

Math-Net.Ru

Общероссийский математический портал

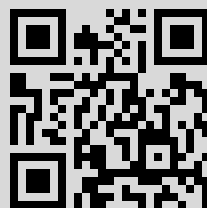
В. А. Давыдов, Коды, исправляющие ошибки в модульной метрике, метрике Ли и ошибки оператора, *Пробл. передачи информ.*, 1993, том 29, выпуск 3, 10–20

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением
<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 92.242.58.13

31 октября 2018 г., 10:13:30



УДК 621.391.15

© 1993 г. В. А. Давыдов

**КОДЫ, ИСПРАВЛЯЮЩИЕ ОШИБКИ В МОДУЛЬНОЙ МЕТРИКЕ,
МЕТРИКЕ ЛИ И ОШИБКИ ОПЕРАТОРА**

Приводится метод построения кодов с асимптотически минимальной избыточностью, исправляющих t ошибок в модульной метрике. Вводится понятие гомоморфизма метрик и показывается гомоморфность перестановочной метрики и метрики Ли модульной метрике. В указанных метриках строятся новые семейства кодов.

§ 1. Введение

Необходимость использования модульной метрики для описания канала передачи информации с аддитивным гауссовским шумом возникает в том случае, если в канале применяется амплитудная модуляция. Коды длины $n = p^m - 1$, исправляющие $t < p$ ошибок в модульной метрике, где p – основание кода, были построены Дарьяном [1]. Коды, исправляющие ошибки большого веса в модульной метрике и допускающие мажоритарное декодирование, рассматривались Мазуром в [2]. Сравнение параметров указанных кодов затруднено тем, что коды Дарьяна существуют только для больших скоростей передачи, а коды Мазура являются низкоскоростными.

К числу наиболее типичных ошибок, возникающих в процессе общения человека с машиной, можно отнести перестановки соседних символов. В теории кодирования такие ошибки обычно называют ошибками оператора. Коды, корректирующие ошибки этого вида, рассматривались в работах ряда авторов. Касами [3] построил класс кодов, исправляющих одиночные ошибки оператора. Геворкяном [4] построены коды с исправлением фазированных ошибок оператора. Наиболее полный обзор результатов по данной области приводится в [5].

Метрика Ли применяется для описания каналов с фазовой модуляцией и аддитивным гауссовским шумом. Негациклические коды, исправляющие в метрике Ли ошибки веса $t \leq (p-1)/2$, где p – основание кода, были построены Берлекэмпом [6]. Дарьян [7] рассмотрел декодирование кодов БЧХ в метрике Ли при $t \leq (p-1)/2$, а также построение кодов, исправляющих одиночные ошибки. Мазур [2] построил широкий класс констациклических кодов с мажоритарным декодированием, исправляющих ошибки большого веса.

В §2 рассматривается класс высокоскоростных кодов, являющийся обобщением кодов Дарьяна и включающий их в себя в виде подкласса. В §3 вводится понятие метрики ρ , гомоморфной модульной метрике, позволяющее получать коды для ρ , используя коды в модульной метрике. Оценкам мощности кодов в метрике ρ посвящен §4. Как частный случай таких оценок получают границы мощности для кодов в модульной метрике. В §§5,6 показывается, что метрика перестановок соседних символов, описывающая канал ошибок оператора, и метрика Ли являются метриками, гомоморфными модульной метрике. На основе этого факта строятся новые классы кодов в указанных метриках.

§ 2. Коды для модульной метрики

Пусть $A = \{0, 1, \dots, Q-1\}$ – Q -ичный алфавит. Определим A^n как множество Q -ичных векторов длины n .

$$A^n = \{u = (u_1, u_2, \dots, u_n), u_i \in A, 1 \leq i \leq n\}.$$

Расстояние в модульной метрике $d_M(u, v)$ между двумя векторами $u, v \in A^n$ вычисляется по формуле [1]

$$d_M(u, v) = \sum_{i=1}^n |u_i - v_i|. \quad (1)$$

Вес $w_M(u)$ вектора u в модульной метрике определяется как расстояние $d_M(u, 0)$, где 0 – нулевой вектор. Таким образом,

$$w_M(u) = \sum_{i=1}^n u_i.$$

Если $d_M(u, v) = e$, то будем говорить, что вектор u получен e ошибками из вектора v , или наоборот, вектор v получен e ошибками из u .

Введем отношения порядка на множестве векторов A^n . Обозначим $u \geq v$, если для всех $1 \leq i \leq n$ выполняется неравенство $u_i \geq v_i$. В том случае, если указанное неравенство выполнено не для всех i , назовем u и v не сравнимыми векторами и обозначим это $u \not\leq v$. Пусть $d_M(u, v) = e$ и выполняется условие $u \geq v$ ($u \leq v$). Тогда будем говорить, что вектор u получен из вектора v путем e однонаправленных увеличивающихся (уменьшающихся) ошибок.

Множество слов $\mathcal{A} \subset A^n$ называется кодом, исправляющим t однонаправленных увеличивающих (уменьшающих) ошибок, если для любой пары различных векторов $u, v \in \mathcal{A}$ не существует вектор $c \in A^n$ такого, что

$$c \geq u, c \geq v, (c \leq u, c \leq v), \quad (2)$$

$$d_M(c, u) \leq t, d_M(c, v) \leq t. \quad (3)$$

Выберем конечное поле $GF(q)$, $q \neq p^m$, где p – простое число, m – натуральное число и $q > n$. В дальнейшем такое поле будем обозначать F . Определим отображение множества Q -ичных векторов длины n в множество полиномов от формальной переменной x над полем F . Для этого поставим в соответствие i -й позиции ($1 \leq i \leq n$) векторов множества A^n ненулевой элемент a_i поля F . Из неравенства $q > n$ следует, что такое сопоставление возможно. Множество выбранных элементов $\mathcal{L} = \{a_1, a_2, \dots, a_n\}$, будем называть множеством локаторов кодовых позиций, а сами элементы a_i – локаторами. Определим отображение $\mathfrak{Z}_{\mathcal{L}}$ вектора $u = (u_1, u_2, \dots, u_n)$ в многочлен $u(x)$ по правилу

$$\mathfrak{Z}_{\mathcal{L}}(u) = u(x) = \prod_{i=1}^n (1 - x\alpha_i^{-1})^{u_i}. \quad (4)$$

Многочлен $u(x)$, соответствующий вектору $u \in A^n$, будем называть локаторным многочленом вектора u .

