$$

Аналогично определяется вспомогательное бинарное отношение $\hat{}\theta_п$ на множестве $\{h_x: x\in X\}$ для стабильного справа бинарного отношения $\theta_п$ на G: $h_x\hat{}\theta_п h_{x`}$ тогда и только тогда, если существуют $g,g`\in G$, при которых

$$g\theta_п\, g`,\ h_x g\theta_л h_{x`}g`.$$

Определение 3. Периодическая последовательность $P = h_{x(1)}, h_{x(2)}, ..., h_{x(j)}, ...$ элементов семейства $(h_x)_{x\in X}$ периода ω называется антипериодической последовательностью с антипериодом C, если $h_{x(j)} \neq h_{x(j+C)}$ при любом j. Если, дополнительно, $C \mid \omega$ и $h_{x(j)} \neq h_{x(j+kC)}$ при любом $k\in\{1, 2, ..., \frac{\omega}{C}-1\}$, то P называется антипериодической с полным антипериодом C.

Теорема 1. Пусть θ – стабильное слева (справа) бинарное отношение на группе $G = \langle(h_x)_{x\in X}\rangle$, а $\hat{}\theta$ – вспомогательное бинарное отношение на $\{h_x: x\in X\}$, соответствующее θ; $L \geq 2$, $(\omega, L) = (\omega, H) = 1$; W – θ-период последовательности $A^H(P^1)$; различные образующие элементы группы G не находятся в бинарном отношении $\hat{}\theta$; периодическая последовательность $P = h_{x(1)}, h_{x(2)}, ..., h_{x(j)}, ...$ элементов семейства $(h_x)_{x\in X}$ периода ω не является антипериодической с антипериодом WH. Тогда $\omega \mid W$. Если W – минимальный θ-период последовательности $A^H(P^1)$, то $W = \omega$.

Доказательство. Так как W – θ-период последовательности $A^H(P^1) = y(1), y(1+H), ..., y(1+jH), ...$, то для $j\in\{0, 1, ...\}$

$$y(1+jH)\ \theta\ y(1+(j+W)H).$$

Из того, что $(H, \omega) = 1$, найдутся натуральные числа к(1), к(2), при которых для любого $c\in\{0, 1, ...\}$

$$ск(1)H - ск(2)\omega = c \qquad (26)$$

и из предыдущих отношений получаем

$$y(1+ск(1)H)\ \theta\ y(1+ск(1)H+WH),$$
$$y(1+(c+1)к(1)H)\ \theta\ y(1+(c+1)к(1)H+WH).$$

Учитывая, что $y(j) = h_{x(j+L-1)}\cdot \ldots \cdot h_{x(j+1)}\cdot h_{x(j)}$, $j\in\{1, 2, \ldots\}$, ω – период последовательности P^1 и (2), имеем для $c\in\{1, 2, \ldots\}$

$$h_{x(c+L-1)}\cdot\ldots\cdot h_{x(c+1)}\cdot h_{x(c)}\ \theta\ h_{x(c+L-1+WH)}\cdot\ldots\cdot h_{x(c+1+WH)}\cdot h_{x(c+WH)},$$
$$h_{x(c+L)}\cdot\ldots\cdot h_{x(c+1)}\ \theta\ h_{x(c+L+WH)}\cdot\ldots\cdot h_{x(c+1+WH)}, \qquad (27)$$

или

$$g_1 h_{x(c)}\ \theta\ g_2 h_{x(c+WH)}, \qquad (28)$$
$$h_{x(c+L)}g_1\ \theta\ h_{x(c+L+WH)}g_2,$$

где

$$g_1 = h_{x(c+L-1)}\cdot\ldots\cdot h_{x(c+1)}$$
$$g_2 = h_{x(c+L-1+WH)}\cdot\ldots\cdot h_{x(c+1+WH)}.$$

Сначала рассмотрим случай $\theta = \theta_л$. Так как WH не является антипериодом последовательности P, то существует $c`\in\{1, 2, \ldots\}$, при котором $h_{x(c`+L)} = h_{x(c`+L+WH)}$. Поэтому из (28) получаем $h_{x(c`)}\wedge\theta_л h_{x(c`+WH)}$. Следовательно, $h_{x(c`)} = h_{x(c`+WH)}$. Повторяя предыдущий шаг рассуждений и, используя условия $(\omega, L) = (\omega, H) = 1$, получаем

$$h_{x(j)} = h_{x(j+WH)}, \qquad j\in\{1, 2, \ldots\}.$$

Таким образом, $\omega \mid W$.

Если W – минимальный $\theta_л$-период последовательности $A^H(P^1)$, то он не превосходит периода последовательности $A^H(P^1)$, который, очевидно, является делителем ω. Значит, в этом случае, $W=\omega$.

Рассмотрим случай $\theta = \theta_п$. Если при некотором $c`\in\{1, 2, \ldots\}$

$$h_{x(c`)} = h_{x(c`+WH)},$$

то из (28) следует

$$h_{x(c`+L)}\wedge\theta_п h_{x(c`+L+WH)}.$$

Аналогично рассмотренному выше случаю получаем требуемое утверждение.

Замечание 1. Заметим, что полученные при доказательстве теоремы 1 отношения

$$h_{x(c+L-1)}\cdot\ldots\cdot h_{x(c+1)}\cdot h_{x(c)}\ \theta\ h_{x(c+L-1+WH)}\cdot\ldots\cdot h_{x(c+1+WH)}\cdot h_{x(c+WH)},$$
$$h_{x(c+L)}\cdot\ldots\cdot h_{x(c+1)}\ \theta\ h_{x(c+L+WH)}\cdot\ldots\cdot h_{x(c+1+WH)},$$

могут быть записаны в виде

$$y_c \theta y_{c+WH},$$
$$y_{c+1}\theta y_{c+1+WH}.$$

Пусть для некоторых фиксированных произвольных натуральных чисел c, W, H выполняются данные отношения и различные образующие группы G не находятся в отношении $\hat{}\theta$.

При $\theta = \theta_л$ и них вытекает следующее. Если $h_{x(c+L)} = h_{x(c+L+WH)}$, то $h_{x(c)} = h_{x(c+WH)}$.

При $\theta = \theta_п$, если $h_{x(c)} = h_{x(c+WH)}$, то $h_{x(c+L)} = h_{x(c+L+WH)}$.

Если θ стабильное одновременно слева и справа бинарное отношение, то $h_{x(c)} = h_{x(c+WH)}$ тогда и только тогда, если $h_{x(c+L)} = h_{x(c+L+WH)}$.

Заметим, что для стабильного слева (справа) бинарного отношения θ бинарное отношение θ^k (k-я степень θ) также стабильно слева справа). Через $\hat{}\theta^k$ обозначим вспомогательное бинарное отношение на $\{h_x: x \in X\}$, соответствующее θ^k.

Теорема 2. Пусть θ – стабильное слева (справа бинарное отношение на группе G; W – минимальный θ-период последовательности $A^H(P^1)$; $(\omega, L) = (\omega, H) = 1$, $L \geq 2$; при каждом $j \in \{1, ..., |\{h_x: x \in X\}| - 1\}$ различные образующие элементы группы G не находятся в отношении $\hat{}\theta^j$. ω – период последовательности $P = h_{x(1)}, h_{x(2)}, ..., h_{x(j)}, ...$ Если W не равен ω, то

1) последовательность P антипериодическая с антипериодами jWH, $j \in \{1, ..., K\}$, где K – минимальное натуральное число, при котором $\omega | KW$;

2) $K \leq |\{h_x: x \in X\}|$, W кратен величине вида $\frac{\omega}{d}$, где $d | K$;

3) если, дополнительно, $W | \omega$, то $W = \frac{\omega}{K}$, и последовательность P является антипериодической с полным антипериодом W.

Доказательство. Так как W – минимальный θ-период периодической последовательности $A^H(P^1)$, то W не превосходит периода этой последовательности, который, в свою очередь, является делителем величины ω. Следовательно, $W \leq \omega$. Пусть $W \neq \omega$. По теореме 1 последовательность P антипериодическая с аньтипериодом WH. Для любого $j \in \{1, ..., K-1\}$ последовательность $A^H(P^1)$ является θ^j-периодической с θ^j-периодом, равным jW. По теореме 1 получаем, что последовательность P имеет антипериод jWH для каждого $j \in \{1, ..., \min(|\{h_x: x \in X\}| - 1, K-1)$. Рассмотрим два случая:

1) $|\{h_x: x \in X\}| - 1 < K - 1$;

2) $\min(|\{h_x: x \in X\}| - 1, K-1) = K - 1$.

Покажем, что первый случай невозможен. Действительно, в этом случае очевидно, что $\omega \mid WH|\{h_x: x\in X\}|$. Следовательно, $\omega \mid W|\{h_x: x\in X\}|$. Из определения величины К получаем противоречие с 1): $К \le |\{h_x: x\in X\}|$. Таким образом, выполняется случай 2). Следовательно, $К \le |\{h_x: x\in X\}|$. Так как $\omega \mid KW$, то W имеет вид:

$$W = \frac{C\omega}{K},$$

где С – некоторое натуральное число, $С < К$. Откуда вытекают утверждения 1), 2) теоремы. При дополнительном условии $W \mid \omega$ положим $\omega = NW$, $N \ge 2$. Тогда $N = К$. Последовательность Р антипериодическая с антипериодами jWH, $j\in\{1, ..., N–1\}$. Для любого $k\in\{1, 2, ...\}$ все элементы $h_{x(k)}$, $hx_{(k+WH)}$, ..., $h_{x(k+(N–1)WH)}$ различны. Учитывая, что $(H, \omega) = 1$, $NW = \omega$, получаем утверждение 3.

23.3. Оценки мер приближенных σ-периодов последовательности $A^H(P^1)$ для стабильных слева (справа) бинарных отношений на группе G

Здесь, как и ранее мы рассматриваем класс стабильных слева (справа) бинарных отношений θ на конечной группе $G = <(h_x)_{x\in X}>$.

Определим вспомогательные отображения множества X^4 в $\{0, 1\}$:

1) $\gamma: X^4 \to \{0, 1\}$, $\gamma(z(1), z(2), z(3), z(4)) = 1$ тогда и только тогда, когда

$$z(1) = z(2), z(3) \ne z(4)$$

или

$$z(1) \ne z(2), z(3) = z(4);$$

2) $\gamma_п: X^4 \to \{0, 1\}$, $\gamma_п(z(1), z(2), z(3), z(4)) = 1$ тогда и только тогда, когда

$$z(1) = z(2), z(3) \ne z(4);$$

3) $\gamma_л: X^4 \to \{0, 1\}$, $\gamma_л(z(1),z(2), z(3), z(4)) = 1$ тогда и только тогда, когда

$$z(1) \ne z(2), z(3) = z(4).$$

Для фиксированной периодической последовательности $\Im(d)= \Im^1 = x(1), x(2), ...$ периода d элементов алфавита X и натуральных чисел L, W, H для $j\in\{1, 2, ...\}$ положим

$$\Im^j = x(j), x(j+1), ...$$

$$\Phi_{HW, L}(\Im^j) = \gamma(x(j), x(j+HW), x(j+L), x(j+HW+L)),$$

$$||\Phi_{HW,\,L}(\mathfrak{I}(d)|| = \sum_{j=1}^{d} \Phi_{HW,L}(\mathfrak{I}^j)$$

Аналогично определим величины $\Phi_{л,\ HW,\ L}(\mathfrak{I}^j)$, $||\ \Phi_{л,\ HW,\ L}(\mathfrak{I}(d)||$, заменив функцию γ на $\gamma_л$. Определим и $\Phi_{п,\ HW,\ L}(\mathfrak{I}^j)$, $||\ \Phi_{п,\ HW,\ L}(\mathfrak{I}(d)||$, заменив γ на $\gamma_п$.

Теорема 3. Пусть $|\{h_x: x\in X\}| = |X|$; θ – стабильное слева (справа) бинарное отношение на группе $G = \langle(h_x)_{x\in X}\rangle$, а $\hat{}\theta$ – бинарное отношение на $\{h_x: x\in X\}$, соответствующее θ; $\mu(A^H(P^1), W, \theta)$ – мера приближенного θ-периода W-последовательности $A^H(P^1)$; $(\omega, L) = (\omega, H) = 1$, $L \geq 2$; различные образующие элементы группы G не находятся в отношении $\hat{}\theta$. $\mathfrak{I} = x(1), x(2), ..., x(j), ...$ – вспомогательная последовательность для периодической последовательности $P=h_{x(1)}, h_{x(2)}, ..., h_{x(j)}, ...$ элементов семейства $(h_x)_{x\in X}$ периода ω. Тогда

1) $\mu(A^H(P^1), W, \theta) \geq \frac{1}{4\omega}\ ||\ \Phi_{HW,L}(\mathfrak{I})||$,

если θ – стабильное одновременно слева и справа бинарное отношение на G;

2) $\mu(A^H(P^1), W, \theta) \geq \frac{1}{4\omega}\ ||\Phi_{п,HW,L}(\mathfrak{I})||$,

если $\theta = \theta_п$;

3) $\mu(A^H(P^1), W, \theta) \geq \frac{1}{4\omega}\ ||\Phi_{л,HW,L}(\mathfrak{I})||$,

если $\theta = \theta_л$.

Доказательство. Напомним, что $A^H(P^1)$ имеет вид

$$A^H(P^1) = y(1), y(1+H), ..., y(1+jH),...$$

где $A(P^1) = Q = y(1), y(2), ..., y(j), ...$ – последовательность элементов из G вида

$$y(j) = h_{x(j+L-1)}\cdot...\cdot h_{x(j+1)}\cdot h_{x(j)},\ j\in\{1, 2, ...\}.$$

Пусть $\overline{Q} = \overline{y(1)}, \overline{y(2)}, ...$ – периодическая последовательность элементов группы G с θ-периодом W, для которой

$$\mu(A^H(P^1), \overline{Q}) - \mu(A^H(P^1),W,\theta) \leq \varepsilon,$$

где $\varepsilon > 0$.

