В. А. Давыдов, Коды для исправления дефектов, *Пробл. передачи информ.*, 1993, том 29, выпуск 1, 99–104

ПРОБЛЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

Том 29 1993 Вып. 1

КРАТКИЕ СООБЩЕНИЯ

УДК 621.391.15

© 1993 г. В.А. Давыдов

КОДЫ ДЛЯ ИСПРАВЛЕНИЯ ДЕФЕКТОВ

Предлагается новая конструкция аддитивных кодов и универсальных тестов. Для заданных параметров строятся лучшие коды и тесты в классе известных.

§ 1. Введение

Рассмотрим двоичную матрицу $\mathcal{A}$, состоящую из M строк и N столбцов. Будем называть такую матрицу согласованной с t дефектами и обозначать через $\mathcal{A}(t, N, M)$, если подматрица, составленная из любых различных t столбцов $\mathcal{A}$, содержит в своих строках все 2^t двоичных векторов длины t. В работах [1, 2] матрица $\mathcal{A}(t, N, M)$ называется (N, t)-тестом, а число $M = M(t, N)$ строк такой матрицы – объемом t-теста длины N.

Матрица $\mathcal{A}(t, N, M)$ является аддитивным кодом длины N с исправлением t дефектов, если содержит подматрицу из r столбцов, все строки которой различны. Такая подматрица называется контрольной [3]. Наличие r столбцов контрольной подматрицы в матрице, согласованной с t дефектами, обозначим $\mathcal{A}^r(t, N, M)$. Величину $r = r(t, N)$ будем называть избыточностью аддитивного кода длины N, исправляющего t дефектов.

Проблема заключается в построении матрицы $\mathcal{A}(t, N, M)$ с минимальным числом строк M или кода $\mathcal{A}^r(t, N, M)$ с минимальной избыточностью r. В работе [1] показывается, что с полиномиальной сложностью могут быть получены аддитивные коды, исправляющие t дефектов, избыточность которых оценивается неравенством

$$r(t,N) \leqslant \log_2\log_2 N + \log_2 k + 1,$$

а также матрицы, согласованные с t дефектами, с числом строк

$$M(t,N) = k\log_2 N,$$

где

$$k < 2^{t\log_2 t} t^5 / (4\log_2 t)$$

если задана оптимальная матрица $\mathcal{A}(t, t^2, m)$. Данная конструкция является асимптотически оптимальной. Однако для конечных значений величины N большую роль в оценках $M(t, N)$ и $r(t, N)$ начинает играть величина константы k. Таким образом, остается актуальной задача улучшения оценок $M(t, N)$ и $r(t, N)$ для конкретных значений N и t.

В качестве одного из примеров решения этой задачи может быть приведен итеративный алгоритм построения матриц, согласованных с t дефектами, для $t = \text{const}$ [2]. В результате f-кратного применения этого алгоритма к матрице $\mathcal{A}(t, n, m)$ получим матрицу $\mathcal{A}(t, N, M)$, для параметров которой выполняются неравенства

$$M(t,N) < m\left(t^2\alpha\log_2\varepsilon/2\right)^f \log_2 N/\log_2 n, \tag{1}$$

где $\alpha = 1{,}25506$, $\varepsilon = 2{,}71828$. При этом число n_{i+1} столбцов матрицы, полученной после i шагов алгоритма, связано с числом n_i столбцов матрицы, полученной на предыдущем шаге, следующим неравенством

$$n_{i+1} \geq 1 + \left\lfloor 2^{n_i/2\left\lfloor t^2/4\right\rfloor}\right\rfloor. \tag{2}$$

Настоящая работа содержит итеративный алгоритм построения аддитивных кодов и матриц, согласованных с t дефектами, для $t = \text{const}$. Данный алгоритм позволяет получить лучшую оценку для $M(t, N)$ по сравнению с оценкой, приведенной в [2]. Величина $r(t, N)$ для кодов, полученных по этому алгоритму, меньше избыточности конкретных конструкций, приводимых в [1].