Отображение $\mathfrak{Z}_{\mathcal{L}}$ обладает следующим элементарным свойством. Если векторы $u, v, e \in A^n$ связаны соотношением

$$u = v + e,$$

т.е. для компонент этих векторов выполняется условие $u_i = v_i + e_i$, $1 \leq i \leq n$, то справедливо тождество

$$\mathfrak{Z}_{\mathcal{L}}(\mathbf{u}) = \mathfrak{Z}_{\mathcal{L}}(\mathbf{v})\mathfrak{Z}_{\mathcal{L}}(\mathbf{e}).$$

Заметим, что для любых $\mathbf{u}, \mathbf{v}$ выполняется равенство

$$\mathfrak{Z}_{\mathcal{L}}(\mathbf{u}) \equiv \mathfrak{Z}_{\mathcal{L}}(\mathbf{v}) \equiv 1 \pmod{x}.$$

Обозначим через $F[x]$ кольцо многочленов от формальной переменной x над полем F . Пусть $s(x) \in F[x]$ – многочлен степени меньше или равной t , младший коэффициент которого равен 1. Определим множество векторов $\mathcal{A} = \mathcal{A}(\mathcal{L}, n, s)$ следующим образом:

$$\mathcal{A} = \{\mathbf{u} | \mathbf{u} \in A^n, \mathfrak{Z}_{\mathcal{L}}(\mathbf{u}) \equiv s(x) \pmod{x^{t+1}}\}. \quad (5)$$

Т е о р е м а 1. *Множество векторов $\mathcal{A}$ является кодом, исправляющим t однонаправленных увеличивающих ошибок.*

Д о к а з а т е л ь с т в о. Предположим, что слова $\mathbf{v}, \mathbf{u} \in \mathcal{A}$ различны, а $\mathbf{e}_1, \mathbf{e}_2$ – векторы увеличивающих ошибок, вес каждого из которых не превосходит t . Пусть существует слово $\mathbf{c}$, удовлетворяющее условиям (2) и (3), которое может быть получено путем сложения слова $\mathbf{v}$ с вектором ошибок $\mathbf{e}_1$ и слова $\mathbf{u}$ с вектором ошибок $\mathbf{e}_2$. Тогда имеют место следующие соотношения:

$$c(x) = v(x)e_1(x) \equiv s(x)e_1(x) \pmod{x^{t+1}},$$

$$c(x) = u(x)e_2(x) \equiv s(x)e_2(x) \pmod{x^{t+1}},$$

где $u(x) = \mathfrak{Z}_{\mathcal{L}}(\mathbf{u})$, $e_1(x) = \mathfrak{Z}_{\mathcal{L}}(\mathbf{e}_1)$, $v(x) = \mathfrak{Z}_{\mathcal{L}}(\mathbf{v})$, $e_2(x) = \mathfrak{Z}_{\mathcal{L}}(\mathbf{e}_2)$, $c(x) = \mathfrak{Z}_{\mathcal{L}}(\mathbf{c})$. Следовательно, выполняется тождество

$$s(x)e_1(x) \equiv s(x)e_2(x) \pmod{x^{t+1}},$$

после преобразования которого получим

$$e_1(x) - e_2(x) \equiv 0 \pmod{x^{t+1}}. \quad (6)$$

Степени полиномов $e_1(x)$ и $e_2(x)$ равны весу векторов $\mathbf{e}_1$ и $\mathbf{e}_2$ соответственно и, следовательно, не превосходят t . Тогда из (6) получаем, что

$$e_1(x) = e_2(x) = e(x).$$

Учитывая, что для отличающихся друг от друга $\mathbf{u}, \mathbf{v} \in A^n$ выполняется неравенство $u(x) \neq v(x)$, имеем

$$u(x)e(x) \neq v(x)e(x).$$

Таким образом, получили факт, противоречащий предположению о существовании слова $\mathbf{c}$, удовлетворяющего условиям (2) и (3). Следовательно, такого слова не существует, и множество слов $\mathcal{A}$ является кодом, исправляющим t увеличивающих ошибок. Что и требовалось доказать.

С л е д с т в и е 1. *Код $\mathcal{A}$, исправляющий t увеличивающих ошибок, является кодом, исправляющим t уменьшающих ошибок.*

Д о к а з а т е л ь с т в о. Предположим, что существует слово $\mathbf{c}$ длины n , получаемое путем прибавления к слову $\mathbf{v} \in \mathcal{A}$ вектора $\mathbf{e}$ и путем прибавления к слову $\mathbf{u} \in \mathcal{A}$ вектора $\mathbf{f}$, где $\mathbf{e} = (e_1, e_2, \dots, e_n)$ и $\mathbf{f} = (f_1, f_2, \dots, f_n)$ – векторы уменьшающих ошибок, вес каждого из которых не превосходит t . Заметим, что для компонент векторов $\mathbf{e}$ и $\mathbf{f}$ выполняются неравенства $e_i \leq 0$, $f_i \leq 0$, $1 \leq i \leq n$. Пусть $\mathbf{g} =$