Рассмотрим случай $\theta = \theta_п$. Введем две вспомогательные последовательности $(A^H(P^1), (A^H(P^1))^{1+W})$, $(\overline{Q}, \overline{Q}^{1+W})$ пар элементов:

$$(A^H(P^1), (A^H(P^1))^{1+W}) = (y(1), y(1+WH)), (y(1+H), y(1+H+WH)), ...;$$

$$(\overline{Q}, \overline{Q}^{1+W}) = (\overline{y(1)}, \overline{y(1+W)}, (\overline{y(2)}, \overline{y(2+W)}, ...$$

и последовательности $A^H(P^1)\bullet((A^H(P^1))^{1+W}))^{-1}$, $\overline{Q}\bullet(\overline{Q}^{1+W})^{-1}$ элементов из G

$$A^H(P^1)\bullet((A^H(P^1))^{1+W}))^{-1} = y(1)\cdot(y(1+WH))^{-1}, y(1+H)\cdot(y(1+H+WH))^{-1}, ...,$$
$$\overline{Q}\bullet(\overline{Q}^{1+W})^{-1} = \overline{y(1)}\cdot(\overline{y(1+W)})^{-1}, \overline{y(2)}\cdot(\overline{y(2+W)})^{-1}, ...$$

Ниже мы будем пользоваться рядом очевидных свойств функции μ на множестве всех периодических последовательностей элементов из G, в частности тем, что на этом множестве μ является метрикой.

Имеем

$$2\mu(A^H(P^1); \overline{Q}) \geq \mu((A^H(P^1), (A^H(P^1))^{1+W}); (\overline{Q}, \overline{Q}^{1+W})),$$

так как

$$\mu(A^H(P^1); \overline{Q}) = \mu((A^H(P^1))^{1+W}; \overline{Q}^{1+W}).$$

Ясно, что

$$\mu((A^H(P^1), (A^H(P^1))^{1+W}); (\overline{Q}, \overline{Q}^{1+W}))\geq$$
$$\mu(A^H(P^1)\bullet((A^H(P^1))^{1+W}))^{-1}, \overline{Q}\bullet(\overline{Q}^{1+W})^{-1}.$$

В силу выбора $\overline{Q}$, при любом j элемент $\overline{y(j)}\cdot(\overline{y(j+W)})^{-1}$ принадлежит $\theta_п^{-1}(e)$ – образу единицы e группы G бинарного отношения $\theta_п^{-1}$.

Введем на множестве элементов группы G бинарное отношение эквивалентности с помощью следующего разбиения множества G: первое подмножество есть множество $\theta_п^{-1}(e)$, остальные множества одноэлементные. Через [y] будем обозначать класс эквивалентности, содержащий элемент y из G. Рассмотрим последовательности:

$$[A^H(P^1)\bullet((A^H(P^1))^{1+W}))^{-1}]=$$
$$= [y(1)\cdot(y(1+WH))^{-1}], [y(1+H)\cdot(y(1+H+WH))^{-1}], ...,$$
$$[\overline{Q}\bullet(\overline{Q}^{1+W})^{-1}] = [\overline{y(1)}\cdot(\overline{y(1+W)})^{-1}], [\overline{y(2)}\cdot(\overline{y(2+W)})^{-1}], ... =$$
$$= [e], [e], \ldots,$$
$$A^H(P^1) = Q = y(1), y(2), ..., y(j), ...,$$
$$Q^{1+WH} = y(1+WH), y(1+WH+1), y(1+WH+2), ...,$$
$$Q\bullet(Q^{1+WH})^{-1} = y(1)\cdot(y(1+WH))^{-1}, y(2)\cdot(y(2+WH))^{-1}, ...,$$
$$[Q\bullet(Q^{1+WH})^{-1}] = [y(1)\cdot(y(1+WH))^{-1}], [y(2)\cdot(y(2+WH))^{-1}], ...$$

Очевидно, что

$$\mu(A^H(P^1)\bullet((A^H(P^1))^{1+W}))^{-1}; \overline{Q}\bullet(\overline{Q}^{1+W})^{-1}) \geq$$
$$\geq \mu([A^H(P^1)\bullet((A^H(P^1))^{1+W}))^{-1}]; [\overline{Q}\bullet(\overline{Q}^{1+W})^{-1}]) .$$

Учитывая, что периоды последовательностей Q, $Q\bullet(Q^{1+WH})^{-1}$ являются делителями величины ω, период последовательности $[\overline{Q}\bullet(\overline{Q}^{1+W})^{-1}]$ равен единице, последовательность $[A^H(P^1)\bullet((A^H(P^1))^{1+W}))^{-1}]$ является выборкой шага H из последовательности $[Q\bullet(Q^{1+WH})^{-1}]$ и условие (H, ω) = 1, несложно получить

$$\mu([Q\bullet(Q^{1+WH})^{-1}]; [\overline{Q}\bullet(\overline{Q}^{1+W})^{-1}]) =$$
$$= \mu([A^H(P^1)\bullet((A^H(P^1))^{1+W}))^{-1}]; [\overline{Q}\bullet(\overline{Q}^{1+W})^{-1}]).$$

Для последовательностей пар классов эквивалентности

$$([Q\bullet(Q^{1+WH})^{-1}], [Q^2\bullet(Q^{2+WH})^{-1}]) =$$
$$= ([y(1)\cdot(y(1+WH))^{-1}], [y(2)\cdot(y(2+WH))^{-1}]),... ,$$
$$([\overline{Q}\bullet(\overline{Q}^{1+W})^{-1}], [\overline{Q}\bullet(\overline{Q}^{1+W})^{-1}]) = ([e], [e]), ([e], [e]), ...$$

имеем

$$\mu(([Q\bullet(Q^{1+WH})^{-1}], [Q^2\bullet(Q^{2+WH})^{-1}]); ([\overline{Q}\bullet(\overline{Q}^{1+W})^{-1}], [\overline{Q}\bullet(\overline{Q}^{1+W})^{-1}])) \le$$
$$\le 2\mu([Q\bullet(Q^{1+WH})^{-1}]; [\overline{Q}\bullet(\overline{Q}^{1+W})^{-1}]).$$

Первую величину представим в виде

$$\mu(([Q\bullet(Q^{1+WH})^{-1}], [Q^2\bullet(Q^{2+WH})^{-1}]); ([\overline{Q}\bullet(\overline{Q}^{1+W})^{-1}], [\overline{Q}\bullet(\overline{Q}^{1+W})^{-1}])) =$$
$$= \frac{1}{\omega}\rho_\omega(([Q\bullet(Q^{1+WH})^{-1}], [Q^2\bullet(Q^{2+WH})^{-1}]); ([\overline{Q}\bullet(\overline{Q}^{1+W})^{-1}], [\overline{Q}\bullet(\overline{Q}^{1+W})^{-1}])).$$

Величина, представленная в числителе данного выражения, равна числу таких $c\in\{1, ..., \omega\}$, для которых одновременно не выполняются условия

$$y(c)\theta_\pi y(c+WH),$$
$$y(c+1)\theta_\pi y(c+1+WH).$$

Используя замечание 1, условие $|\{H_x: x\in X\}| = |X|$, заключаем, что число таких $c\in\{1, ..., \omega\}$ не меньше величины $\|\Phi_{\pi,HW,L}(\Im)\|$.

В итоге мы получили:

$$\mu(A^H(P^1); \overline{Q}) - \varepsilon \le \mu(A^H(P^1); W,\theta_\pi),$$
$$\mu(A^H(P^1); \overline{Q}) \ge \frac{1}{2}\mu((A^H(P^1), (A^H(P^1))^{1+W}); (\overline{Q}, \overline{Q}^{1+W})) \ge$$
$$\frac{1}{2}\mu(A^H(P^1)\bullet((A^H(P^1))^{1+W}))^{-1}; \overline{Q}\bullet(\overline{Q}^{1+W})^{-1}) \ge$$
$$\frac{1}{2}\mu([A^H(P^1)\bullet((A^H(P^1))^{1+W}))^{-1}]; [\overline{Q}\bullet(\overline{Q}^{1+W})^{-1}]) \ge$$
$$\frac{1}{2}\mu([Q\bullet(Q^{1+WH})^{-1}]; [\overline{Q}\bullet(\overline{Q}^{1+W})^{-1}]) \ge$$
$$\frac{1}{4}\mu([Q\bullet(Q^{1+WH})^{-1}], [Q^2\bullet(Q^{2+WH})^{-1}]; [\overline{Q}\bullet(\overline{Q}^{1+W})^{-1}], [\overline{Q}\bullet(\overline{Q}^{1+W})^{-1}] =$$
$$= \frac{1}{4\omega}\rho_\omega([Q\bullet(Q^{1+WH})^{-1}], [Q^2\bullet(Q^{2+WH})^{-1}]; [\overline{Q}\bullet(\overline{Q}^{1+W})^{-1}], [\overline{Q}\bullet(\overline{Q}^{1+W})^{-1}]) \ge$$
$$\ge \frac{1}{4\omega}\|\Phi_{\pi, HW, L}(\Im)\|;$$

Итак,

$$\mu(A^H(P^1); W,\theta_\pi) \ge \mu(A^H(P^1); \overline{Q}) - \varepsilon \ge \frac{1}{4\omega}\|\Phi_{\pi, HW, L}(\Im)\| - \varepsilon.$$

Утверждение пункта 2) теоремы 3 доказано, так как ε – произвольное положительное число.

Полностью аналогично доказываются утверждения пунктов 1) и 3) теоремы 3.

Теорема 4. Пусть $|\{h_x: x\in X\}| = |X|$; последовательность $P = h_{x(1)}, h_{x(2)}, ..., h_{x(j)}, ...$ элементов семейства $(h_x)_{x\in X}$ выбирается случайно и равновероятно из множества периодических последовательностей элементов алфавита $\{h_x: x\in X\}$ периода ω, $\omega \geq 3$.

θ – стабильное слева (справа) бинарное отношение на группе $G = <(h_x)_{x\in X}>$, а ^θ – бинарное отношение на $\{h_x: x\in X\}$, соответствующее θ; $E\mu(A^H(P^1), W, \theta)$ – мера приближенного θ-периода W-последовательности $A^H(P^1)$; $(\omega, L) = (\omega, H) = 1$, $2 \leq L < \omega$, $1 \leq W < \omega$; различные образующие элементы группы G не находятся в отношении ^θ. Тогда выполняются оценки:

1) $$E\mu(A^H(P^1), W, \theta) \geq \frac{(|X|-1)\sum\limits_{d|\omega, d\notin\Theta} \bar{\mu}\left(\frac{\omega}{d}\right)|X|^{d-2}}{2\sum\limits_{d|\omega} \bar{\mu}\left(\frac{\omega}{d}\right)|X|^{d}},$$

если θ – стабильное одновременно слева и справа бинарное отношение на G. Здесь Θ – множество следующих натуральных чисел

$$\Theta = \{1, 2\}\cup\{n: n|HW\}\cup\{n: n| L\}\cup\{n: L \equiv HW \bmod(n), L+HW \equiv 0 \bmod(n)\},$$

$\bar{\mu}$ – функция Мебиуса.

2) $$E\mu(A^H(P^1), W, \theta) \geq \frac{(|X|-1)\sum\limits_{d|\omega, d\notin\Theta} \bar{\mu}\left(\frac{\omega}{d}\right)|X|^{d-2}}{4\sum\limits_{d|\omega} \bar{\mu}\left(\frac{\omega}{d}\right)|X|^{d}},$$

если $\theta = \theta_п$, или $\theta = \theta_л$.

Доказательство. Пусть D(d) – все различные делители числа d; M_d – множество всех периодических последовательностей элементов алфавита X периода d. Положим

$$M_{D(d)} = \bigcup_{d`\in D(d)} M_{d`}.$$

Справедливость утверждений сформулированной теоремы непосредственно следует из утверждения теоремы 3 и утверждения следующей леммы.

Лемма 1. Пусть $\omega \geq 3$, $2 \leq L < \omega$, $(L, \omega) = (H, \omega) = 1$, $1 \leq W < \omega$. Тогда

1) средние значения

$$\frac{1}{|M_\omega|}\sum_{\Im\in M_\omega}\ ||\Phi_{HW,\,L}(\Im)||,$$

$$\frac{1}{|M_\omega|}\sum_{\Im\in M_\omega}\ ||\Phi_{п,HW,L}(\Im)||,\quad \frac{1}{|M_\omega|}\sum_{\Im\in M_\omega}\ ||\Phi_{л,HW,L}(\Im)||$$

весов $||\Phi_{HW,\,L}(\Im)||$, $||\Phi_{п,\,HW,\,L}(\Im)||$, $||\Phi_{л,\,HW,\,L}(\Im)||$ функций $\Phi_{HW,\,L}(\Im)$, $\Phi_{п,\,HW,\,L}(\Im)$, $\Phi_{л,\,HW,\,L}(\Im)$, построенных для вспомогательной последовательности $\Im$ = x(1), x(2), ..., x(j), ..., при случайно и равновероятно выбранной последовательности $\Im$ из M_ω равны величинам

$$E_\omega||\Phi_{HW,L}(\Im)|| = \frac{2\omega(|X|-1)\sum\limits_{d|\omega,\,d\notin\Theta}\bar{\mu}\left(\frac{\omega}{d}\right)|X|^{d-2}}{\sum\limits_{d|\omega}\bar{\mu}\left(\frac{\omega}{d}\right)|X|^{d}},$$

$$E_\omega||\Phi_{п,\,HW,\,L}(\Im)|| = E||\Phi_{л,\,HW,\,L}(\Im)|| = \frac{\omega(|X|-1)\sum\limits_{d|\omega,\,d\notin\Theta}\bar{\mu}\left(\frac{\omega}{d}\right)|X|^{d-2}}{\sum\limits_{d|\omega}\bar{\mu}\left(\frac{\omega}{d}\right)|X|^{d}},$$

где $\bar{\mu}$ – функция Мебиуса,

Θ = {1, 2}∪{n: n|HW}∪{n: n| L}∪{n:L ≡ HW mod(n), L+HW ≡ 0 mod(n)};

2) $E_{D(\omega)}||\Phi_{HW,L}(\Im)|| = \frac{1}{|M_{D(\omega)}|}\sum\limits_{\Im\in M_{D(\omega)}}||\Phi_{HW,L}(\Im)|| = \frac{2\omega(|X|-1)}{|X|^2}$,

$E_{D(\omega)}||\Phi_{п,\,HW,\,L}(\Im)|| = \frac{1}{|M_{D(\omega)}|}\sum\limits_{\Im\in M_{D(\omega)}}||\Phi_{HW,\,L}(\Im)|| = \frac{\omega(|X|-1)}{|X|^2}$,

$E_{D(\omega)}||\Phi_{л,\,HW,\,L}(\Im)|| = \frac{1}{|M_{D(\omega)}|}\sum\limits_{\Im\in M_{D(\omega)}}||\Phi_{HW,\,L}(\Im)|| = \frac{\omega(|X|-1)}{|X|^2}$.