§ 2. Матрицы, согласованные с t дефектами

Обозначим произвольную q-ичную матрицу $\mathcal{B}$, состоящую из N столбцов и M строк, через $\mathcal{B}_l[q, N, M]$. Нижний индекс l обозначает, что два любых столбца матрицы совпадают не более чем в l позициях. Пусть заданы двоичный вектор $\mathbf{L}$ длины s и матрица $\mathcal{B}_l[2, s, M]$. Перенумеруем столбцы $\mathcal{B}_l[2, s, M]$ и позиции $\mathbf{L}$ от 1 до s. Будем говорить, что матрица $\mathcal{B}_l[2, s, M]$ связана с вектором $\mathbf{L}$ тогда и только тогда, когда матрица не содержит одинаковых столбцов под номерами, где вектор имеет различные символы.

Л е м м а 1. *Пусть* $\mathcal{B}_l[2, s, M]$ *составлена из столбцов матрицы* $\mathcal{A}(t, N, M)$ *и связана с двоичным вектором* $\mathbf{L}$ *длины* $s \leq t$. *Тогда* $\mathcal{B}_l[2, s, M]$ *содержит* $\mathbf{L}$ *в одной из строк.*

Д о к а з а т е л ь с т в о. Пусть матрица $\mathcal{B}_l[2, s, M]$ содержит z различных столбцов. Множество номеров, под которыми такие столбцы расположены, обозначим $\mathcal{F} = \{f_1, f_2, \ldots, f_z\}$. Построим из различных столбцов $\mathcal{A}(t, N, M)$ матрицу $C_u[2, s, M]$ такую, что в столбцах, расположенных под номерами из множества $\mathcal{F}$, $C_u[2, s, M]$ совпадает с $\mathcal{B}_l[2, s, M]$. По построению $C_u[2, s, M]$ и из условия $s \leq t$ получаем, что существует строка этой матрицы, содержащая вектор $\mathbf{L}$.

Пусть $\mathcal{P}$ – дополнение $\mathcal{F}$ до множества $\{1, 2, \ldots, s\}$. Заменим $p_i \in \mathcal{P}$ столбец матрицы $C_u[2, s, M]$ на p_i-й столбец $\mathcal{B}_l[2, s, M]$. Из связанности $\mathcal{B}_l[2, s, M]$ с вектором $\mathbf{L}$ следует, что такая замена не изменит строку $C_k[2, s, M]$, содержащую $\mathbf{L}$. Заменим оставшиеся столбцы $C_u[2, s, M]$ под номерами из множества $\mathcal{P}$ на соответствующие столбцы $\mathcal{B}_l[2, s, M]$. В результате, во-первых, приведем $C_u[2, s, M]$ к виду $\mathcal{B}_l[2, s, M]$. Во-вторых, сохраним строку $C_u[2, s, M]$, содержащую $\mathbf{L}$, что и требовалось доказать.

Пусть $\mathbf{Z}$ и $\mathbf{L}$ – q-ичный и двоичный векторы длины s. Будем говорить, что $\mathbf{Z}$ связан с $\mathbf{L}$ тогда и только тогда, когда $\mathbf{Z}$ не содержит одинаковых элементов на тех позициях, где $\mathbf{L}$ имеет различные символы.

Л е м м а 2. [1] *Пусть задан двоичный вектор* $\mathbf{L}$ *длины* s *и матрица* $\mathcal{B}_l[q, N, M]$ *такая, что* $M > s^2 l/4$ *для четных* s *и* $M > (s^2 - 1)l/4$ *для нечетных. Тогда в подматрице* $\mathcal{D}_l[q, s, M]$, *составленной из* s *различных столбцов* $\mathcal{B}_l[q, N, M]$, *найдется строка, содержащая вектор, связанный с* $\mathbf{L}$.