$= (g_1, g_2, \dots, g_n)$ и $\mathbf{h} = (h_1, h_2, \dots, h_n)$ – векторы увеличивающих ошибок, компоненты которых удовлетворяют равенствам

$$g_i = -e_i, \quad h_i = -f_i, \quad 1 \leq i \leq n. \quad (7)$$

Заметим, что из предложения $\mathbf{c} = \mathbf{v} + \mathbf{e} = \mathbf{u} + \mathbf{f}$ и равенств (7) следует выполнение условия $\mathbf{v} + \mathbf{h} = \mathbf{u} + \mathbf{g} = \mathbf{d}$ где $\mathbf{d}$ – некоторое слово длины n . Слова $\mathbf{u}$ и $\mathbf{v}$ принадлежат коду $\mathcal{A}$, исправляющему t увеличивающих ошибок. Следовательно, слова $\mathbf{d}$ не существует, и предположение о существовании $\mathbf{c}$ неверно. Тогда согласно (2) и (3) получаем, что код $\mathcal{A}$ исправляет t уменьшающих ошибок. Что и требовалось доказать.

Множество слов $B \subset A^n$ называется кодом, исправляющим t ошибок в модульной метрике, если для любой пары различных векторов $\mathbf{u}, \mathbf{v} \in B$ выполняется условие

$$d_M(\mathbf{v}, \mathbf{u}) \geq 2t + 1.$$

Пусть σ – целое число такое, что $0 \leq \sigma \leq 2t$. Определим множество векторов $B = B(\mathcal{L}, n, s, \sigma)$ следующим образом:

$$B(\mathcal{L}, n, s, \sigma) = \left\{ \mathbf{u} \mid \mathbf{u} \in \mathcal{A}(\mathcal{L}, n, s), \sum_{i=1}^n u_i = \sigma \pmod{2t+1} \right\}. \quad (8)$$

Т е о р е м а 2. Пусть B – подмножество слов кода с исправлением t увеличивающих ошибок, вес которых равен σ по модулю $2t + 1$. Тогда B является кодом, исправляющим t ошибок в модульной метрике.

Д о к а з а т е л ь с т в о 1. Пусть слова $\mathbf{u}$ и $\mathbf{v}$, принадлежащие множеству B , имеют различный вес. Тогда по определению B получаем, что веса слов $\mathbf{u}$ и $\mathbf{v}$ отличаются на величину, кратную $(2t + 1)$. Следовательно, $d_M(\mathbf{u}, \mathbf{v}) \geq 2t + 1$.

2. Пусть слова $\mathbf{u}$ и $\mathbf{v}$, принадлежащие множеству B , имеют одинаковый вес. Предположим, что $d_M(\mathbf{u}, \mathbf{v}) \leq 2t$. Следовательно, слово $\mathbf{u}$ может быть получено из слова $\mathbf{v}$ путем m увеличивающих и ℓ уменьшающих ошибок, и $m + \ell \leq 2t$. Из условия равенства $w_M(\mathbf{u}) = w_M(\mathbf{v})$ имеем, что $m = \ell$. Таким образом, должно существовать слово $\mathbf{c}$, получаемое из $\mathbf{u}$ и из $\mathbf{v}$ путем $m \leq t$ увеличивающих ошибок. По определению B слова $\mathbf{u}$ и $\mathbf{v}$ принадлежат коду $\mathcal{A}$, исправляющему t увеличивающих ошибок. Следовательно, слова $\mathbf{c}$ не существует и наше предположение о том, что $d_M(\mathbf{u}, \mathbf{v}) \leq 2t$, неверно. Что и требовалось доказать.

Определим множество векторов $B^* = B^*(\mathcal{L}, n + 1, s, \sigma)$ следующим образом:

$$B^* = \left\{ \mathbf{u} = (u_0, \dots, u_n) \in A^{n+1} \mid (u_1, \dots, u_n) \in \mathcal{A}(\mathcal{L}, n, s), \sum_{i=0}^n u_i = \sigma \pmod{2t+1} \right\}. \quad (9)$$

С л е д с т в и е 2. Множество слов B^* является кодом, исправляющим t ошибок в модульной метрике.

Д о к а з а т е л ь с т в о. Пусть в кодовом слове $\mathbf{u} \in B^*$ произошло $m = m_1 + m_2 \leq t$ увеличивающих ошибок, из которых m_1 ошибок произошло на символах кода $\mathcal{A}(\mathcal{L}, n, s)$, и m_2 ошибок – на символе u_0 . По весу принятого слова однозначно определяется число m произошедших увеличивающих ошибок. Множество слов $\mathcal{A}(\mathcal{L}, n, s)$ является кодом, исправляющим t увеличивающих ошибок. Из условия $m_1 \leq t$ получаем, что при декодировании кода $\mathcal{A}(\mathcal{L}, n, s)$ будут определены ошибки, имевшие место на его символах, и их вес m_1 . Следовательно, вес увеличивающей ошибки, произошедшей на символе u_0 вектора $\mathbf{u} \in B^*$, вычисляется по формуле $m_2 = m - m_1$.

Таким образом, код B^* исправляет t увеличивающих ошибок, а слова этого кода имеют вес, кратный $(2t + 1)$. Тогда из утверждения теоремы 2 получаем, что код B^* исправляет t ошибок в модульной метрике. Что и требовалось доказать.

Будем называть код B^* расширением кода B или просто расширенным кодом.