Доказательство. Проведем доказательство утверждения леммы для параметра $||\Phi_{п,\,HW,\,L}(\Im)||$ функции $\Phi_{п,\,HW,\,L}(\Im)$. Для параметров $|\Phi_{HW,\,L}(\Im)||$, $||\Phi_{л,\,HW,\,L}(\Im)||$ доказательство проводится аналогично.

Ясно, что

$$|M_\omega| = \sum_{d|\omega}\bar{\mu}(d)\,|X|^{\frac{\omega}{d}},$$

где $\bar{\mu}$ – функция Мебиуса.

Для функции $\Phi = \Phi_{п,\,HW,\,L}$ имеем

$$\sum_{\Im\in M_{D(\omega)}}||\Phi(\Im)||=\sum_{j=1}^{\omega}\sum_{\Im\in M_{D(\omega)}}\gamma_n\,(x(j),\,x(j+HW),\,x(j+L),\,x(j+HW+L).$$

В случае, когда все элементы 0, HW, L, HW+L различны по модулю ω, полученное выражение можно преобразовать так:

$$\sum_{\Im\in M_{D(\omega)}}||\Phi(\Im)||=\sum_{j=1}^{\omega}|X|^{\omega-4}\sum\gamma_n\,(x(j),\,x(j+HW),\,x(j+L),\,x(j+HW+L)),$$

где вторая сумма берется по всем (x(j), x(j+HW), x(j+L), x(j+HW+L))$\in X^4$. Последнее выражение равно величине

$$\omega|X|^{\omega-4}|X|^2(|X|-1) = \omega|X|^{\omega-2}(|X|-1).$$

При указанных в постановке задачи ограничениях элементы 0, HW, L, HW+L не все различны по модулю ω, лишь в случае 1) среди величин 0, HW, L, HW+L три различных числа по модулю ω и HW+L $\equiv$ 0 mod(ω) либо HW $\equiv$ L mod(ω).

Заметим, что случай: L $\equiv$ HW mod(ω), HW+L $\equiv$ 0 mod(ω) невозможен, так как в этом случае несложно получить ω = 2. Исключение остальных возможных вариантов, когда 0, HW, L, HW+L не все различны по модулю ω, проводится элементарно.

Для случая 1) имеем

$$\sum_{\Im\in M_{D(\omega)}} ||\Phi(\Im)|| = \sum_{j=1}^{\omega} |X|^{\omega-3}|X|(|X|-1),$$

и это выражение совпадает с полученным ранее выражением. Следовательно,

$$\sum_{\Im\in M_{D(\omega)}} ||\Phi(\Im)|| = \frac{\omega|X|^{\omega-2}(|X|-1)}{|X|^{\omega}} = \frac{\omega(|X|-1)}{|X|^2}.$$

Перейдем к подсчету величины $E_\omega||\Phi||$. Для n$\in${1, 2, ...} рассмотрим две функции:

$$g_{\omega, HW, L}(n) = \sum_{\Im(n)\in M_n} ||\Phi(\Im(n)|| ;$$

и $f_{\omega, HW, L}(n) = 0$ в случае n$\in\Theta$,

$f_{\omega, HW, L}(n) = \omega|X|^{n-2}(|X|-1)$ в случае n$\notin\Theta$.

Покажем, что выполняется следующее основное равенство

$$\sum_{d|n} g_{\omega, HW, L}(d) = f_{\omega, HW, L}(n), \quad n\in\{1, 2, ...\}.$$

Действительно,

$$\sum_{d|n} g_{\omega, HW, L}(d) = \sum_{\Im\in D(n)} ||\Phi(\Im)|| =$$

$$\sum_{j=1}^{\omega}\sum_{\Im\in M_{D(n)}} \gamma_n(x(j), x(j+HW), x(j+L), x(j+HW+L).$$

Очевидно, в трех случаях: n = 1; n| HW; n| L, получаем

$$\gamma_n(x(j), x(j+HW), x(j+L), x(j+HW+L) = 0.$$

В двух случаях:

n = 2, 2 не делит HW, 2 не делит L;

{n: L $\equiv$ HW mod(n), L+HW $\equiv$ 0 mod(n)},

получаем

$$x(j) = x(j+HW+L), x(j+L) = x(j+HW).$$

Таким образом, для $n \in \Theta$

$$\sum_{d|n} g_{\omega,HW,L}(d)=0.$$

Для $n \notin \Theta$ возможны лишь следующие случаи:

1) числа 0, HW, L, HW+L все различны по модулю n;

2) среди чисел 0, HW, L, HW+L имеется три различных числа по модулю n:

а) $HW \equiv L \bmod(n)$,

б) $HW+L \equiv 0 \bmod(n)$.

Непосредственно проверяется, что в каждом из указанных случаев

$$\sum_{d|n} g_{\omega,HW,L}(d)=\omega|X|^{n-2}(|X|-1).$$

Таким образом, доказано требуемое основное равенство. Прямое использование формулы обращения Мебиуса для функций $f_{\omega, HW, L}$, $g_{\omega, HW, L}$ позволяет получить

$$\sum_{\Im \in M_\omega} | |\Phi(\Im)| | = \sum_{d|\omega} \overline{\mu}(d) f_{\omega,HW,L}(\frac{\omega}{d}),$$

и следовательно,

$$\sum_{\Im \in M_\omega} | |\Phi(\Im)| | = \sum_{d|\omega, d \notin \Theta} \overline{\mu}(\frac{\omega}{d}) \omega |X|^{d-2} (|X|-1).$$

Замечание 2. Случай (H, ω) = (L,ω) = d ≠ ω сводится к указанному случаю путем рассмотрения d-грамм последовательности P (ℑ) в качестве нового алфавита.

23.4. Примеры стабильных слева (справа) бинарных отношений на группе G

Пример 1. $\theta_л$ – бинарное отношение равенства на G. Соответствующее $\theta_л$ бинарное отношение $\hat{}\theta_л$ на $\{h_x: x \in X\}$ есть бинарное отношение равенства.

Пример 2. $\theta_л$: $g_1 \theta_л g_2$ тогда и только тогда, когда $g_2 = g_1 g$, где g – фиксированный элемент группы G. $\hat{}\theta_л$: $h_x \hat{}\theta_л h_{x`}$ тогда и только тогда, когда $h_x = g h_{x`} g^{-1}$. В этом случае удобно говорить, что элементы h_x, $h_{x`}$ g-сопряжены в G.

Пример 3. $\theta_л$: $g_1 \theta_л g_2$ тогда и только тогда, когда $(g_1)^{-1} g_2 \in C$, где C – фиксированная подгруппа G; $\hat{}\theta_л$: $h_x \hat{}\theta_л h_{x`}$ тогда и только тогда, когда элементы $h_x$, $h_{x`}$ лежат в одном смежном классе по двойному модулю (C, C). В частном случае, когда C – нормальный делитель

группы G, последнее условие равносильно условию: h_x, $h_{x`}$ лежат в одном смежном классе группы G по C.

Пример 4. G – группа подстановок. $\theta_л$: $g_1\theta_л g_2$ тогда и только тогда, когда подстановки g_1, g_2 одинаковой четности; $\wedge\theta_л$: $h_x\wedge\theta_л h_{x`}$ тогда и только тогда, когда подстановки $h_x$, $h_{x`}$ одинаковой четности.

Очевидно, данный пример является частным случаем второй части примера 3.

Пример 5. Здесь мы используем новые обозначения. Пусть G – группа подстановок степени n. Подстановку $g\in G$ будем записывать в виде

$$g = \begin{pmatrix} 1 & 2 & \dots & n \\ g(1) & g(2) & \dots & g(n) \end{pmatrix}.$$

Через $\rho(g, g`) = \rho(g(1), g(2), ..., g(n); g`(1), g`(2), ..., g`(n))$ – обозначим расстояние Хемминга между подстановками g, g`. Положим

$$\mu^*(g, g`) = \frac{\rho(g, g`)}{n}.$$

Очевидно, что μ^* – метрика на G и для любых g, g`, g_1, g_2 из G

$$\mu^*(gg_1, gg_2) = \mu^*(g_1g`, g_2g`) = \mu^*(g_1, g_2).$$

Определим стабильное слева бинарное отношение $\theta_л$ на группе подстановок $G= \langle (h_x)_{x\in X}\rangle$. Положим $\theta_л$: $g_1\theta_л g_2$ тогда и только тогда, когда $\mu^*(g_1, g_2) \le \nu$, где ν – фиксированное число, $0\le \nu < 1$; $\wedge\theta_л$: $h_x\wedge\theta_л h_{x`}$ тогда и только тогда, когда существует подстановка $g\in G$, для которой

$$\mu^*(e, g) \le \nu,\ \ \mu^*(e,(h_x)^{-1}gh_{x`}) \le \nu,$$

где e – тождественная подстановка. Отметим, что в этом случае выполняется неравенство

$$\mu^*(h_x, h_{x`}) \le 2\nu.$$

Примерами бинарных отношений $\theta_п$, $\wedge\theta_п$ являются приведенные выше примеры 1, 4, 5 и следующие примеры.

Пример 6. $\theta_п$: $g_1\theta_п g_2$ тогда и только тогда, когда $g_2 = gg_1$, где g – фиксированный элемент группы G; $\wedge\theta_п$: $h_x\wedge\theta_п h_{x`}$ тогда и только тогда, когда $h_x=g^{-1}h_{x`}g$.

Пример 7. $\theta_п$: $g_1\theta_п g_2$ тогда и только тогда, когда $g_1(g_2)^{-1}\in C$, где C – фиксированная подгруппа G; $\wedge\theta_п$: $h_x\wedge\theta_п h_{x`}$ тогда и только тогда, когда элементы $h_x$, $h_{x`}$ лежат в одном смежном классе по двойному модулю (C, C).

Указанные в примерах 1, 4, 5 бинарные отношения одновременно являются стабильными слева и справа.

Замечание 3. Любое отображение φ: $G \to G$ является одновременно и бинарным отношением на G: $g_1 \varphi g_2$ тогда и только тогда, если $\varphi(g_1)=g_2$. В примере 2, таким образом, записано отображение φ_g:$G \to G$, $\varphi_g(g_1)=g_1 g$. Пример 6 дает отображение $\psi_g(g_1) = g g_1$. Представляет интерес изучение вопросов σ-периодичности последовательности $A^H(P^1) = y(1), y(1+H), ..., y(1+jH), ...$ при отображении $\sigma = \varphi$, φ: $G \to G$, не совпадающим с отображением указанного в примерах 2, 6 вида. (Приводимые ниже результаты пунктов 4, 5 получены автором совместно с А. Е. Тришиным.)

23.5. φ-периоды последовательности $A^H(P^1)$ для автоморфизмов φ-группы G

Удобно для σ-периодической последовательности элементов алфавита Y отдельно выделять случай: $\sigma = \varphi$ есть отображение Y в Y, в связи с чем напомним следующее.

Определение 4. Последовательность $Q = y(1), y(2), ..., y(j), ...$ элементов алфавита Y называется φ-изопериодической, если найдется натуральное число d, при котором для любого j

$$y(j+d) = \varphi(y(j))$$

Любое такое число d называется φ-изопериодом последовательности Q. Если для последовательности Q при некотором натуральном d выполняется условие $\varphi(y_j) \neq y_{j+d}$ при любом $j \in \{1, 2, ...\}$, то такая последовательность называется φ-антиизопериодической, а число d называется ее φ-антиизопериодом.

Через AutG обозначим множество всех автоморфизмов группы $G = \langle (h_x)_{x \in X} \rangle$, $\mathrm{ord}\varphi$ – порядок $\varphi \in \mathrm{Aut}G$.

Теорема 5. Пусть $\varphi \in \mathrm{Aut}G$, $G = \langle (\delta_x)_{x \in X} \rangle$. Тогда если последовательность $A^H(P^1)$ φ-изопериодична с минимальным φ-изопериодом W, то выполняется одно из условий:

1) $\varphi(\{h_x: x \in X\}) = \{h_x: x \in X\}$, $\omega \mid W \cdot \mathrm{ord}\varphi$ и WH – один из φ-изопериодов последовательности $P^1 = h_{x(1)}, h_{x(2)}, ..., h_{x(j)}, ...$

2) WH – один из φ-антиизопериодов последовательности P^1.

Доказательство. Из условия φ-изопериодичности последовательности $A^H(P^1)$ с минимальным φ-изопериодом W следует, что любого натурального числа t имеет место равенство:

$$\varphi(y_{1+tH}) = y_{1+tH+WH}.$$

Отсюда и из условия взаимной простоты чисел H и ω (аналогично доказательству теоремы 1) вытекает, что для любого c∈{1, 2, ...}

$$\varphi(yc) = yc+WH.$$

Далее, следуя схеме доказательства теоремы 1, для c∈{1, 2, ...} получаем

$$\phi(h_{x_c}) = h_{x_{c+WH}}$$

тогда и только тогда, когда

$$\phi(h_{x_{c+L}}) = h_{x_{c+L+WH}} \qquad (29)$$

и, в силу взаимной простоты чисел ω и L, WH является либо φ-изопериодом последовательности P, либо ее φ-антиизопериодом.