Пусть заданы матрицы $\mathcal{A}(t, n, m)$ и $\mathcal{B}_l[q, N, M]$ такие, что $q \leqslant n$. Поставим в соответствие каждому из q элементов матрицы $\mathcal{B}_l[q, N, M]$ свой столбец из $\mathcal{A}(t, n, m)$. Используя метод, описанный в [4, 5], произведем замену всех q-ичных символов матрицы $\mathcal{B}_l[q, N, M]$ на соответствующие им столбцы. Описанную процедуру назовем операцией расширения матрицы $\mathcal{A}(t, n, m)$ матрицей $\mathcal{B}_l[q, N, M]$. Полученную в результате матрицу, состоящую из N столбцов и Mm строк, будем называть расширенной и обозначать $\mathcal{A}(t, n, m) * \mathcal{B}_l[q, N, M]$.

Т е о р е м а 1. *Пусть заданы матрицы* $\mathcal{A}(t, n, m)$ *и* $\mathcal{B}_l[q, N, M]$ *такие, что* $M > t^2 l/4$. *Тогда* $\mathcal{A}(t, n, m) * \mathcal{B}_l[q, N, M] = \mathcal{A}(t, N, Mm)$.

Д о к а з а т е л ь с т в о. Из утверждения леммы 2 имеем, что в произвольной подматрице, составленной из t различных столбцов $\mathcal{B}_l[q, N, M]$, найдется строка, содержащая q-ичный вектор длины t, связанный с произвольным двоичным вектором $\mathbf{L}$ той же длины. В результате операции расширения такая строка преобразуется в двоичную подматрицу, состоящую из t столбцов и m строк, связанную с вектором $\mathbf{L}$. Полученная подматрица, по утверждению леммы 1, содержит вектор $\mathbf{L}$ в одной из строк. Следовательно, любые t столбцов расширенной матрицы образуют подматрицу, содержащую в своих строках произвольный двоичный вектор. Что и требовалось доказать.

Пусть $\mathfrak{J}(M, t, q, m)$ – набор M в общем случае различных матриц, каждая из которых состоит из q столбцов, m строк и согласована с t дефектами. Обозначим j-ю матрицу такого набора через $\mathcal{A}_j(t, q, m)$, где $1 \leqslant j \leqslant M$. Перенумеруем столбцы матрицы $\mathcal{A}_j(t, q, m)$ от 1 до q, а строки матрицы $\mathcal{B}_l[q, N, M]$ от 1 до M. Поставим в соответствие i-му элементу j-й строки $\mathcal{B}_l[q, N, M]$ i-й столбец $\mathcal{A}_j(t, n, m)$ из набора $\mathfrak{J}(M, t, q, m)$. Операцию замены элементов матрицы $\mathcal{B}_l[q, N, M]$ на соответствующие им столбцы набора назовем расширением набора $\mathfrak{J}(M, t, q, m)$ матрицей $\mathcal{B}_l[q, N, M]$. Полученную в результате такой операции матрицу будем называть расширенной и обозначать $\mathfrak{J}(M, t, q, m) * \mathcal{B}_l[q, N, M]$.

С л е д с т в и е. *Пусть заданы* $\mathfrak{J}(M, t, q, m)$ *и* $\mathcal{B}_l[q, N, M]$ *такие, что* $M > t^2 l/4$, *тогда* $\mathfrak{J}(M, t, q, m) * \mathcal{B}_l[q, N, M] = \mathcal{A}(t, N, Mm)$.

§ 3. Аддитивные коды, исправляющие t дефектов

В этом параграфе обсуждается модификация алгоритма построения расширенной матрицы, позволяющая получать в этой матрице контрольную подматрицу.

Л е м м а 3. *Пусть матрица* $C_l[2, q, m]$ *получена из* $\mathcal{A}(t, q, m)$ *путем инвертирования заданных* s *столбцов* $(1 \leqslant s \leqslant q)$. *Тогда* $C_l[2, q, m] = C(t, q, m)$.