§ 3. Методы построения кодов в метриках, гомоморфных модульной метрике

Пусть $\mathcal{X}$ – конечное множество слов, на котором определена некоторая метрика ρ . Определим отображение $\mathcal{G}_n$ множества $\mathcal{X}$ в множество A^n Q -ичных слов длины n

$$\mathcal{G}_n : \mathcal{X} \Rightarrow A^n.$$

Пусть отображение $\mathcal{G}_n$ обладает следующими свойствами. Для любых $\mathbf{x}, \mathbf{y} \in \mathcal{X}$ имеем

- 1) $\mathcal{G}_n(\mathbf{x}) \neq \mathcal{G}_n(\mathbf{y})$, если $\mathbf{x} \neq \mathbf{y}$,
- 2) $d_M(\mathcal{G}_n(\mathbf{x}), \mathcal{G}_n(\mathbf{y})) \leq \rho(\mathbf{x}, \mathbf{y})$,
- 3) На образе $\mathcal{X}$ в A^n определено обратное отображение

$$\mathcal{G}_n^{-1}(\mathbf{c}), \mathbf{c} \in \mathcal{G}_n(\mathcal{X}).$$

Таким образом, отображение $\mathcal{G}_n$ задает взаимно-однозначное соответствие между множествами $\mathcal{X}$ и $\mathcal{G}_n(\mathcal{X}) \subset A^n$. Метрику ρ , определенную на множестве $\mathcal{X}$ и удовлетворяющую п.2, будем называть метрикой, гомоморфной модульной метрике. Свойство гомоморфности метрики ρ позволяет использовать коды, исправляющие ошибки в модульной метрике, и отображение $\mathcal{G}_n^{-1}$ для построения кодов, исправляющих ошибки в метрике ρ .

Отношение порядка, определенное между векторами множества A^n , задает аналогичное отношение на векторах множества $\mathcal{X}$. Будем обозначать $\mathbf{x} \geq \mathbf{y}$ ($\mathbf{x} \leq \mathbf{y}$) и говорить, что вектор $\mathbf{x}$ сравним с вектором $\mathbf{y}$, если для образов этих векторов $\mathbf{u} = \mathcal{G}_n(\mathbf{x})$, $\mathbf{v} = \mathcal{G}_n(\mathbf{y})$ выполняется условие $\mathbf{u} \geq \mathbf{v}$ ($\mathbf{u} \leq \mathbf{v}$). Назовем $\mathbf{x} \in \mathcal{X}$ словом, полученным из слова $\mathbf{y} \in \mathcal{X}$ путем t однонаправленных увеличивающих (уменьшающих) ошибок в метрике ρ , если выполняются условия

$$\mathbf{x} \geq \mathbf{y}, \quad (\mathbf{x} \leq \mathbf{y}), \quad \rho(\mathbf{x}, \mathbf{y}) = t.$$

Будем говорить, что множество слов $C \subset \mathcal{X}$ является кодом, исправляющим t однонаправленных ошибок в метрике ρ , если не существует слова $\mathbf{z} \in \mathcal{X}$ и пары слов $\mathbf{x}, \mathbf{y} \in C$, для которых возможно выполнение условий

$$\mathbf{z} \geq \mathbf{x}, \quad \mathbf{z} \geq \mathbf{y}, \quad \rho(\mathbf{z}, \mathbf{x}) \leq t, \quad \rho(\mathbf{z}, \mathbf{y}) \leq t.$$

Множество слов $D \subset \mathcal{X}$ назовем кодом, исправляющим любые t ошибок в метрике ρ , если для любой пары $\mathbf{x}, \mathbf{y}$ различных слов множества D выполняется неравенство

$$\rho(\mathbf{x}, \mathbf{y}) \geq 2t + 1.$$

Используя конструкции теорем 1, 2 и следствия 2, определим коды C , D и D^* в метрике ρ .

$$C = C(\mathcal{L}, n, s) = \mathcal{G}_n^{-1}(\mathcal{G}_n(\mathcal{X} \cap \mathcal{A}(\mathcal{L}, n, s))),$$

$$D = D(\mathcal{L}, n, s, \sigma) = \mathcal{G}_n^{-1}(\mathcal{G}_n(\mathcal{X} \cap \mathcal{B}(\mathcal{L}, n, s, \sigma))), \quad (10)$$

$$D^* = D^*(\mathcal{L}, n, s, \sigma) = \mathcal{G}_n^{-1}(\mathcal{G}_n(\mathcal{X}) \cap \mathcal{B}^*(\mathcal{L}, n, s, \sigma)). \quad (11)$$

Из определения отображения $\mathcal{G}_n$ и гомоморфности метрики ρ модульной метрике следует, что код C исправляет t однонаправленных ошибок в метрике ρ , а коды D и D^* исправляют любые t ошибок в метрике ρ . Код D^* будем называть расширением кода D или просто расширенным кодом.

§ 4. Оценки мощности кодов в модульной метрике и метрике ρ

Пусть $\psi(x)$ – минимальное число $\geq x$, для которого существует $\text{GF}(\psi(x))$. Имеет место следующая

Т е о р е м а 3. *Мощность кода $\mathcal{C}(\mathcal{L}, n, s)$, исправляющего t однонаправленных увеличивающих (уменьшающих) ошибок в метрике ρ , удовлетворяет неравенству*

$$|\mathcal{C}(\mathcal{L}, n, s)| \geq \frac{|\mathcal{X}|}{\psi(n+1)^t}.$$

Д о к а з а т е л ь с т в о. Каждому многочлену $s(x)$ степени t и меньше соответствует свой код $\mathcal{C}(\mathcal{L}, n, s)$, исправляющий t однонаправленных ошибок в метрике ρ . Любое слово $y \in \mathcal{X}$ принадлежит ровно одному из таких кодов. Число различных многочленов $s(x)$ с единичным младшим коэффициентом, заданных над полем $\text{GF}(\psi(n+1))$, равно $\psi(n+1)^t$. Следовательно, найдется код $\mathcal{C}(\mathcal{L}, n, s)$, соответствующий многочлену $s(x)$, мощность которого удовлетворяет доказываемому неравенству.