Предположим, что WH – φ-изопериод последовательности P^1, следовательно, WH·ordφ – один из ее периодов (возможно не минимальный) и поэтому ω| WH·ord φ. Учитывая, что (ω, H) = 1, получаем ω | W·ord φ.

Если же WH – φ-изопериод последовательности P^1, то

$$\phi(h_{x_c}) = h_{x_{c+WH}}, \; c\in\{1, 2, ...\},$$

и условие $\varphi(\{\delta_x: x\in X\}) = \{\delta_x: x\in X\}$ следует из того, что в последовательности P встречаются все подстановки из множества образующих группы G. Теорема доказана.

Следствие 1. Пусть φ∈AutG, $G = <(\delta_x)_{x\in X}>$, последовательность $A^H(P^1)$ φ-изопериодична с минимальным φ-изопериодом W. Тогда для любого m∈{1, ..., ordφ –1} выполняется одно из условий:

1) последовательность $P^1 = h_{x(1)}, h_{x(2)}, ..., h_{x(j)}, ...$ φ^m-антиизопериодична с φ^m-антиизопериодом mWH.

2) Последовательность P^1 φ^m-изопериодична с φ^m-изопериодом, равным mWH. При этом $W = \frac{k_m\omega}{[m, ord\phi]}$, где k_m – некоторое натуральное число, $k_m \le [m, ord\ \varphi]$.

Доказательство. Так как W – φ-изопериод последовательности $A^H(P^1)$, то $W_m = mW$ – ее φ^m-изопериод. По теореме 5 выполняется одно из условий:

1) mWH – один из φ-антиизопериодов последовательности P;

2) $\varphi^m(\{\delta_x : x\in X\}) = \{\delta_x : x\in X\}$, W_mH – один из φ-изопериодов последовательности P, причем ω| $W_m \cdot ord\ \varphi^m$.

Последнее условие равносильно тому, что существует натуральное число k_m, при котором

$$k_m\omega = W_m\cdot ord\varphi^m,$$

то есть

$$W = \frac{k_m \omega}{[m, ord\phi]}.$$

Так как минимальный φ-изопериод последовательности не превосходит ее периода, а период последовательности $A^H(P^1)$ делит период ω последовательности P, то $W \le \omega$. Откуда имеем:

$$K_m \le m \cdot ord\ \varphi^m = m\frac{ord\phi}{(m, ord\phi)} = [m, ord\ \varphi].$$

Следствие доказано.

Следствие 2. Пусть $\varphi \in AutG$, $G = \langle (h_x)_{x \in X} \rangle$, последовательность $A^H(P^1)$ φ-изопериодична с минимальным φ-изопериодом W. Тогда, если ω не делит $W \cdot ord\varphi$, то выполняются следующие условия:

1) P – антиизопериодическая последовательность с φ^m-антиизопериодами, равными mWH, $m \in \{1, ..., k-1\}$, где $k = \max\{k' \in \{1, 2, ...\}: \omega | k' W \cdot ord\varphi\}$;

2) $k \le ord\varphi$.

Доказательство. Пусть $m \in \{1, ..., k-1\}$. По определению числа k период ω последовательности P не делит $mW \cdot ord\varphi$. Следовательно, из теоремы 5 получаем, что mWH – φ^m-антиизопериод последовательности P.

Докажем неравенство $k \le ord\varphi$. Предположим $k > ord\varphi$. Тогда для $m = ord\varphi$ получаем: $WH \cdot ord\varphi$ – антипериод последовательности P, значит, $W \cdot ord\varphi$ – антипериод последовательности $A^H(P^1)$, что неверно, так как $W \cdot ord\varphi$ – один из периодов последовательности $A^H(P^1)$.

Из доказанного следствия 2 можно легко получить нижнюю оценку для минимального φ-изопериода последовательности $A^H(P^1)$ (следствие 3). Верхняя оценка $W \le \omega$ очевидна.

Следствие 3. Пусть выполняются условия теоремы 5. Тогда, если $\omega | W \cdot ord\varphi$, то

$$\frac{\omega}{ord\phi} \le W \le \omega.$$

Если же ω не делит $W \cdot ord\varphi$, то

$$\frac{\omega}{(ord\phi)^2} \le W \le \omega.$$

Замечание 4. Пусть W – минимальный φ-изопериод последовательности $A^H(P^1)$, тогда $W \cdot ord\varphi$ – один из периодов последовательности $A^H(P^1)$, и, следовательно, либо $WH \cdot ord\varphi$ – период последова-

тельности P^1 и $\omega | W \cdot ord\varphi$, либо $WH \cdot ord\varphi$ – антипериод последовательности P^1 и ω не делит $W \cdot ord\varphi$. Поэтому следствие 3 можно переформулировать следующим образом: если $WH \cdot ord\varphi$ – период последовательности P^1, то $\frac{\omega}{ord\phi} \le W \le \omega$. В противном случае, $WH \cdot ord\varphi$ – антипериод P и имеет место оценка $\frac{\omega}{(ord\phi)^2} \le W \le \omega$.

Замечание 5. Оценка $\frac{\omega}{(ord\phi)^2} \le W$ достигается в том и только в том случае, когда последовательность P^1 антипериодическая с φ^m-антипериодами mWH, $m \in \{1, ..., ord\varphi - 1\}$, то есть когда число k из условия следствия 2 равно $ord\ \varphi$. Если же $k < ord\ \varphi$, то эту оценку можно усилить: $W \ge \frac{\omega}{ord\phi(ord\phi - 1)}$.

23.6 Оценки мер приближенных φ-периодов последовательности $A^H(P^1)$ для автоморфизмов группы

Рассмотрим теперь вопрос оценки меры $\mu(A^H(P^1), W, \varphi)$ приближенного φ-изопериода последовательности $A^H(P^1)$, $\varphi \in AutG$ в предположении, что $(\omega, L) = (\omega, H) = 1$, $2 \le L < \omega$, $1 \le W < \omega$.

Для периодической последовательности $g = g_1, g_2, ...$ элементов группы G периода d и для чисел L, W, $H \in \{1, 2, ...\}$ положим

$$\|\Phi_{\varphi, HW, L}(g)\| = \sum_{j=1}^{d} F_\phi(g_j, g_{j+hW}, g_{j+L}, g_{j+hW+L}),$$

где F_φ: $G^4 \to \{0,1\}$ – вспомогательное отображение, задаваемое условием:

$$F_\varphi(g_1, g_2, g_3, g_4) = 1$$

тогда и только тогда, когда

$$\varphi(g_1) = g_2, \varphi(g_3) \ne g_4$$

или

$$\varphi(g_1) \ne g_2, \varphi(g_3) = g_4.$$

Теорема 6. Пусть $\varphi \in AutG$, $G = \langle (h_x)_{x \in X} \rangle$, $P^1 = h_{x(1)}, h_{x(2)}, ..., h_{x(j)}, ...$ – периодическая последовательность периода ω, $\mu(A^H(P^1), W, \varphi)$ – мера приближенного φ-изопериода W последовательности $A^H(P^1)$, $\varphi \in AutG$. Тогда

$$\mu(A^H(P^1), W, \varphi) \ge \frac{\left\|\Phi_{\phi, hW, L}(P^1))\right\|}{4\omega}.$$

Доказательство. Пусть $\varepsilon > 0$ – произвольное фиксированное число и пусть $\overline{Q}^1 = g_1, g_2, \ldots$ – периодическая последовательность элементов группы G с φ-изопериодом W, такая что имеет место неравенство

$$\mu\left(A^H(P^1); \overline{Q}^1\right) - \mu(A^H(P^1), W, \varphi) \le \varepsilon.$$

Положим для краткости ${}^H y^1 = A^H(P^1)$ и определим вспомогательные последовательности пар элементов:

$$({}^H y^1, {}^H y^{1+W}) = (y_1, y_{1+WH}), (y_{1+H}, y_{1+H+WH}), \ldots$$

$$(\overline{Q}^1, \overline{Q}^{1+W}) = (g_1, g_{1+W}), (g_2, g_{2+W}), \ldots$$

и последовательности

$${}^h y^1 \bullet \left(\phi^{-1}\left({}^h y^{1+W}\right)\right)^{-1} = y_1\left(\phi^{-1}\left(y_{1+Wh}\right)\right)^{-1}, \; y_{1+h}\left(\phi^{-1}\left(y_{1+h+Wh}\right)\right)^{-1}, \ldots$$

$$\overline{Q}^1 \bullet \left(\phi^{-1}\left(\overline{Q}^{1+W}\right)\right)^{-1} = g_1\left(\phi^{-1}\left(g_{1+W}\right)\right)^{-1}, \; g_2\left(\phi^{-1}\left(g_{2+W}\right)\right)^{-1}, \ldots$$

Так как

$$\mu({}^H y^1, \overline{Q}^1) = \mu({}^H y^{1+W}, \overline{Q}^{1+W}),$$

то

$$2\mu({}^H y^1, \overline{Q}^1) \ge \mu(({}^H y^1, {}^H y^{1+W}); (\overline{Q}^1, \overline{Q}^{1+W})). \qquad (30)$$

Заметим, что если j-е элементы последовательностей ${}^h y^1 \bullet \left(\phi^{-1}\left({}^h y^{1+W}\right)\right)^{-1}$ и $\overline{Q}^1 \bullet \left(\phi^{-1}\left(\overline{Q}^{1+W}\right)\right)^{-1}$ не совпадают, то либо $y_{1+jH} \ne g_{1+j}$, либо $y_{1+jH+W} \ne g_{1+j+W}$, следовательно, не совпадают j-е элементы последовательностей пар $({}^H y, {}^H y^{1+W})$ и $(\overline{Q}^1, \overline{Q}^{1+W})$. Поэтому имеет место неравенство:

$$\mu(({}^H y^1, {}^H y^{1+W}); (\overline{Q}^1, \overline{Q}^{1+W})) \ge$$

$$\mu({}^h y^1 \bullet \left(\phi^{-1}\left({}^h y^{1+W}\right)\right)^{-1}; \overline{Q}^1 \bullet \left(\phi^{-1}\left(\overline{Q}^{1+W}\right)\right)^{-1}) \qquad (31)$$

В силу того, что W – φ-изопериод последовательности $\overline{Q}$, имеем:

$$\overline{Q}^1 \bullet \left(\phi^{-1}\left(\overline{Q}^{1+W}\right)\right)^{-1} = E, \qquad (32)$$

где E=e,e,… – последовательность, состоящая из единичного элемента группы G. Объединяя (30), (31), (32), получаем:

$$\mu({}^H y^1, \overline{Q}^1) \ge \frac{1}{2}\mu({}^h y^1 \bullet \left(\phi^{-1}\left({}^h y^{1+W}\right)\right)^{-1}; E). \qquad (33)$$

Пусть T_1 – период последовательности ${}^h y^1 \bullet \left(\phi^{-1}\left({}^h y^{1+W}\right)\right)^{-1}$. Период последовательности $A^H(P^1)$ делит ω, следовательно, $T_1 | \omega$. А так как $(\omega, H) = 1$, то $(T_1, H) = 1$. Поэтому

$$\mu({}^h y^1 \bullet \left(\phi^{-1}\left({}^h y^{1+W}\right)\right)^{-1}; E) = \mu(y^1 \bullet \left(\phi^{-1}\left(y^{1+W}\right)\right)^{-1}; E). \qquad (34)$$

Так как последовательность $y^1 \bullet \left(\phi^{-1}\left(y^{1+W}\right)\right)^{-1}$ – чисто периодическая периода T_1 (того же периода, что и выборка из нее с шагом H), то

$$\mu(y^1 \bullet \left(\phi^{-1}\left(y^{1+W}\right)\right)^{-1};\ E) = \frac{1}{T_1}\rho_{T_1}(y^1 \bullet \left(\phi^{-1}\left(y^{1+W}\right)\right)^{-1};$$

$$E) = \frac{1}{T_1}\rho_{T_1}(y^2 \bullet \left(\phi^{-1}\left(y^{2+W}\right)\right)^{-1};E)=\mu(y^2 \bullet \left(\phi^{-1}\left(y^{2+W}\right)\right)^{-1};\ E). \qquad (35)$$

Из (34) и (35), учитывая условие $T_1 | \omega$, имеем:

$$\mu({}^h y^1 \bullet \left(\phi^{-1}\left({}^h y^{1+W}\right)\right)^{-1};\ E\ ) \geq$$

$$\geq \mu(\ (y^1 \bullet \left(\phi^{-1}\left(y^{1+W}\right)\right)^{-1}, y^2 \bullet \left(\phi^{-1}\left(y^{2+W}\right)\right)^{-1});\ (E,E)\ ) =$$

$$= \frac{1}{2\omega}\rho_{\omega}(\ (y^1 \bullet \left(\phi^{-1}\left(y^{1+W}\right)\right)^{-1}, y^2 \bullet \left(\phi^{-1}\left(y^{2+W}\right)\right)^{-1});\ (E,E)\ ) =$$

$$= \frac{1}{2\omega}\ |\{\ c \in \overline{1,\omega}:\ y_c\left(\phi^{-1}\left(y_{c+W}\right)\right)^{-1} \neq e \text{ либо } y_{c+1}\left(\phi^{-1}\left(y_{c+1+W}\right)\right)^{-1} \neq e\ \}| =$$

$$= \frac{1}{2\omega}\ |\{\ c \in \overline{1,\omega}:\ \varphi(y_c) \neq y_{c+W} \text{ либо } \varphi(y_{c+1}) \neq y_{c+1+W}\ \}| \geq$$

$$\geq \frac{1}{2\omega}\sum_{c=1}^{\omega} F(h_{x_c}, h_{x_{c+Wh}}, h_{x_{c+L}}, h_{x_{c+L+Wh}}) = \frac{1}{2\omega}\|\Phi_{\varphi,HW,L}(P^1)\|. \qquad (36)$$

Поясним, почему имеет место последнее неравенство. Пусть $F(h_{x_c}, h_{x_{c+Wh}}, h_{x_{c+L}}, h_{x_{c+L+Wh}}) = 1$, тогда возможны два случая:

а) $\phi(h_{x_c}) = h_{x_{c+Wh}}$, $\phi(h_{x_{c+L}}) \neq h_{x_{c+L+Wh}}$;

б) $\phi(h_{x_c}) \neq h_{x_{c+Wh}}$, $\phi(h_{x_{c+L}}) = h_{x_{c+L+Wh}}$.