Д о к а з а т е л ь с т в о. Объединим t различных столбцов $\mathcal{A}(t, q, m)$ в матрицу $\mathcal{D}(t, t, m)$. Из свойства согласованности матрицы с t дефектами следует, что $\mathcal{D}(t, t, m)$ содержит подматрицу $\mathcal{F}(t, t, 2^t)$, состоящую из различных строк длины t. Пусть при преобразовании $\mathcal{A}(t, q, m)$ в $C_l[2, q, m]$ инвертировались некоторые столбцы матрицы $\mathcal{D}(t, t, m)$, а значит и соответствующие столбцы подматрицы $\mathcal{F}(t, t, 2^t)$. Такое преобразование $\mathcal{F}(t, t, 2^t)$ может привести лишь к перестановке ее строк. Следовательно, любые t столбцов $C_l[2, q, m]$ содержат подматрицу, составленную из 2^t различных строк. Что и требовалось доказать.

Пусть задана матрица $\mathcal{A}'(t, q, m)$, содержащая контрольную подматрицу в первых r столбцах. Будем считать, что q – степень простого числа. Тогда существует q-ичный расширенный код Рида–Соломона с k информационными символами, содержащий единичное слово. Выпишем слова этого кода в виде строк матрицы $\mathcal{B}_{k-1}[q, q^k, q]$ и назовем полученную матрицу кодовой матрицей. Зададим натуральное число z такое, что

$$r + z \leqslant q, \tag{3}$$

$$t^2(k-1)/4 < 2^z \leqslant q. \tag{4}$$

Объединим произвольные 2^z строк кодовой матрицы $\mathcal{B}_{k-1}[q, q^k, q]$ в матрицу $\mathcal{B}_{k-1}[q, q^k, 2^z]$. Переставим ее столбцы таким образом, чтобы любая строка полученной матрицы начиналась с последовательности 1, 2, 3, ..., q. Такая перестановка возможна, так как расширенный код Рида–Соломона содержит единичное слово. Перенумеруем строки матрицы $\mathcal{B}_{k-1}[q, q^k, 2^z]$ от 0 до $2^z - 1$, а столбцы матрицы $\mathcal{A}^r(t, q, m)$ от 1 до q. Пусть $\{\mathbf{L}_0, ..., \mathbf{L}_{2^z-1}\}$ – множество двоичных векторов длины q, позиции которых перенумерованы от 1 до q. Будем считать, что вектор $\mathbf{L}_j$ содержит на позициях $r + 1, r + 2, ..., r + z$ двоичное представление числа $j (0 \leqslant j \leqslant 2^z - 1)$, а на оставшихся позициях нули. Пусть i-му столбцу матрицы $\mathcal{A}^r(t, q, m)$ соответствует i-я позиция вектора $\mathbf{L}_j$, $0 \leqslant j \leqslant 2^z - 1$. Для каждого вектора $\mathbf{L}_j$ определим матрицу, полученную из $\mathcal{A}^r(t, q, m)$ путем инвертирования тех столбцов, которым соответствуют единичные позиции вектора $\mathbf{L}_j$. По утверждению леммы 3 все такие матрицы согласованы с t дефектами и, следовательно, образуют набор $\mathfrak{J}(2^z, t, q, m)$.

Т е о р е м а 2. *Матрица, полученная в результате расширения набора* $\mathfrak{J}(2^z, t, q, m)$ *матрицей* $\mathcal{B}_{k-1}[q, q^k, 2^z]$, *согласована с* t *дефектами и в первых* $z + r$ *столбцах содержит контрольную подматрицу, т.е.* $\mathfrak{J}(2^z, t, q, m) * \mathcal{B}_{k-1}[q, q^k, 2^z] = \mathcal{A}^{r+z}(t, q^k, m2^z)$.