С л е д с т в и е 3. *Для кода $\mathcal{D}(\mathcal{L}, n, s, \sigma)$, исправляющего t ошибок в метрике ρ , имеет место оценка мощности*

$$|\mathcal{D}(\mathcal{L}, n, s, \sigma)| \geq \frac{|\mathcal{X}|}{(2t+1)\psi(n+1)^t}.$$

С л е д с т в и е 4. *Для кода $\mathcal{D}^*(\mathcal{L}, n, s, \sigma)$, исправляющего t ошибок в метрике ρ , имеет место оценка мощности*

$$|\mathcal{D}^*(\mathcal{L}, n, s, \sigma)| \geq \frac{|\mathcal{X}|}{(2t+1)\psi(n)^t}.$$

Из определения множества A^n и утверждения теоремы 3 следует, что существует Q -ичный код $\mathcal{A}(\mathcal{L}, n, s)$ длины n с исправлением t однонаправленных ошибок в модульной метрике, мощность которого удовлетворяет неравенству

$$|\mathcal{A}(\mathcal{L}, n, s)| \geq \frac{Q^n}{\psi(n+1)^t}.$$

Из следствий 3, 4 имеем оценки

$$|\mathcal{B}(\mathcal{L}, n, s, \sigma)| \geq \frac{Q^n}{\psi(n+1)^t(2t+1)}.$$

$$|\mathcal{B}^*(\mathcal{L}, n, s, \sigma)| \geq \frac{Q^n}{\psi(n)^t(2t+1)}.$$

В случае выполнения строгих равенств $\psi(n+1) = n+1$, $\psi(n) = n$ полученные оценки запишутся в виде

$$\begin{aligned} |\mathcal{A}| &\geq \frac{Q^n}{(n+1)^t}, \\ |\mathcal{B}| &\geq \frac{Q^n}{(n+1)^t(2t+1)}, \\ |\mathcal{B}^*| &\geq \frac{Q^n}{n^t(2t+1)}. \end{aligned} \tag{12}$$

Пусть γ – примитивный элемент поля $\text{GF}(p^m)$, p – простое число, и выполняется неравенство $n \leq (p^m - 1)$. В работе [1] Дарьян показал, что справедлива

Т е о р е м а 4. Множество Q -ичных решений системы уравнений

$$\left\{ \begin{array}{l} \sum_{i=0}^{n-1} \gamma^{ij} x_i = a_j, \quad 1 \leq j \leq t, \quad t < p, \\ \left(\sum_{i=0}^{n-1} x_i \right) \bmod (2t+1) = b \end{array} \right.$$

является Q -ичным кодом $\mathcal{E}$ длины n , исправляющим t ошибок в модульной метрике.

Сравним мощность полученных кодов $\mathcal{B}$ и $\mathcal{B}^*$ с мощностью кодов $\mathcal{E}$. Если существует конечное поле $\text{GF}(q)$, у которого число элементов $q = n + 1$, то оценка мощности кодов $\mathcal{E}$ совпадает с неравенством (12). Однако коды $\mathcal{E}$ существуют только при условии выполнения неравенства

$$t < p, \quad (13)$$

где p – характеристика поля $\text{GF}(q)$. Указанное ограничение для кодов $\mathcal{B}$ отсутствует. Расширенные коды $\mathcal{B}^*$ при той же избыточности имеют длину на единицу большую, чем коды $\mathcal{E}$. Ограничение (13) на число ошибок, исправляемых кодами $\mathcal{B}^*$, отсутствует.

Число векторов, находящихся в модульной t -сфере любого вектора $\mathbf{x} \in A^N$ не меньше, чем число векторов в двоичной Хэмминговой t -сфере. Таким образом, полученные коды, как и коды Дарьяна, обладают асимптотически минимальной избыточностью для случая $t = \text{const}$.

§ 5. Коды, исправляющие ошибки оператора

Пусть $\{1, 2, \dots, Q\}$ – Q -ичный алфавит и $\mathcal{F}$ – множество Q -ичных векторов длины n . Для произвольной пары векторов $\mathbf{u}, \mathbf{v} \in \mathcal{F}$ определим расстояние $d_P(\mathbf{u}, \mathbf{v})$ как минимальное число перестановок соседних символов, переводящих слово $\mathbf{u}$ в слово $\mathbf{v}$. Множество слов $\mathcal{G} \subset \mathcal{F}$ назовем Q -ичным кодом длины n , исправляющим t перестановок (или ошибок оператора), если для любых различных $\mathbf{u}, \mathbf{v} \in \mathcal{G}$ выполняется неравенство $d_P(\mathbf{u}, \mathbf{v}) \geq 2t + 1$. Обозначим через s_i число компонент вектора $\mathbf{u} \in \mathcal{F}$, равных i , где $1 \leq i \leq Q$. Вектор $\mathbf{s} = (s_1, s_2, \dots, s_Q)$ назовем типом слова $\mathbf{u}$. В дальнейшем будем говорить, что слово $\mathbf{u}$ обладает типом $\mathbf{s}$ или, что тип $\mathbf{s}$ соответствует слову $\mathbf{u}$. Обозначим через $\mathcal{S}$ множество всевозможных типов, а через $\mathcal{F}_s$ – множество слов $\mathbf{u}$, обладающих типом $\mathbf{s} \in \mathcal{S}$. Заметим, что перестановки символов слова $\mathbf{u}$ не влияют на его тип. Следовательно, если векторы $\mathbf{u}, \mathbf{v} \in \mathcal{F}$ обладают различными типами, то $d_P(\mathbf{u}, \mathbf{v}) = \infty$.