Используя условие (34), в случае а) получим: если $\varphi(y_c)=y_{c+W}$, то $\varphi(y_{c+1})\neq y_{c+1+W}$, а в случае б) получим: если $\varphi(y_{c+1})=y_{c+1+W}$, то $\varphi(y_c)\neq y_{c+W}$.

Из (33) и (36) имеем:

$$\mu({}^H y^1, Q^1) \geq \frac{1}{4\omega}\ \|\Phi_{\varphi,HW,L}(P^1)\|,$$

следовательно,

$$\mu(A^H(P^1),W,\varphi)) \geq \mu({}^H y, Q^1) - \varepsilon \geq \frac{1}{4\omega}\ \|\Phi_{\varphi,HW,L}(P^1)\| - \varepsilon,$$

а так как ε выбиралось произвольно, то

$$\mu(A^H(P^1),W,\varphi) \geq \frac{1}{4\omega}\ \|\Phi_{\varphi,HW,L}(P^1)\|.$$

Теорема доказана.

Аналогично доказательству теоремы 4 доказывается

Теорема 7. Пусть $|\{h_x:\ x \in X\}| = |X|$; последовательность $P^1 = h_{x(1)}, h_{x(2)}, ..., h_{x(j)}, ...$ элементов семейства $(h_x)_{x\in X}$ выбирается случайно и равновероятно из множества периодических последовательно-

стей элементов алфавита $\{h_x: x\in X\}$ периода ω, $\omega \geq 3$; $\varphi\in AutG$, $G = <(h_x)_{x\in X}>$, $E\mu(A^H(P^1), W, \varphi)$ – средняя мера приближенного φ-изопериода W последовательности $A^H(P^1)$, $\varphi\in AutG$, $(\omega, L) = (\omega, H) =1$, $2 \leq L < \omega$, $1 \leq W <\omega$. Тогда

$$E\mu(A^H(P^1), W, \varphi) \geq \frac{(|X|-1)\sum\limits_{\substack{d|\omega \\ d\notin\Theta}} \overline{\mu}\left(\frac{\omega}{d}\right)|\Delta|^{d-2}}{2\sum\limits_{d|\omega'} \overline{\mu}(\frac{\omega}{d})|\Delta|^{d}},$$

где $\Theta =\{n: n|Wh\}\cup\{n: n|L\}\cup\{ n: Wh \equiv L \pmod n, Wh+L \equiv 0 \pmod n)\}$, $\overline{\mu}$ – функция Мебиуса.

Глава 24. КЛАССЫ ВЕКТОРНЫХ АВТОМАТОВ С ГАРАНТИРОВАННЫМИ ПЕРИОДАМИ ВЫХОДНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ ПРИ ЗАДАННОЙ ВХОДНОЙ ПЕРИОДИЧЕСКОЙ ПОСЛЕДОВАТЕЛЬНОСТИ

24.1. Основные понятия. Вспомогательные результаты

Пусть A = (X, S, Y, h, f) – автомат с входным алфавитом X, |X| > 1. Далее мы рассмотрим автоматы с фиксированными входным X и выходным Y алфавитами.

В изучении периодов выходных последовательностей автомата при заданной периодической входной последовательности большое значение имеют следующие обобщения понятия автономности автомата [12].

Определение 1. Входные слова $P_1, P_2, \ldots, P_L$ одинаковой длины автомата A = (X, S, У, h, f) называются слабо неотличимыми относительно A (или кратко – слабо неотличимыми), если найдутся состояния $s_1, s_2, \ldots, s_к$ из S, при которых

$$A(s_1, P_1) = A(s_2, P_2) = \ldots = A(s_к, P_L).$$

В противном случае слова $P_1, P_2, \ldots, P_L$ называются сильно различимыми относительно A (сильно различимыми).

Определение 2. Автомат A называется слабо k-автономным, если все его входные слова длины k слабо неотличимы (относительно A).

Определение 3. Степенью слабой автономности σ(A) автомата A называется максимальное число k, если оно существует, при котором он слабо k-автономен. В противном случае полагаем σ(A) = ∞.

Определение 4. Входные слова P, P` автомата A сильно различимы относительно A, если

$$\{\{\bigcup_{s\in S} A(s,P)\}\bigcap\{\bigcup_{s\in S} A(s,P`)\} = \varnothing$$

(∅ – пустое множество).

Напомним, что для любых натуральных чисел a,b из условия (a,b)=d следует: существуют натуральные числа n(1), n(2), при которых

$$an(1) – bn(2) = d.$$

Положим W(s, P) – период выходной последовательности A(s, P) автомата A, полученной при его начальном состоянии s∈S при

входной периодической (имеется в виду: чисто периодической) последовательности P = x(0), x(1), … Заметим, что последовательность A(s, P) для произвольного автомата A, вообще говоря, смешанно-периодическая. Для последовательности P = x(0), x(1), x(2), … будем использовать обозначение: $P^{(j)}$ = x(j), x(j+1), … Через A(s) обозначим связную компоненту автомата A содержащую состояние $s \in S$.

Теорема 1. Пусть P = x(0), x(1), x(2), … – входная периодическая последовательность периода ω(P) автомата A = (X, S, Y, h, f) и d = (ω(P), W(s, P)). Тогда множество мультиграмм вида

$$P^{(kd)} = x(kd), x(kd+1), \ldots, k \in \{0, 1, \ldots\}, P^{(0)} = P \qquad (37)$$

слабо неотличимо относительно связной компоненты A(s) автомата A, содержащей состояние $s \in S$.

Доказательство. Для произвольного состояния s_o автомата A рассмотрим выходную (вообще говоря, смешанно-периодическую) последовательность $A(s_0, P) = y_1, y_2, \ldots$ и последовательность состояний $A_M(s_0, P) = s_0, s_1, \ldots$, отвечающих входной последовательности P и начальному состоянию $s_0 \in S$. Легко видеть, что существует t, при котором последовательность $y_t, y_{t+1}, \ldots$ – чисто периодическая и может быть получена при входной периодической последовательности P, то есть $A(s_t, P) = y_t, y_{t+1}, \ldots$ При этом связная компонента $A(s_t)$ автомата A содержится в компоненте $A(s_0)$. Для доказательства утверждения теоремы достаточно показать, что множество слов (37) слабо неотличимо относительно связной компоненты $A(s_t)$ автомата A, содержащей состояние $s_t \in S$.

Положим для краткости: $s_t = s$, ω(P) = ω, $W(s_t, P) = W$.

При (ω,W) = ω утверждение теоремы очевидно. Предположим, что (ω, W) = d ≠ ω. Пусть k – произвольное число из $\{1, \ldots, \frac{\omega}{d}\}$. Существуют натуральные числа n(1), n(2), при которых n(1)ω–n(2)W = = kd. Имеем

$$A(s, P) = A(s, P^{(0)}) = A(s, P^{(kd-kd)}) = A(s, P^{(kd - n(1)\omega + n(2)W)}) = A(s, P^{(kd + n(2)W)}) \qquad (38)$$

Выберем натуральное число n(3) так, чтобы ω делило n(2)+n(3) и продолжим равенства (38) следующим образом:

$$A(s, P^{(kd + n(2)W)}) = A(h_{x(kd+n(2)W+n(3)W-1)} \ldots h_{x(kd+n(2)W}s, P^{kd+n(2)W+n(3)W}) =$$
$$= A(h_{x(kd+n(2)W+n(3)W-1)} \ldots h_{x(kd+n(2)W}s, P^{kd}).$$

Здесь было учтено, что

$$\omega(P^{kd+n(2)W+n(3)W}) = \omega.$$

Очевидно, состояние $s_{kd}=h_{x(kd+n(2)W+n(3)W-1)}\ldots h_{x(kd+n(2)W}s$ принадлежит связной компоненте A(s) автомата A. Таким образом, доказано существование состояний s, s_d, …, $s_{к-1}$, к = $\frac{\omega}{d}$ связной компоненты A(s) автомата A, при которых

$$A(s, P) = A(s_d, P^{(d)}) = \ldots = A(s_{к-1}, P^{(к-1)d)}),$$

что и доказывает утверждение теоремы 1.

Условимся в дальнейшем говорить, что при входной последовательности $\Im$ периода $\omega(\Im)$ автомат A = (X, S, Y, h, f) является *автоматом с гарантированным выходным периодом***,** если периоды W(s,P) его выходных последовательностей A(s, $\Im$), $s \in S$, кратны $\omega(\Im)$.

На основе теоремы 1 можно сформулировать, по крайней мере, следующие два метода построения автоматов с гарантированным выходным периодом.

1. На основе оценки слабой автономности автомата.

Строится автомат A = (X, S, Y, h, f) с известной оценкой сверху k степени слабой автономности $\sigma(A)$ автомата A. Далее строится периодическая входная последовательность $\Im$ автомата A, обладающая свойствами:

– $\Im$ содержит в качестве k-грамм все слова из X^k;

– период $\omega(\Im)$ последовательности $\Im$ является простым числом.

Из теоремы 1, определения 3 вытекает, что автомат A будет автоматом с гарантированным выходным периодом.

2. На основе нахождения сильно различимых входных слов.

Строится автомат A, у которого входные слова P, P` сильно различимы относительно A. Далее строится периодическая входная последовательность $\Im$ автомата A, обладающая свойствами:

– $\Im$ содержит в качестве мультиграмм слова P, P`;

– период $\omega(\Im)$ последовательности $\Im$ является простым числом.

Из теоремы 1, определения 4 вытекает, что автомат A будет автоматом с гарантированным выходным периодом.

Ниже конкретизируется общая схема этих методов для векторных автоматов, то есть для автоматов, у которых множество состояний является векторным пространством V_n-размерности n над конечным полем F_q.

24.2. Способ построения векторного автомата с гарантированным выходным периодом на основе оценки его слабой автономности

Пусть A = (X, S, Y, h, f) – конечный неавтономный автомат с входным алфавитом X (|X| > 1), множеством состояний S, выходным алфавитом Y. Для $P \in X^k$ рассмотрим множество $\bigcup_{s \in S} A(s, P)$, представляющее собой объединение выходных слов A(s, P) при фиксированном $P \in X^k$, и множество $\Pi(k, A) = \bigcap_{P \in X^k} (\bigcup_{s \in S} A(s, P))$. В введенных обозначениях степень слабой автономности σ(A) неавтономного автомата A есть минимальное число k, если оно существует, при котором

$$\Pi(k+1, A) = \varnothing,$$

в противном случае σ(A) = ∞. Иными словами, σ(A) в случае его конечности есть максимальное число k, при котором

$$\Pi(k, A) \neq \varnothing.$$

Основная цель данного способа состоит в обосновании гипотезы, состоящей в том, что для почти всех векторных автоматов A размерности n

$$\sigma(A) \leq n.$$

Точнее говоря, при случайном и равновероятном выборе некоторого автомата A неравенство

$$\sigma(A) \leq n$$

выполняется с вероятностью, весьма близкой к единице.

При условии, что данное утверждение верно, можно легко строить векторные автоматы с гарантированным (с надежностью, близкой к единице) выходным периодом, беря в качестве их входных последовательностей периодические последовательности простого периода, содержащие все слова из X^{n+1}.

В обосновании гипотезы ограничимся рассмотрением векторных автоматов с множеством состояний $S = V_n$, являющимся n-мерным векторным пространством над полем из двух элементов F_2, входным и выходным алфавитами $X = Y = F_2$.

Для вычисления вероятности события Π(L, A) = ∅ при случайном и равновероятном выборе векторного автомата мы будем пользоваться приводимой ниже вероятностной моделью, которая, на наш взгляд, вполне отражает поведение множества Π(L, A) для L, много меньших |S|.

Вероятностная модель. Проводится 2^L испытаний, каждое из которых состоит в случайном независимом и равновероятном выборе (выборка с возвращением) 2^n двоичных последовательностей длины L из множества V_L всех двоичных последовательностей длины L. Берется общее пересечение Π_L выбранных при 2^L испытаниях множеств. Рассматриваемая случайная величина представляет собой мощность $|\Pi_L|$ пересечения Π_L.