Д о к а з а т е л ь с т в о. 1. Число строк $\mathcal{B}_{k-1}[q, q^k, 2^z]$, согласно неравенству (4), удовлетворяет условию следствия теоремы 1. Таким образом, расширенная матрица $\mathfrak{J}(2^z, t, q, m) * \mathcal{B}_{k-1}[q, q^k, 2^z]$ согласована с t дефектами.

2. Пусть двоичный вектор $\mathbf{F}_{ij}$ длины $r + z$ содержит первые $r + z$ позиций i-й строки j-й матрицы набора $\mathfrak{J}(2^z, t, q, m)$, где $1 \leqslant i \leqslant m$, $0 \leqslant j \leqslant 2^z - 1$. Из построения набора следует, что все матрицы набора содержат одинаковые первые r столбцов, образующих контрольную подматрицу. Следовательно, $\mathbf{F}_{ij} \neq \mathbf{F}_{lk}$, если $i \neq l$. Из неравенства (3) вытекает, что каждая матрица набора получена из $\mathcal{A}^r(t, q, m)$ путем инвертирования столбцов, расположенных под номерами от $r + 1$ до $r + z$. Следовательно, $\mathbf{F}_{ij} \neq \mathbf{F}_{ik}$, если $j \neq k$. Таким образом, $\mathbf{F}_{ij} = \mathbf{F}_{lk}$ тогда и только тогда, когда $i = l$ и $j = k$. Каждая строка $\mathcal{B}_{k-1}[q, q^k, 2^z]$ начинается с последовательности 1, 2, ..., q. Следовательно, расширенная матрица в первых q столбцах содержит все 2^z матриц набора. Подматрица, составленная из первых $r + z$ столбцов расширенной матрицы, содержит в своих строках векторы $\mathbf{F}_{ij}$. Такие векторы различны. Таким образом, эта подматрица является контрольной. Что требовалось доказать.

Итак, при условии выполнения для $\mathcal{A}^r(t, q, m)$ неравенств (3) и (4), построение аддитивного кода $\mathcal{A}^{r+z}(t, q^k, m2^z)$ эквивалентно построению матрицы, согласованной с t дефектами.

§ 4. Оценка числа строк матриц, согласованных с t дефектами

Пусть заданы матрицы $\mathcal{A}(t, q, m)$ и $\mathcal{B}_{k-1}[q, q^k, q]$, параметры которых удовлетворяют неравенству $q > (k - 1)t^2/4$. Будем считать, что одна из строк $\mathcal{A}(t, q, m)$ состоит из одних нулей. Если это не так, что по утверждению леммы 3 всегда можно инвертировать любые столбцы $\mathcal{A}(t, q, m)$, сохраняя свойство согласованности матрицы с t дефектами. Тогда по теореме 1 получим расширенную матрицу $\mathcal{A}(t, q^k, mq)$, содержащую q нулевых строк. Удалив $q-1$ нулевую строку, перейдем к $\mathcal{A}(t, q^k, (m-1)\, q+1)$. Используем построенную матрицу в качестве исходной для следующего расширения. Обозначим матрицу, полученную после i-го расширения, через $\mathcal{A}(t, q_{i+1}, m_{i+1})$. Рассмотрим зависимость между параметрами матриц $\mathcal{A}(t, q_i, m_i)$ и $\mathcal{A}(t, q_{i+1}, m_{i+1})$. Пусть для i-го расширения использовалась матрица $\mathcal{B}_{k_i-1}[q_i, q_i^{k_i}, q_i]$. Из метода построения