Таким образом, задача построения Q -ичного кода $\mathcal{G}$ длины n с исправлением t перестановок сводится к нахождению в каждом множестве $\mathcal{F}_s$ подмножества $\mathcal{G}_s$, являющегося кодом с исправлением t перестановок. Решив эту задачу, получим, что

$$\mathcal{G} = \bigcup_{\mathbf{s} \in \mathcal{S}} \mathcal{G}_s. \quad (14)$$

Пусть задан вектор $\mathbf{u} \in \mathcal{F}_s$ и соответствующий ему $\mathbf{s} = (s_1, s_2, \dots, s_Q)$. Будем считать, что $s_i \neq 0$ для $1 \leq i \leq Q$. В противном случае $\mathbf{u}$ может рассматриваться как вектор над меньшим алфавитом.

Вектор, получаемый из $\mathbf{u}$ путем удаления всех символов от 1 до m включительно, будем обозначать $\mathbf{u}^{(m)} = (u_1^{(m)}, u_2^{(m)}, \dots, u_{n(m)}^{(m)})$, где $n(m)$ – длина такого вектора. Заметим, что для $n(m)$ выполняется равенство

$$n(m) = n - \sum_{i=1}^m s_i. \quad (15)$$

Для удобства обозначений доопределим $n(0) = n$, $u^{(0)} = u$. Вектор $u^{(m)}$ содержит s_{m+1} символов, равных $m + 1$. Перенумеруем слева направо позиции $u^{(m)}$ числами от 1 до $n(m)$, а символы вектора $u^{(m)}$, равные $(m + 1)$, числами от 1 до s_{m+1} . Поставим в соответствие вектору $u^{(m)}$ $n(m)$ -ичный вектор $p^{(m)} = (p_1^{(m)}, p_2^{(m)}, \dots, p_\ell^{(m)})$ длины $\ell = s_{m+1}$, где $p_i^{(m)}$ – номер позиции, в которой расположен i -й символ $m + 1$ вектора $u^{(m)}$. Таким образом, любому вектору $u \in \mathcal{F}_s$ соответствует набор векторов $P = \{p^{(0)}, p^{(1)}, \dots, p^{(Q-1)}\}$. Длина вектора $p^{(m)}$ равна s_{m+1} , где $0 \leq m \leq Q - 1$. Следовательно, суммарная длина векторов набора равна n .

П р и м е р 1. Пусть задан троичный вектор $u = (1, 2, 3, 1, 1, 2, 2, 3, 3) \in \mathcal{F}_s$ и соответствующий ему тип $s = (3, 3, 3) \in \mathcal{S}$. Тогда

$$\begin{aligned} u^{(0)} &= (1, 2, 3, 1, 1, 2, 2, 3, 3), & n(0) &= 9, & p^{(0)} &= (1, 4, 5), \\ u^{(1)} &= (2, 3, 2, 2, 3, 3), & n(1) &= 6, & p^{(1)} &= (1, 3, 4), \\ u^{(2)} &= (3, 3, 3), & n(2) &= 3, & p^{(2)} &= (1, 2, 3). \end{aligned}$$

Т е о р е м а 5. Пусть векторам $u, v \in \mathcal{F}_s$ отвечают наборы $P = \{p^{(0)}, p^{(1)}, \dots, p^{(Q-1)}\}$ и $H = \{h^{(0)}, h^{(1)}, \dots, h^{(Q-1)}\}$ соответственно. Тогда справедливо неравенство

$$d_P(u, v) \geq \sum_{i=0}^{Q-1} d_M(p^{(i)}, h^{(i)}).$$

Д о к а з а т е л ь с т в о. Из определения расстояния в модульной метрике имеем

$$d_M(p^{(i)}, h^{(i)}) = \sum_{j=1}^{s_{i+1}} |p_j^{(i)} - h_j^{(i)}|.$$

Пусть $p_j^{(i)} - h_j^{(i)} = \delta > 0$ ($\delta < 0$) для некоторых $1 \leq i \leq Q - 1$ и $1 \leq j \leq s_{i+1}$. Это эквивалентно тому, что j -й символ $(i + 1)$ в векторе $u^{(i)}$ расположен на δ позиций правее (левее) j -го символа $(i + 1)$ в векторе $v^{(i)}$. Следовательно, для перевода $u^{(i)}$ в $v^{(i)}$ необходимо δ перестановок соседних символов, в результате которых j -й символ $(i + 1)$ вектора $u^{(i)}$ сместится на δ позиций влево (вправо). Если между j -ми символами $(i + 1)$ в векторах u и v содержатся символы m , где $1 \leq m \leq i$, то число перестановок соседних символов, переводящих u в v будет больше числа δ . В противном случае, число таких перестановок равно δ .

П р и м е р 2. Пусть задан троичный вектор $v = (1, 2, 2, 1, 1, 3, 2, 3, 3) \in \mathcal{F}_s$ и соответствующий ему тип $s = (3, 3, 3) \in \mathcal{S}$. Рассмотрим $d_P(u, v)$, где u – вектор из примера 1. Тогда

$$\begin{aligned} v^{(0)} &= (1, 2, 2, 1, 1, 3, 2, 3, 3), & h^{(0)} &= (1, 4, 5), & p^{(0)} &= (1, 4, 5), & d_M(p^{(0)}, h^{(0)}) &= 0, \\ v^{(1)} &= (2, 2, 3, 2, 3, 3), & h^{(1)} &= (1, 2, 4), & p^{(1)} &= (1, 3, 4), & d_M(p^{(1)}, h^{(1)}) &= 1, \\ v^{(2)} &= (3, 3, 3), & h^{(2)} &= (1, 2, 3), & p^{(2)} &= (1, 2, 3), & d_M(p^{(2)}, h^{(2)}) &= 0. \end{aligned}$$

Таким образом

$$\sum_{i=0}^2 d_M(p^{(i)}, h^{(i)}) = 0 + 1 + 0 = 1.$$

Число перестановок соседних символов, переводящих вектор $u^{(1)}$ в вектор $v^{(1)}$, также равно 1. В векторах u и v вторые по счету слева символы $\langle 2 \rangle$ расположены на 6-й

и 3-й позициях соответственно. На 4-й и 5-й позициях этих векторов расположены символы $\langle 1 \rangle$. Следовательно, $d_P(u, v) > d_M(u^{(1)}, v^{(1)})$. В данном примере $d_P(u, v) = 5$.