При условии, что L много меньше |S|, по нашему мнению, поведение случайной величины Π_L достаточно хорошо моделирует весьма сложную по своей природе случайную величину |П(L, A)|. В частности, мы предполагаем, что вероятность

$$P(|\Pi(L, A)| = r)$$

при случайном и равновероятном выборе автомата A из достаточно широкого класса автоматов, незначительно отличается от вероятности

$$P(|\Pi_L| = r).$$

Лемма 1. Математическое ожидание случайной величины $|\Pi_L|$ равно

$$2^L[1-(1-\frac{1}{2^L})^{2^n}]^{2^L}.$$

Доказательство. Обозначим через ζ_y, $y \in V_n$ случайную величину

$$\zeta_y = \begin{cases} 1, если\ \ y \in \Pi_L \\ 0, если\ \ y \notin \Pi_L \end{cases}.$$

Очевидно,

$$|\Pi_L| = \sum_{y \in V_n} \zeta_y,$$

поэтому

$$E|\Pi_L| = \sum_{y \in V_n} E(\zeta_y) = 2^L \cdot P(\zeta_y = 1).$$

Но

$$P(\zeta_y = 1) = [1-(1-\frac{1}{2^L})^{2^n}]^{2^L},$$

и, таким образом,

$$E|\Pi_L| = 2^L \cdot [1-(1-\frac{1}{2^L})^{2^n}]^{2^L}.$$

Лемма 2. При L > n выполняется

$$P(|\Pi_L| = 0) > 1-2^{(n-L)\cdot 2^L+L}.$$

Доказательство. Оценим сверху $E|\Pi_L|$. Для этого предварительно оценим снизу величину $(1-\frac{1}{2^L})^{2^n}$. Имеем

$$(1-\frac{1}{2^L})^{2^n} = 1-\frac{2^n}{2^L}+\frac{2^n(2^n-1)}{2}\cdot\frac{1}{2^{2L}}-\ldots+\frac{2^n(2^n-1)\ldots(2^n-i+1)}{i!}(-\frac{1}{2^L})^i .$$

Этот ряд знакопеременный и при L > n Лейбницевский, поэтому

$$(1-\frac{1}{2^L})^{2^n} > 1-2^{n-L} .$$

Подставляя эту оценку в формулу для $E|\Pi_L|$, получаем

$$E|\Pi_L| < 2^{(n-L)\cdot 2^L+L} .$$

В то же время

$$E|\Pi_k| = \sum_{i=0}^{2^n} i\cdot P(|\Pi_L| = i),$$

поэтому

$$P(|\Pi_L| = 0) = 1-\sum_{i=1}^{2^n} P(|\Pi_L| = i) > 1-E|\Pi_L| > 1-2^{(n-L)\cdot 2^L+L},$$

что и требовалось доказать.

Замечание. Утверждение леммы 2 можно получить и другим способом. Несложно получить формулу

$$P(|\Pi_L| = 0) = (1-[1-(1-\frac{1}{2^L})^{2^n}]^{2^L})^{2^L},$$

а из нее с помощью неравенства

$$(1-\frac{1}{2^L})^{2^n} > 1-2^{n-L}$$

и утверждение леммы 2.

Лемма 3. Для любого L выполняется

$$P(|\Pi_L| = 0) > 1-2^L\cdot\exp(-2^L\cdot\exp(-\frac{2^n}{2^L-1})) .$$

Доказательство. Имеем

$$2^L\ln(1-\frac{1}{2^L}) = -2^n(\frac{1}{2^L}+\frac{1}{2^{2L}\cdot 2}+\frac{1}{2^{3L}\cdot 3}+\ldots+\frac{1}{2^{i\cdot L}\cdot i}+\ldots),$$

и, следовательно,

$$2^n\ln(1-\frac{1}{2^L}) > -2^n(\frac{1}{2^L}+\frac{1}{2^{2L}}+\frac{1}{2^{3L}}+\ldots+\frac{1}{2^{i\cdot L}}+\ldots) = -2^n(\frac{1}{2^L-1}),$$

то есть

$$(1-\frac{1}{2^L})^{2^n} > \exp(-\frac{2^n}{2^L-1}) .$$

Используя формулу для $E(|\Pi_L|)$, получаем

$$E(|\Pi_L|) < 2^L[1-\exp(-\frac{2^n}{2^L-1})]^{2^L} .$$

В свою очередь,

$$[1-\exp(-\frac{2^n}{2^L-1})]^{2^L} < \exp(-2^L\cdot\exp(-\frac{2^n}{2^L-1})),$$

так как

$$2^L \ln(1-\exp(-\frac{2^n}{2^L-1})) < -2^L \cdot \exp(-\frac{2^n}{2^L-1}).$$

Таким образом,

$$E(|\Pi_L|) < 2^L \cdot \exp(-2^L \cdot \exp(-\frac{2^n}{2^L-1})),$$

поэтому

$$P(|\Pi_L| = 0) > 1-2^L \cdot \exp(-2^L \cdot \exp(-\frac{2^n}{2^L-1})).$$

Из леммы 3 легко получить следствие.

Следствие.

$$P(|\Pi_L| = 0) > 1-\frac{2^L}{2^{2^{L-2^{n-L}+2}}}.$$

Полученные оценки вероятности $P(|\Pi_L| = 0)$ показывают, в частности, что для $n > 8$, $L > n$ вероятность того, что пересечение Π_L пусто, практически можно считать равной единице.

Таким образом, считая, что выбранная вероятностная модель правильно отражает поведение случайной величины $|\Pi(L, A)|$, можно заключить, что для почти всех векторных автоматов (с $S = V_n$, $X = Y = F_2$) размерности n степень слабой автономности не превосходит n.

24.3. Способ построения векторного автомата с гарантированным выходным периодом на основе нахождения его сильно различимых входных слов

Пусть P – входное слово (входная последовательность) автоматов A = (X, S, Y, h, f), A` = (X, S` Y, h`, f`).

Определение 5. Автомат A называется P-вложимым в автомат A` (или A` P покрывает автомат A), если для любого состояния $s \in S$ автомата A найдется состояние $s` \in S`$ автомата A`, для которых

$$A(s, P) = A`(s`, P)$$

Определение 6. Автоматы A, A` называются P – неотличимыми, если они P-вложимы друг в друга.

Легко доказывается лемма 4.

Лемма 4. Пусть автомат A одновременно P-вложим и P`-вложим в автомат A^, причем слова (мультиграммы) P, P` сильно различимы относительно автомата A^. Тогда P, P` сильно различимы и относительно автомата A.

Предположим теперь, что автомат A = (X, S, Y, h, f) P-вложим в автомат A` = (X, S`, Y, h`, f`). В этом случае найдется отображение Ψ_P S в S`, при котором для любого s ∈ S

$$A(s, P) = A`(\Psi_P(s), P).$$

Определение 7. Автомат A = (X, S, Y, h, f) называется инъективно P-вложимым в автомат A` = (X, S`,Y, h`, f`), если найдется инъективное отображение Ψ_P: S→S`, при котором

$$A(s, P) = A`(\Psi_P(s), P), s \in S.$$

Определение 8. Входное слово P автомата A называется диагностическим (инъективным) для A, если из условия

$$A(s,P) = A(s`,P)$$

вытекает s = s`.

Легко проверить справедливость следующего утверждения.

Лемма 5. Если автомат A инъективно P-вложим в A` и P – диагностическое слова для A`, то P будет диагностическим словом и для A.

Далее под периодической входной последовательностью $\Im$ = = x(1), x(2), ..., x(j), ... автомата A мы будем понимать чисто периодическую последовательность элементов алфавита X, а под ее периодом – минимальный период.

Следствие теоремы 1. Пусть $\Im$ = x(1), x(2), ..., x(j), ... – входная периодическая последовательность перестановочного автомата A простого периода $\omega(\Im)$, содержащая сильно различимые мультиграммы P, P` относительно A. Тогда для любого s∈S период $W(s,\Im)$ выходной последовательности $A(s, \Im)$ автомата A кратен $\omega(\Im)$.

Предлагаемый метод синтеза автоматов с гарантированными выходными периодами состоит из двух этапов:

1) построение автомата A^ с сильно различимыми относительно A^ входными словами P, P`;

2) построение перестановочного автомата A, который одновременно P – вложим в A^ и P` – вложим в A^.

Входные мультиграммы P, P` построенного таким образом автомата A будут, согласно лемме 4, сильно различимы относительно A, а согласно следствию теоремы 1, при входной последовательности простого периода, содержащей мультиграммы P, P`, автомат A будет автоматом с гарантированным выходным периодом.

Ниже конкретизируется общая схема этого метода для векторных автоматов, то есть автоматов, у которых множество состояний является векторным пространством надконечным полем. В качестве

исходного автомата A^ мы выбираем линейный автомат. При этом рассматриваются следующие случаи применения данного метода: в качестве мультиграмм P, P` будут взяты однородные мультиграммы $x^k = \underbrace{x,x,...,x}_{k}$, $x`^k = \underbrace{x`,x`,...,x`}_{k}$ (мультиграммы, составленные из одного символа алфавита X), а P-вложимость и P`-вложимость автоматов будет осуществлена с помощью гомоморфизмов соответствующих подавтоматов автоматов A, A`. Для осуществления намеченного плана предварительно напомним необходимые нам основные понятия теории автоматов.

Говорят, что отображение Ψ S в S` определяет гомоморфизм по состояниям автомата $A = (X, S, Y, (h_x)_{x\in X}, (f_x)_{x\in X})$ в автомат $A` = (X, S`, Y, (h`_x)_{x\in X}, (f`_x)_{x\in X})$, если

$$\Psi h_x = h`_x\Psi, \qquad f_x = f`_x\Psi, \quad x\in X.$$

Для автомата $A = (X, S, Y, (h_x)_{x\in X}, (f_x)_{x\in X})$ автономный автомат $a_x = (S, h_x, Y, f_x)$ с функцией перехода h_x и функцией выхода f_x назовем *x*-м ассоциированным с A автономным автоматом.

Под *векторным линейным автоматом* будем понимать автомат $^A = (X, V_n, F_q, (\alpha_x)_{x\in X}, (\beta_x)_{x\in X})$ – с множеством состояний V_n, являющимся векторным пространством над конечным полем F_q (из q элементов), выходным алфавитом F_q, частичными функциями перехода $(\alpha_x)_{x\in X}$, представляющими собой линейные преобразования векторного пространства V_n, и частичными функциями выхода $(\beta_x)_{x\in X}$, являющимися линейными отображениями V_n в F_q. Нас далее будут интересовать векторные линейные перестановочные автоматы, то есть векторные линейные автоматы, у которых линейные преобразования $(\alpha_x)_{x\in X}$ векторного пространства V_n являются невырожденными преобразованиями.

Наряду с векторным линейным перестановочным автоматом $^A = (X, V_n, F_q, (\alpha_x)_{x\in X}, (\beta_x)_{x\in X})$ нас будет интересовать его подавтомат, определенный на множестве $V_n\backslash 0$, являющимся векторным пространством V_n над конечным полем F_q (из q элементов) с исключенным нулевым вектором. Этот подавтомат мы будем обозначать той же буквой A^ (ограничения отображений α_x, β_x на $V_n\backslash 0$ будем обозначать теми же буквами), то есть $A^ = (X, V_n\backslash 0, F_q, (\alpha_x)_{x\in X}, (\beta_x)_{x\in X})$, где $\alpha_x: V_n\backslash 0 \to V_n\backslash 0$, $\beta_x: V_n\backslash 0 \to F_q$.

Обозначим через $A = (X, V_m, F_q, (h_x)_{x\in X}, (f_x)_{x\in X})$ – произвольный векторный перестановочный автомат с множеством состояний V_m, для которого $h_x(0) = 0$, $f_x(0) = 0$. Той же буквой A будем обозначать

векторный перестановочный автомат с множеством состояний $V_m\backslash 0$: $A = (X, V_m\backslash 0, F_q, (h_x)_{x\in X}, (f_x)_{x\in X})$. Ниже всегда будет ясно, о каких автоматах идет речь с множеством состояний $V_m\backslash 0$, или V_m.

Для линейного автомата $A^\wedge = (X, V_n, F_q, (\alpha_x)_{x\in X}, (\beta_x)_{x\in X})$ введем дополнительные обозначения: V_n^* – пространство линейных функций, определенных на V_n; ${}^t\alpha_x$ – линейное преобразование пространства V_n^*, сопряженное с линейным преобразованием α_x, $x\in X$; $\chi(\beta_x, {}^t\alpha_x)$ – минимальный многочлен вектора β_x, относительно линейного преобразования ${}^t\alpha_x$, $x\in X$; $\deg\chi(\beta_x, {}^t\alpha_x)$ – степень многочлена $\chi(\beta_x, {}^t\alpha_x)$.

Теорема 2. Пусть $A = (X, V_m\backslash 0, F_q, (h_x)_{x\in X}, (f_x)_{x\in X})$ – векторный перестановочный автомат, $A^\wedge = (X, V_n\backslash 0, F_q, (\alpha_x)_{x\in X}, (\beta_x)_{x\in X})$ – векторный линейный перестановочный автомат, для которого при некоторых x и x` из X многочлены $\chi(\beta_x, {}^t\alpha_x)$, $\chi(\beta_{x`}, {}^t\alpha_{x`})$ взаимно просты и $\chi(\beta_x, {}^t\alpha_x) = n$. Пусть отображения $\Psi_x$, $\Psi_{x`}$ V_m в V_n, $m \geq n$, таковы, что $\Psi_x(0) = \Psi_{x`}(0) = 0$ и они осуществляют гомоморфизмы по состояниям ассоциированных с $A=(X, V_m\backslash 0, F_q, (h_x)_{x\in X}, (f_x)_{x\in X})$ автономных автоматов $a_x = (V_m\backslash 0, h_x, F_q, f_x)$, $a_{x`} = (V_m\backslash 0, h_{x`}, F_q, f_{x`})$, соответственно, в ассоциированные с $A^\wedge = (X, V_n\backslash 0, F_q, (\alpha_x)_{x\in X}, (\beta_x)_{x\in X})$ автономные линейные автоматы $\wedge a_x = (V_n\backslash 0, F_q, \alpha_x, \beta_x)$, $\wedge a_{x`} = (V_n\backslash 0, F_q, \alpha_{x`}, \beta_{x`})$. Тогда при любой входной периодической последовательности P простого периода, содержащей однородные мультиграммы $x^k$, $x`^k$, $k \geq \deg(\chi(\beta_x, {}^t\alpha_x) \cdot \chi(\beta_{x`}, {}^t\alpha_{x`}))$, автомат A будет автоматом с гарантированным выходным периодом.

Доказательство. При выполнении условий теоремы мультиграммы x^k, $x`^k$ будут сильно различимыми относительно автомата $A^\wedge$; то же время очевидно, автомат A будет одновременно $x^k$-вложим и $x`^k$-вложим в автомат $A^\wedge$. Следовательно, согласно лемме 4, мультиграммы x^k, $x`^k$ будут сильно различимыми и относительно автомата A, а согласно следствию теоремы 1, при входной последовательности P автомат A будет автоматом с гарантированным выходным периодом.