$\mathcal{A}(t, q^k, (m-1)\,q+1)$ следует, что

$$q_{i+1} = q_i^{k_i}, \tag{5}$$

$$m_{i+1} = (m_i - 1)q_i + 1. \tag{6}$$

Для согласованности матрицы, полученной после i-го расширения с t дефектами, k_i можно выбрать равным

$$k_i = \lceil q_i 4 / t^2 \rceil, \tag{7}$$

где $\lceil x \rceil$ – ближайшее целое $\geqslant x$. Выразим q_{f+1} и m_{f+1} через параметры матрицы $\mathcal{A}(t, q_1, m_1)$, используемой для первого расширения

$$q_{f+1} = q_1^{\lceil q_1 4/t^2 \rceil \lceil q_2 4/t^2 \rceil \cdot \ldots \cdot \lceil q_i 4/t^2 \rceil}, \tag{8}$$

$$m_{f+1} = (m_1 - 1)q_1 q_2 \cdot \ldots q_i + 1. \tag{9}$$

Обозначим $q_{f+1} = N$, $m_{f+1} = M$, $q_1 = n$, $m_1 = m$. Тогда из (8) и (9) получаем

$$M < 1 + (m-1)(t^2/4)^f \log_2 N / \log_2 n, \tag{10}$$

где f – число шагов алгоритма. Сравнивая (1) с (10) и (2) с (5) и (7), получаем, что матрицы, согласованные с t дефектами и построенные по теореме 1, содержат меньшее число строк, чем матрицы, полученные в работе [2] при прочих равных условиях.

§ 5. Параметры аддитивных кодов

Пусть задан аддитивный код $\mathcal{A}^r(t, n, m)$, у которого параметры удовлетворяют неравенствам (3), (4) и n – степень двойки. Тогда число R проверочных символов аддитивного кода, полученного в результате f расширений $\mathcal{A}^r(t, n, m)$, оценивается неравенством

$$R < r + f \log_2(t^2/4) + \log_2(\log_2 N / \log_2 n).$$

В результате каждого расширения получается аддитивный код с контрольной подматрицей, построенной способом, описанным в § 3. Параметры R, $\log_2 N$, t построенных аддитивных кодов $\mathcal{A}^r(t, N, M)$ приведены в таблице. Параметры стартовых матриц, полученных из [3], помечены символом "*".

$t=3$	R	4*	5*	6	7	8	9	10	11	12
	$\log_2 N$	3*	5*	6	12	20	40	80	96	192
	R	9*	11*	12	13	15	16	17	18	19
$t=5$	$\log_2 N$	4*	5*	8	12	15	30	48	88	176
	R	11*	15	19	20	21	22	23	27	28
$t=7$	$\log_2 N$	4*	8	16	24	48	88	176	352	688
	R	21*	26	31	32	33	34	35	36	
$t=11$	$\log_2 N$	5*	10	20	30	50	90	180	350	
	R	34*	40	46	47	48	49	50	51	52
$t=13$	$\log_2 N$	6*	12	24	48	84	156	300	588	1176

Сравнение данных таблицы с параметрами кодов, приведенными в работе [1], позволяет сделать вывод, что для рассмотренных значений N и t коды, построенные по теореме 2, обладают меньшей избыточностью, чем коды в [1].

СПИСОК ЛИТЕРАТУРЫ

1. *Dumer I.I.* On constructing optimal tests and defect – correcting codes // IEEE Int. Sympos. Inform. Theory. Budapest, 1991. P. 313.
2. *Seroussi G. and Bshouty N.H.* Vector Sets for Exhaustive Testing of Logic Circuits // IEEE Trans. Inform. Theory. 1988. V. 34. P. 513–522.
3. *Конопелько В.И., Лосев В.В.* Надежное хранение информации в полупроводниковых запоминающих устройствах. М.: Радио и связь, 1986.
4. *Кауц В., Синглтон Р.* Двоичные дизъюнктивные коды // Кибернетический сб. М.: Мир, 1986. С. 153–187.
5. *Poljak S., Pultr A., Rodl V.* On Qualitatively Independent Partitions and Related Problems // Discrete Applied Math. 1983. V. 6. P. 193–205.

Поступила в редакцию
15.07.91
После переработки
31.07.92