По построению каждому набору векторов P соответствует единственный вектор $u \in \mathcal{F}_s$ и каждому вектору u соответствует единственный набор P . В дальнейшем будем отождествлять набор векторов $P = \{p^{(0)}, p^{(1)}, \dots, p^{(Q-1)}\}$ с вектором P длины $n - s_Q$, у которого на первых s_1 позициях расположен вектор $p^{(0)}$, на следующих s_2 позициях – вектор $p^{(1)}$, и т.д. На последних s_{Q-1} позициях вектора P располагается вектор $p^{(Q-2)}$. Такой вектор, вследствие очевидного изоморфизма между множеством векторов $\mathcal{F}_s$ и множеством наборов P , будем называть эквивалентом вектора u . Вектор $p^{(Q-1)}$ набора не включен в эквивалент потому, что он одинаковый для всех наборов множества P . Обозначим через $\mathcal{G}_k$ отображение, ставящее в соответствие любому из векторов $\mathcal{F}_s$ его эквивалент P , где $k = n - s_Q$. Тогда из определения $\mathcal{G}_k$ и теоремы 5 получаем, что метрика перестановок гомоморфна модульной метрике.

Пусть $\mathcal{N}$ – множество всевозможных эквивалентов векторов из $\mathcal{F}_s$ и $\psi(k) = k$. Тогда по утверждению следствия 4 существует множество $\mathcal{M} \subset \mathcal{N}$, являющееся кодом с исправлением t ошибок в модульной метрике, мощность которого удовлетворяет неравенству

$$|\mathcal{M}| \geq \frac{|\mathcal{N}|}{(2t+1)(n-s_Q)^t}.$$

Из определения отображения $\mathcal{G}_k$ и гомоморфности метрики перестановок модульной метрике получаем, что множество $\mathcal{G}_s = \mathcal{G}_k^{-1}(\mathcal{M})$ является кодом, исправляющим t перестановок соседних символов. Из изоморфности множеств $\mathcal{G}_s$ и $\mathcal{M}$, $\mathcal{F}_s$ и $\mathcal{N}$ следует оценка

$$|\mathcal{G}_s| = \frac{|\mathcal{F}_s|}{(2t+1)(n-s_Q)^t}. \quad (16)$$

Оценим мощность кода $\mathcal{G}_s$. Из (16) и (14) следует, что

$$|\mathcal{G}| \geq \frac{1}{(2t+1)} \sum_{s \in \mathcal{S}} \frac{|\mathcal{F}_s|}{(n-s_Q)^t}. \quad (17)$$

Без потери общности можно считать, что для компонент всех спектров $s \in \mathcal{S}$ выполняется условие

$$s_Q \geq s_i, \quad 1 \leq i \leq Q. \quad (18)$$

В противном случае всегда можно определить переобозначение элементов алфавита, однозначно соответствующее спектру, в результате которого условие (18) выполняется. Тогда имеет место неравенство

$$s_Q \geq \lceil n/Q \rceil,$$

где $\lceil x \rceil$ – наименьшее целое, большее или равное x . С учетом этого неравенства оценка мощности кода (17) примет вид

$$|\mathcal{G}| > \frac{Q^n}{(2t+1)(n - \lceil n/Q \rceil)^t}. \quad (19)$$

Заметим, что при $Q = 2$ из (19) получается оценка мощности кода, исправляющего t битовых сдвигов.

Коды, исправляющие перестановки соседних символов, изучались в работах [4,5]. Перестановки соседних символов всегда можно рассмотреть как пакет ошибок длины 2, однако такое представление избыточно. Касами [3] показал, что при определенных условиях одиночные перестановки соседних символов могут корректировать коды, исправляющие одиночные ошибки замещения. Мощность таких кодов оценивается неравенством

$$|\mathcal{C}| \geq Q^n/n^2.$$

Сравнивая эту оценку с (19), получаем, что на одинаковой длине коды Касами имеют меньшую мощность, чем коды данного параграфа. Кроме того, построенные коды способны исправлять не одну, а любое заданное число ошибок оператора.

§ 6. Коды, исправляющие ошибки в метрике Ли

Пусть $\mathcal{H}$ – множество Q -ичных слов длины n . Будем считать, что слова $\mathcal{H}$ заданы над алфавитом $\mathcal{A} = \{0, 1, 2, \dots, Q-1\}$ и Q – четное. Определим отображение $\mathcal{G}_{2n}$ множества $\mathcal{H}$ в множество $\mathfrak{N}$ $Q/2$ -ичных слов длины $2n$. Для этого поставим в соответствие любому $i \in \mathcal{A}$ пару символов $(i^{(1)}, i^{(2)})$ по следующему правилу.

$$\begin{cases} i^{(1)} = 1, \text{ если } 2i/Q \geq 1, & \text{и } i^{(1)} = 0 \text{ в противном случае,} \\ i^{(2)} = i, \text{ если } i^{(1)} = 0, & \text{и } i^{(2)} = Q-1-i \text{ в противном случае.} \end{cases} \quad (20)$$