Теорема 3. Пусть $A = (X, V_m, F_q, (h_x)_{x\in X}, (f_x)_{x\in X})$ – векторный перестановочный автомат ($h_x(0) = 0$, $f_x(0) = 0$, $x\in X$) $A^\wedge = (X, V_n, F_q, (\alpha_x)_{x\in X}, (\beta_x)_{x\in X})$ – векторный линейный перестановочный автомат, для которого при некоторых x и x` из X $\deg\chi(\beta_x, {}^t\alpha_x) = \deg\chi(\beta_{x`}, {}^t\alpha_{x`}) = n$. Пусть $m = n$ и отображения $\Psi_x$, $\Psi_{x`}$ V_n в V_n таковы, что $\Psi_x(0) = \Psi_{x`}(0) = 0$ и они осуществляют изоморфизмы по со-

стояниям ассоциированных с $A = (X, V_m, F_q, (h_x)_{x\in X}, (f_x)_{x\in X})$ автономных автоматов $a_x = (V_m, h_x, F_q, f_x)$, $a_{x`} = (V_m, h_{x`}, F_q, f_{x`})$ соответственно в ассоциированные с $A^\wedge = (X, V_n, F_q, (\alpha_x)_{x\in X}, (\beta_x)_{x\in X})$ автономные линейные автоматы $\wedge a_x = (V_n, F_q, \alpha_x, \beta_x)$, $\wedge a_{x`} = (V_n, F_q, \alpha_{x`}, \beta_{x`})$. Если отображение $\Psi_x \cdot (\Psi_{x`})^{-1}$: $V_n \to V_n$ является нелинейным отображением, то A – нелинейный (с точностью до неотличимости векторных автоматов) автомат.

Доказательство. При выполнении условий теоремы каждый из автоматов a_x, $a_{x`}$, $\wedge a_x$, $\wedge a_{x`}$ находится в приведенной форме, в частности, сами автоматы A, $\wedge A$ – приведенные автоматы.

Предположим, что условия теоремы выполнены, но тем не менее автомат A неотличим от некоторого векторного линейного автомата $\tilde{\tilde{A}}$. В силу того что приведенная форма линейного автомата является линейным автоматом, будем без ограничения общности рассуждений считать, что $\tilde{\tilde{A}}$ – приведенный автомат. Положим $\tilde{\tilde{A}} = (X, V_n, F_q, (\tilde{\tilde{a}}_x)_{x\in X}, (\tilde{\tilde{c}}_x)_{x\in X})$. Из неотличимости приведенных автоматов A, $\tilde{\tilde{A}}$ вытекает их изоморфизм. Пусть отображение φ: $V_n \to V_n$ осуществляет изоморфизм автомата A в автомат $\tilde{\tilde{A}}$. Имеем

$$\Psi_x h_x (\Psi_x)^{-1} = \alpha_x, \qquad f_x = \beta_x \Psi_x;$$
$$\varphi h_x (\varphi)^{-1} = \tilde{\tilde{a}}_x, \quad f_x = \tilde{\tilde{c}}_x \varphi$$

и, в частности,

$$\varphi(\Psi_x)^{-1} \alpha_x \Psi_x (\varphi)^{-1} = \tilde{\tilde{a}}_x$$
$$\beta_x = \tilde{\tilde{c}}_x \varphi (\Psi_x)^{-1}.$$

Таким образом, отображение $\varphi(\Psi_x)^{-1}$ осуществляет изоморфизм линейного автомата $\wedge a_x = (V_n, F_q, \alpha_x, \beta_x)$ в линейный автомат $\tilde{\tilde{a}}_x = (X, V_n, F_q, \tilde{\tilde{a}}_x, \tilde{\tilde{c}}_x)$.

Аналогично показывается, что отображение $\varphi(\Psi_{x`})^{-1}$ осуществляет изоморфизм автомата $\wedge a_{x`} = (V_n, F_q, \alpha_{x`}, \beta_{x`})$ в линейный автомат $\tilde{\tilde{a}}_{x`} = (X, V_n, F_q, \tilde{\tilde{a}}_{x`}, \tilde{\tilde{c}}_{x`})$.

Ранее было отмечено, что линейные автономные автоматы $\wedge a_x$, $\wedge a_{x`}$ – приведенные. Очевидно, автоматы $\tilde{\tilde{a}}_x$, $\tilde{\tilde{a}}_{x`}$ также являются приведенными. В связи с чем несложно показывается, что любой изоморфизм автомата $\wedge a_{x`} = (V_n, F_q, \alpha_{x`}, \beta_{x`})$ в автомат $\tilde{\tilde{a}}_{x`} = (X, V_n, F_q, \tilde{\tilde{a}}_{x`}, \tilde{\tilde{c}}_{x`})$ является линейным отображением, в частности, отображение $\varphi(\Psi_x)^{-1}$ – линейно. Аналогично получаем, что $\varphi(\Psi_{x`})^{-1}$ – линейное отображение. Следовательно, произведение

$$(\varphi(\Psi_x)^{-1})^{-1} \cdot \varphi(\Psi_{x`})^{-1} = \Psi_x \cdot (\Psi_{x`})^{-1}$$

является линейным отображением V_n в V_n, что противоречит условию теоремы 2. Таким образом, теорема 2 полностью доказана.

24.4. Пример синтеза векторного нелинейного автомата с гарантированным выходным периодом

Ниже используются понятие разветвления нелинейного отображения пространства V_n в себя с помощью линейных преобразований V_n [25].

Пусть автомат A имеет вид:

$$A = (X, S, (h_x)_{x\in X}, (f_x)_{x\in X}) = (F_2, V_n, F_2, ([\alpha_x, \alpha_{x+1}, \eta])_{x\in F_2}, (c_x)_{x\in F_2}).$$

Здесь положено: $X = F_2$ – поле из двух элементов; $S = V_n$ – n-мерное векторное пространство над полем F_2; частичные функции переходов $h_x = [\alpha_x, \alpha_{x+1}, \eta]$, $x \in F_2$, определены равенствами

$$h_x(v) = [\alpha_x, \alpha_{x+1}, \eta]\, v = \alpha_{f(v)+i} = \eta(v)(\alpha_0+\alpha_1)v + \alpha_x v,\ v\in V_n,$$

где α_0, α_1 – линейные преобразования векторного пространства V_n; η-линейная функция на V_n; частичные функции выхода $f_x = c_x$, $x\in X$, являются линейными отображениями V_n в F_2.

Пусть Q – произвольное линейное преобразование n-мерного векторного пространства V_n над полем F_2 с неприводимым характеристическим многочленом $\chi(Q)$; η, $\tilde{c}_0$, $\tilde{c}_1$ – линейные функции, определенные на V_n (η, $\tilde{c}_0$ и η, $\tilde{c}_1$ – линейно независимые пары функций); a, b – векторы пространства V_n, при которых

$$\eta(a) = 0,\ \eta(b) = 0,\ \tilde{c}_0(b)=0,$$
$$\eta(Q^{-1}a)=1,\ \eta(Q^{-1}b) = 0,\ \tilde{c}_1(b) = 0,$$
$$\eta(Qa) = 0,\ \eta(Qb) = 1.$$

Для краткости обозначим через $A(\eta, Q)$ автомат

$$A = (F_2, V_n, F_2, ([\alpha_x, \alpha_{x+1}, \eta])_{x\in F_2}, (c_x)_{x\in F_2})$$

вида

$$\alpha_0 = Q+\alpha\otimes\eta Q,$$
$$\alpha_1 = Q+(Q(a+b)+a+b)\otimes\eta+(Qb+a+b)\otimes\eta Q^{-1}+(a+b)\otimes\eta Q),$$
$$c_0 = \tilde{c}_0(a)\cdot\eta + \tilde{c}_0,$$
$$c_1 = \tilde{c}_1(a)\cdot\eta + \tilde{c}_1,$$

где знак $\otimes$ обозначает операцию тензорного произведения.

Теорема 4. Пусть P – входная последовательность автомата $A(\eta, Q)$ простого периода $\omega(P)$, содержащая однородные L-граммы

$$0^{(L)}=\underbrace{0,0,\ldots,0}_{L},\ 1^{(L)}=\underbrace{1,1,\ldots,1}_{L},\ L \geq 2n.$$

Тогда периоды выходных последовательностей A(s, P) автомата A(η, Q), при любом начальном состоянии $s \in V_n \backslash 0$, кратны ω(P).

Доказательство теоремы разобьем на ряд самостоятельных утверждений.

Лемма 6. Линейные преобразования α_0, α_1 являются невырожденными преобразованиями пространства V_n.

Доказательство. Известно, что линейное преобразование вида

$$Q + \sum_{i=1}^{m} d_i \otimes \beta_i ,$$

где $d_i \in V_n$, а β_i-линейные функции на V_n, $i \in \{1, 2, \ldots, m\}$ невырожденно тогда и только тогда, когда определитель матрицы

$$\| \delta_{ij} + \beta_i Q^{-1} d_j \|, \ \delta_{ij} = \begin{cases} 0 \text{ при } i \neq j, \\ 1 \text{ при } i = j, \end{cases}$$

отличен от нуля. Поэтому преобразование α_0 невырожденно, так как $1+\eta(a) = 1$.

Второе линейное преобразование α_1 можно представить в виде

$$\alpha_1 = (E+b\otimes\eta)\cdot(Q + a\otimes\eta Q)\cdot(E+(a+b)\otimes\eta + b\otimes\eta Q^{-1}) =$$
$$= (E+b\otimes\eta)\cdot\alpha_0\cdot(E+(a+b)\otimes\eta+b\otimes\eta Q^{-1}),$$

где E – тождественное преобразование векторного пространства V_n. Линейные преобразования $E+b\otimes\eta$ и $E+(a+b)\otimes\eta + b\otimes\eta Q^{-1}$ невырождены, так как $1+\eta(b) = 1$ и

$$\begin{vmatrix} 1+\eta(a+b) & \eta(b) \\ \eta(Q^{-1}(a+b) & 1+\eta(Q^{-1}b) \end{vmatrix} = \begin{vmatrix} 1 & 0 \\ 1 & 1 \end{vmatrix} = 1.$$

Отсюда, вследствие невырожденности α_o, вытекает невырожденность линейного преобразования α_1.

Лемма 7. Автомат A(η, Q) является перестановочным автоматом.

Доказательство. Легко показывается, что для $x \in X$ отображение $[\alpha_x, \alpha_{x+1}, \eta]$ с невырожденными линейными преобразованиями α_o, α_1 будет взаимно однозначно тогда и только тогда, если $\eta\alpha_o^{-1} = \eta\alpha_1^{-1}$, то есть $\eta\alpha_o^{-1}\alpha_1 = \eta$. Легко проверить, что $\alpha_o^{-1} = Q^{-1} + Q^{-1}a\otimes\eta$. Поэтому

$$\eta\alpha_o^{-1} = \eta Q^{-1}+\eta(Q^{-1}a)\cdot\eta = \eta Q^{-1}+\eta$$

и

$$\eta\alpha_o^{-1}\alpha_1 = (\eta Q^{-1}+\eta)[Q+(Q(a+b)+a+b)\otimes\eta+(Qb+a+b)\otimes\eta Q^{-1}+$$
$$(a+b)\otimes\eta Q]=$$

$$= \eta+\eta Q^{-1}(Q(a+b)+a+b)\cdot\eta+ \eta Q^{-1}(Qb+a+b)\cdot\eta Q^{-1}+$$
$$+\eta Q^{-1}(a+b)\cdot\eta Q+\eta Q+\eta(Q(a+b)+a+b)\cdot\eta+\eta(Qb+a+b)\cdot\eta Q^{-1}+\eta(a+b)\cdot\eta Q=\eta$$

Лемма 8. Отображения $[E, B_o, \eta]$, $[E, B_1, \eta]$

$$[E, B_o, \eta]v = \eta(v)(E+B_o)+v,$$

$$[E, B_1, \eta]v = \eta(v)(E+B_1)+v, \; v\in V_n,$$

при

$$B_0 = E+(a+b)\otimes\eta+b\otimes\eta Q^{-1};$$

$$B_1 = E+a\otimes\eta+b\otimes\eta Q^{-1}$$

взаимно однозначны.

Доказательство. Действительно,

$$\eta(a+b)+1 = 1$$

и

$$\begin{vmatrix} 1+\eta(a) & \eta(b) \\ \eta(Q^{-1}a) & 1+\eta(Q^{-1}b) \end{vmatrix} = \begin{vmatrix} 1 & 0 \\ 1 & 1 \end{vmatrix} = 1.$$

Следовательно, линейные преобразования B_0, B_1 невырождены. Далее,

$$\eta B_0 = \eta+\eta(a+b)\cdot\eta = \eta$$

и

$$\eta B_1 = \eta+\eta(a)\cdot\eta+ \eta(b)\cdot\eta Q^{-1} = \eta,$$

то есть указанные в лемме отображения взаимно однозначны.

Лемма 9. Имеет место равенство

$$[E, B_o, \eta]\,[\alpha_0, \alpha_1, \eta] = Q[E, B_o, \eta],$$

где

$$B_0 = E+(a+b)\otimes\eta+b\otimes\eta Q^{-1}.$$

Доказательство. Действительно, при $v\in V_n$ имеем

$$[E, B_o, \eta]\,[\alpha_0, \alpha_1, \eta]v = (\eta(v)\cdot\eta(\alpha_0+\alpha_1)v+\eta(\alpha_0 v)((E+ B_0)$$
$$(\eta(v)(\alpha_0+\alpha_1)v+\alpha_0 v))+\eta(v)(\alpha_0+\alpha_1)v+\alpha_0 v.$$

Подсчитаем сначала некоторые вспомогательные выражения.

$$\eta\alpha_0 = \eta(Q+a\otimes\eta Q) = \eta(Q);$$

$$\alpha_0+\alpha_1 = (Q(a+b)+a+b)\otimes\eta +(Q(b)+a+b)\otimes\eta Q^{-1}+b\otimes\eta Q;$$

$$\eta(\alpha_0+\alpha_1)=\eta+\eta Q^{-1};$$

$$\eta(v)\cdot\eta((\alpha_0+\alpha_1)v+\eta(\alpha_0 v) = \eta(v)+\eta(v)\cdot\eta(Q^{-1}v)+\eta(Q v);$$

$$(E+B_1)(\eta(v)(\alpha_0+\alpha_1)v+\alpha_0 v) = a(\eta(v)+ \eta(v)\cdot\eta(Q^{-1}v)+\eta(Q v))+ b\cdot\eta(v);$$

$$\eta(v)(\alpha_0+\alpha_1)v+\alpha_0 v = \eta(v)Qa+a\cdot\eta(v)+(Qb)\cdot\eta(Q^{-1}v)\cdot\eta(v)+a\cdot\eta(Q^{-1}v)\cdot\eta(v)+$$
$$+b\cdot\eta(Q^{-1}v)\cdot\eta(v)+b\cdot\eta(Q\,v)\cdot\eta(v)+Qv+\ a\cdot\eta(Qv).$$

Следовательно,

$$[E,\ B_o,\ \eta]\ [\alpha_0,\ \alpha_1,\ \eta] =$$
$$= (\eta(v)+\eta(Q^{-1}v)+\eta(v)+\eta(Qv))\cdot(a(\eta(v)+\eta(v)\cdot\eta(Q^{-1}v)+\eta(Qv))$$
$$+b\cdot\eta(\ v))+(Qa)\cdot\eta(\ v)+b\cdot\eta(v)+a\cdot\eta(v)+\ b\cdot\eta(v)+(Qb)\cdot\eta(Q^{-1}v)\cdot\eta(v)$$
$$+\ a\cdot\eta(Q^{-1}v)\cdot\eta(v)+b\cdot\eta(Q^{-1}v)\cdot\eta(v)+b\cdot\eta(Qv)\cdot\eta(v)+Qv+a\cdot\eta(Qv) =$$
$$= \eta(v)(Qa)+\eta(v)(Qb)+\eta(v)\eta(Q^{-1}v)(Qb)+Qv =$$
$$= \eta(v)(Q(a+b)\otimes\eta+(Qb)\otimes\eta Q^{-1})v+Qv =$$
$$= \eta(v)(Q(E+B_0)v)+Qv=Q\,[E,\ B_o,\ \eta].$$

Таким образом, лемма 9 полностью доказана.

Аналогично доказывается лемма 10.

Лемма 10. Имеет место равенство

$$[E,\ B_1,\ \eta]\ [\alpha_1,\alpha_0,\eta] = Q_1\,[E,\ B_1,\ \eta],$$

где

$$B_1 = E + a\otimes\eta+b\otimes\eta Q^{-1},$$
$$Q_1 = Q+Q(a+b)\otimes\eta+(Qb)\otimes\eta Q^{-1}.$$

Лемма 11. Справедливы равенства

$$c_0(v) = \tilde{c}_0[E,\ B_0,\ \eta](v),$$
$$c_1(v) = \tilde{c}_1[E,\ B_1,\ \eta](v).$$

При любом $v\in V_n$.

Доказательство. Действительно,

$$\tilde{c}_0[E,\ B_0,\ \eta]v = \tilde{c}_0\,(\eta(v)\cdot(E+B_0)v+v) = \eta(x)\cdot\tilde{c}_0(((a+b)\otimes\eta+b\otimes\eta Q^{-1})v)+\tilde{c}_0(v) =$$
$$= \tilde{c}_o(a)\cdot\eta(v)+\tilde{c}_o(v) = c_o(v).$$

Аналогичным образом доказывается и второе равенство.

Лемма 12. Характеристические многочлены $\chi(Q)$, $\chi(Q_1)$ линейных преобразований Q, Q_1 взаимно просты.

Доказательство. Вследствие утверждений лемм 7, 8, 9, линейные преобразования Q, Q_1 невырожденны. Так как многочлен $\chi(Q)$ неприводим, то для доказательства леммы 12 нам достаточно показать, что след (T_r) линейного преобразования Q не равен следу линейного преобразования Q_1. Имеем

$$T_r(Q_1) = T_r(Q)+\ \eta(Q(a+b))+\ \eta(b) = T_r(Q)+1,$$

что и требовалось доказать.

Обозначим через $\overline{A}(\eta,Q) = (F_2, V_n\backslash 0, F_2, ([\alpha_1, \alpha_{x+1}, \eta])_{x\in F_2}, (c_x)_{x\in F_2})$ компоненту автомата

$$A(\eta,Q) = A = (F_2, V_n, F_2, ([\alpha_1, \alpha_{x+1}, \eta])_{x\in F_2}, (c_x)_{x\in F_2}),$$

определенную на множестве $V_n\backslash 0$ ненулевых векторов пространства V_n, а через $A^\wedge = (F_2, V_n\backslash 0, F_2, (Q_x)_{x\in F_2}, (\tilde{c}_x)_{x\in F_2})$ – линейный автомат с частичными функциями переходов $Q_o = Q$, Q_1 и частичными функциями выхода $\tilde{c}_o$, $\tilde{c}_1$.

Согласно доказанным леммам для автоматов $\overline{A}(\eta,Q)$, $A^\wedge$ выполнены все условия теоремы 2, в связи с чем при указанной в теореме 4 входной последовательности P автомат $\overline{A}(\eta,Q)$ является автоматом с гарантированным выходным периодом. Таким образом, теорема 4 полностью доказана.

Список литературы

1. *Алферов А. П., Зубов А. Ю., Кузьмин А. С., Черемушкин А. В.* Основы криптографии. – 2-е изд. – М. : Гелиос АРВ, 2002.
2. *Бабаш А. В.* Верхняя оценка степени различимости связных перестановочных автоматов с заданным диаметром. – Комбинаторно-алгебраические методы в прикладной математике // Межвузовский сборник. – Горький : ГГУ, 1983.
3. *Бабаш А. В.* Запреты автоматов и двоичных функций // Труды по дискретной математике. – М. : Гелиос АРВ, 2006. – Т. 9. Н 40
4. *Бабаш А. В.* Изопериоды выходных последовательностей автономных автоматов // Методы и технические средства обеспечения безопасности информации. – Санкт-Петербург, 2000. – С. 88–90.
5. *Бабаш А. В.* G-изопериод выходной последовательности автономного последовательного соединения автоматов // Тезисы докладов Пятой Международной Петрозаводской конференции. – Т. 7. – Вып. 1. – М. : ТВП, 2000. – С. 87–88.
6. *Бабаш А. В., Шанкин Г. П.* Криптография. – М. : Солон-Пресс, 2007.
7. *Бабаш А. В.* Локальные периоды выходных последовательностей некоторых классов автоматов // Обозрение прикладной и промышленной математики : тезисы докладов Пятой международной петрозаводской конференции. – М. : ТВП, 2000. – Т. 7. – Вып. 1. – С. 88–89.
8. *Бабаш А. В.* О периодичности последовательности состояний автомата, отвечающей его начальному состоянию и входной периодической последовательности // Дискретная математика. – Том 14. – Вып. 2. – Москва, 2002.
9. *Бабаш А. В.* Об одном подходе к линеаризации уравнений получения выходной последовательности векторного автомата // Материалы VII Всероссийского социально-педагогического конгресса «Современное социальное образование: опыт и проблемы модернизации» (8–9 июня 2007). – М. : РГСУ, 2008. – С. 10.
10. *Бабаш А. В.* Приближенные модели конечных автоматов (обзорная работа). – URL: http://www.fssr.ru/icccs/1251/main_publications.html
11. *Бабаш А. В.* Приближенные модели перестановочных автоматов // Дискретная математика. – 1997. – Т. 9. – Вып. 1.

12. *Бабаш А. В.* Слабая автономность конечных автоматов. Обозрение прикладной и промышленной математики // Тезисы докладов Второго Всероссийского симпозиума по прикладной и промышленной математике. – М. : ТВП, 2001. – Т. 8. – Вып. 1. – С. 95–96.

13. *Беркс А. В., Райт Д. Б.* Теория логических сетей // Кибернетический сборник : сб. переводов. Вып. 4 / под ред. А. А. Ляпунова, О. Б. Лупанова, Н. Н. Рикко. – М. : Изд-во иностр. лит-ры, 1962.

14. *Варфоломеев А. А., Жуков А. Е., Пудовкина М. А.* Поточные криптосхемы. Основные свойства и методы анализа стойкости. – М. : Московский государственный инженерно-физический институт (Технический университет), 2000.

15. *Гаврилов Г. П., Сапоженко А. А.* Задачи и упражнения по курсу дискретной математики. – М. : Наука, 1992.

16. *Гилл А.* Введение в теорию конечных автоматов. – М. : Наука, 1966.

17. *Гинсбург С. В.* О длине кратчайшего однородного эксперимента, устанавливающего конечные состояния машины // Кибернетический сборник. – М. : ИЛ, 1961. – № 3. – С. 167–186.

18. *Гринберг В. С.* Детерминизация систем графов и синтез конечных автоматов // Сибирский математический журнал. – 1966. – Т. 7. – № 6. – С. 1259–1267.

19. *Ершов Ю. Л.* О гипотезе В. А. Успенского // Алгебра и логика (семинар). – 1962. – Т. 1. – № 4. – С. 45–48.

20. *Кобринский Н. Е., Трахтенброт Б. А.* Введение в теорию конечных автоматов. – М., 1962.

21. *Коршунов А. Д.* О верхней оценке длин кратчайших однородных экспериментов по распознаванию заключительного состояния для почти всех автоматов // Докл. АН СССР. – 1969. – Т. 184. – № 1. – С. 28–29.

22. *Коршунов А. Д.* О степени различимости конечных автоматов // Дискретный анализ. –1966. – Вып. 6. – С. 35–50.

23. *Коршунов А. Д.* Об асимптотических оценках числа приведенных конечных автоматов // Дискретный анализ. – Вып. 6. – 1966.

24. *Кудрявцев В. Б., Алешин С. В., Подколзин А. С.* Элементы теории автоматов. – М. : МГУ им. М. В. Ломоносова, 1978.

25. *Логачев О. А., Сальников А. А., Ященко В. В.* Некоторые характеристики «нелинейности» групповых отображений // Дискретный анализ и исследование операций. – М., 2001. – Сер. 1. – Т. 8. – № 1. – С. 40–54.

26. *Лупанов О. Б.* О сравнении двух типов конечных источников // Проблемы кибернетики. – М. : Физмат-гиз, 1963. – Т. 9. – С. 321–326.

27. *Мур Э. Ф.* Умозрительные эксперименты с последовательными машинами // Автоматы : сб. статей. – М. : ИЛ, 1956. – С. 179–210.

28. *Подколзин А. С.* О сложности распознавания автоматов-генераторов // Дискретный анализ : сборник. – Вып. 21. – Новосибирск,1972. – С. 31–36.

29. *Романовский В. И.* Дискретные цепи Маркова. – М.-Л. : Гостехиздат, 1949.

30. *Солодовников В. И.* О полугруппе, порожденной автоматными отображениями обратимого автомата // Труды по дискретной математике. – 2001. – № 4. – С. 231–242.

31. *Сумароков С. Н.* Запреты двоичных функций и обратимость для одного класса кодирующих устройств // Обозрение прикладной и промышленной математики, сер. «Дискретная математика». – 1994. – Т 1. – Вып. 1. – С. 33–55.

32. *Супруненко Д. А.* Группы матриц. – М. : Наука, 1972. Н 24

33. *Трахтенброт В. А., Барздинь Я. М.* Конечные автоматы (поведение и синтез). – М. : Наука, 1970.

34. *Фомичев В. М.* Дискретная математика и криптология. – М. : Диалог-МИФИ, 2003.

35. *Яблонский С. В.* Введение в дискретную математику. – М. : Наука, 1979.

36. *Atkinson M. D.* An Algorithm for Finding the Blocks of Permutation Group // Mathematics of computation. – July 1975. – V. 29. – N 131. – P. 911–913.

37. *Babash A. V.* Isoperiods of output sequences of automata Probabilistic Methods in Discrete Mathematics. – Utrecht : VSP, 2002.

38. *Gill A.* Reduced form if linear automation, Automation theory, 1966.

39. *Golomb S. W.* Shift register sequences // Holden-Day series in information systems. – 1967.

40. *Hartmanis I., Stearns R. E.* Algebraic ctructure theory of sequential machines. – Toronto, 1966.

41. *Hibbard T. H.* Least Upper Bounds on Minimal Terminal State Experiments for Two Classes of Sequential Machines // J. Assoc Comput. – 1961. – Vol. 8. – P. 601–612.

42. *Huffman D. A.* Canonical forms for information-lossless finitestate logical machines // IRE Trans. Circuit Theory. Special supplement. – 1959. – Vol. 6. – P. 41–59.

43. *Majewski W., Albicki A.* Algebraiczna teoria automatow. – Warszawa : Wydawnictwa Naukowo-Techniczne, 1980.

44. *Preparata F. P.* Convolutional Transformations of Binary Sequences: Boolean Functions and Their Resynchronizing Properties // IEEE Transactions on Electronic Computers. – 1966. – Vol. 15. – N 6. – P. 398–909.

45. *Rose G. F.* Output completeness in sequential machines // Proceedings of the American Mathematical Society. – 1962. – Vol. 13. – N 4. – P. 611–614.

Учебное издание

БАБАШ Александр Владимирович

ТЕОРИЯ АВТОМАТОВ.
СИНТЕЗ ШИФРУЮЩИХ АВТОМАТОВ

Учебное пособие

Редактор *Н. В. Пятосина*
Оформление обложки *Ю. С. Жигалова*

Подписано в печать 21.10.2020. Формат 60x84 1/16.
Усл. печ. л. 21,75. Уч.-изд. л. 24,61. Тираж 100 экз. Заказ .

ФГБОУ ВО «РЭУ им. Г. В. Плеханова».
117997, Москва, Стремянный пер., 36.
Напечатано в ФГБОУ ВО «РЭУ им. Г. В. Плеханова».
117997, Москва, Стремянный пер., 36.