Пример 3. Пусть $Q = 8$. Тогда имеет место следующее соответствие

$$\begin{aligned} 0 &\Rightarrow (0, 0), & 1 &\Rightarrow (0, 1), & 2 &\Rightarrow (0, 2), & 3 &\Rightarrow (0, 3), & 4 &\Rightarrow (1, 3), & 5 &\Rightarrow (1, 2), \\ 6 &\Rightarrow (1, 1), & 7 &\Rightarrow (1, 0). \end{aligned}$$

Таким образом, вектору $\mathbf{u} = (i_1, i_2, \dots, i_n) \in \mathcal{H}$ соответствует вектор $\mathcal{G}_{2n}(\mathbf{u}) = (i_1^{(1)}, i_1^{(2)}, i_2^{(1)}, i_2^{(2)}, \dots, i_n^{(1)}, i_n^{(2)}) \in \mathfrak{N}$. Пусть $i \Rightarrow (i^{(1)}, i^{(1)})$, и $j \Rightarrow (j^{(1)}, j^{(2)})$. Из (20) получаем, что

$$d_L(i, j) \geq d_M(i^{(1)}, j^{(1)}) + d_M(i^{(2)}, j^{(2)}).$$

Следовательно, для любой пары векторов $\mathbf{u}, \mathbf{v} \in \mathcal{H}$ выполняется условие

$$d_L(\mathbf{u}, \mathbf{v}) \geq d_M(\mathcal{G}_{2n}(\mathbf{u}), \mathcal{G}_{2n}(\mathbf{v})). \quad (21)$$

Множество $\mathfrak{N}$ будем называть множеством образов векторов из $\mathcal{H}$, т.е. $\mathfrak{N} = \mathcal{G}_{2n}(\mathcal{H})$. Из (21) и определения $\mathcal{G}_{2n}$ получаем, что метрика Ли, определенная на множестве слов $\mathcal{H}$, гомоморфна модульной метрике на множестве $\mathfrak{N}$. Согласно следствию 4 существует множество $\mathfrak{M} \supset \mathfrak{N}$, являющееся кодом с исправлением t ошибок в модульной метрике. Мощность такого кода удовлетворяет неравенству

$$|\mathfrak{M}| \geq \frac{|\mathfrak{N}|}{(2t+1)q^{t/2}}. \quad (22)$$

Из свойства гомоморфности метрик следует, что $\mathcal{C} = \mathcal{G}_{2n}^{-1}(\mathfrak{M})$ является кодом с исправлением t ошибок в метрике Ли. По определению отображения $\mathcal{G}_{2n}$ получаем, что множества $\mathfrak{N}$ и $\mathcal{H}$, $\mathcal{C}$ и $\mathfrak{M}$ равномощны. Следовательно, из (22) с учетом $|\mathcal{H}| = Q^n$ и при $\psi(2n) = 2n$ имеем оценку мощности Q -ичного кода $\mathcal{C}$ длины n , исправляющего t ошибок в метрике Ли

$$|\mathcal{C}| \geq \frac{Q^n}{(2t+1)2^t n^t}. \quad (23)$$

В [6] Берлекэмпом построен класс негациклических кодов. Мощность Q -ичного негациклического кода $\mathfrak{G}$ длины n с исправлением t ошибок в метрике Ли оценивается неравенством

$$|\mathfrak{G}| \geq \frac{Q^n}{2^t n^t}. \quad (24)$$

Дарян в [1] показал, что при определенных условиях Q -ичный БЧХ-код $\mathfrak{G}$ длины n исправляет t ошибок в метрике Ли, и мощность такого кода удовлетворяет неравенству

$$|\mathfrak{G}| \geq \frac{q^n}{(2t+1)n^t}. \quad (25)$$

Сравнивая (25) и (24) с (23), получаем, что коды для метрики Ли, построенные в данном параграфе, уступают по мощности кодам Берлекэмпа и Дарьяна. Однако, в отличие от полученных кодов, негациклические коды определены только при Q , для которого существует поле $GF(Q)$. Кроме того и коды Берлекэмпа, и коды Дарьяна исправляют не более $t \leq (Q-1)/2$ ошибок, а для построенных кодов это ограничение отсутствует.

Впервые Q -ичные коды для метрики Ли, исправляющие $t \geq (Q-1)/2$ ошибок, были описаны Мазуром в [2]. Это низкоскоростные коды и для небольших значений величины t/n имеют меньшую мощность, чем коды данного параграфа.

СПИСОК ЛИТЕРАТУРЫ

1. Дарьян А.В. Построение кодов для модульной метрики // Тр. IV Междунар. симпоз. по теории информации. Тез. докл. Ч.2. Москва – Ленинград, 1976. С.32-34.
2. Мазур Л.Е. Констациклические коды и их использование в системах передачи информации. Дис... канд. техн. наук. Казань, 1981.
3. Касами Т., Токура Н., Иварди Е., Инагаки Я. Теория кодирования. М.: Мир, 1978.
4. Геворкян Д.Н. Коды для общения оператора с машиной // Тр IV Всесоюз. конф. по вычислительным сетям. Тез. докл. Москва – Ташкент, 1979. С.34-37.
5. Бояринов И.М., Давыдов А.А., Мажедов. Использование помехоустойчивого кодирования для защиты информации от ошибок оператора // Автоматика и телемеханика. 1983, №2. С.5-49.
6. Берлекэмп Э. Алгебраическая теория кодирования. М.: Мир, 1971.
7. Дарьян А.В. Кодирование для каналов со специальными типами искажений. Дис... канд. техн. наук. Ленинград, 1979.

Поступила в редакцию
16.12.92

После переработки
31.03.93