ՀԱՅԱՍՏԱՆԻ ԳԻՏՈՒԹՅՈՒՆՆԵՐԻ ԱԶԳԱՅԻՆ ԱԿԱԴԵՄԻԱ
НАЦИОНАЛЬНАЯ АКАДЕМИЯ НАУК АРМЕНИИ
NATIONAL ACADEMY OF SCIENCES OF ARMENIA
ДОКЛАДЫ ԶԵԿՈՒՅՑՆԵՐ REPORTS
Հատոր Том Volume 112 2012 № 1

МАТЕМАТИКА

УДК 621.391.15

В. К. Леонтьев[1], Г. Л. Мовсисян[2], Ж. Г. Маргарян[3]

Геометрия аддитивного канала

(Представлено академиком Г. Г. Хачатряном 2/II 2011)

Ключевые слова: *аддитивный канал, коды, исправление ошибок, расстояние, совершенные коды, базис, ранг, мощность*

Введение. Рассматривается аддитивный канал связи, введенный в работе [1], как некоторый преобразователь информации, являющийся обобщением классического бинарного канала с ограниченным числом искажений $0 \to 1$, $1 \to 0$. Многие понятия и факты, приведенные в настоящей работе, имеют корни в классической теории кодирования и являются прямыми аналогами хорошо известных результатов [1-6].

«Шум», порождаемый аддитивным каналом, приводит к тому, что на выходе канала мы получаем слово, отличное от переданного. Это обстоятельство создает исходные предпосылки для введения стандартных в теории кодирования понятий кода, исправляющего ошибки, скорости передачи, декодирования и т.д.

С другой стороны, в связи с тем, что аддитивных каналов много, возникает проблема упорядочения и классификации таких каналов с учетом доминирующего свойства – возможности исправления ошибок.

Коды в аддитивном канале. В этой статье удобно рассматривать множество B^n как n-мерное векторное пространство над полем $B = \{0,1\}$ из двух элементов.

Если $A = \{y_0, y_1, ..., y_m\}$ – подмножество B^n, то с A связывается понятие аддитивного канала A следующим образом [1].

Любой из векторов $x \in B^n$ в канале A преобразуется в один из векторов вида

$$y = x \oplus y_s \ , \quad s = \overline{0, m} \ , \text{ где } \oplus - \text{сложение по mod 2.}$$

Определение. Для любого вектора $x \in B^n$ окрестностью t-ого порядка относительно A назовем множество

$$A^t(x) = \left\{u \oplus y : u \in A^{t-1}(x), y \in A\right\}.$$

При этом удобно принять, что $A^o(x) = \{x\}$.

Стандартное описание процесса исправления ошибок состоит в построении «таблицы декодирования» [6].

Пусть канал A – это множество преобразований $T = \{T_0, T_1, ..., T_m\}$

$$B^n \to B^n$$

вида $y = T_i(x)$, $i = \overline{0, m}$.

Если $V = \{v_0, v_1, ..., v_N\} \subseteq B^n$, то коду V ставится в соответствие таблица декодирования

v_0	$v_1 \ldots$	v_N
$T_0(v_0)$	$T_0(v_1)$	$T_0(v_N)$
$T_1(v_0)$	$T_1(v_1)$	$T_1(v_N)$
$\vdots$	$\vdots$	$\vdots$
$T_m(v_0)$	$T_m(v_1)$	$T_m(v_N)$

«Исправление» ошибок с помощью таблицы происходит следующим образом. По определению любой «переданный» вектор x преобразуется каналом A в $T_i(x) = y$, который лежит хотя бы в одном из столбцов таблицы. Тогда кодовый вектор, лежащий в первой строке любого из таких столбцов, и является «прообразом» переданного вектора. Ясно, что

если вектор y принадлежит единственному из столбцов таблицы, то процесс «декодирования» приводит к правильному результату.

Очевидно, что каждый столбец таблицы декодирования – это окрестность первого порядка соответствующего кодового вектора v_i, т. е. $A^1(v_i) = \{T_0(v_i),...,T_m(v_i)\}$.

Определение. Код V исправляет ошибки канала A, если столбцы таблицы декодирования не имеют общих векторов.

Отметим также, что векторы одного столбца таблицы декодирования не обязаны быть различными, что не влияет на способность кода V исправлять ошибки канала A.

Если $x \in B^n$ и $T = \{T_i\}$ – некоторое семейство преобразований, то окрестность $t-$ ого порядка вектора x относительно семейства T – это множество векторов

$$T^t(x) = \{u \oplus y : u \in T^{t-1}(x),\ y \in \mathrm{T}\},\ \text{где}\quad T^0(x) = \{x\}.$$

Для случая аддитивного канала $A = \{y_0, y_1,..., y_m\}$ преобразование $T_i(x)$ выглядят так: $T_i(x) = x \oplus y_i$, $i = \overline{0,m}$.

Условием того, что код $V = \{v_0, \mathrm{v}_1,..., v_N\}$ исправляет ошибки аддитивного канала $A = \{\mathrm{y}_0, y_1,..., y_m\}$, является: $A^1(v_i) \cap A^1(v_j) = \varnothing$, для $i \neq j$.

Эквивалентная запись этого условия выглядит так: $v_i \oplus y_s \neq \mathrm{v}_\mathrm{j} \oplus y$ или, симметрично ей, $v_i \oplus v_j \neq y_s \oplus y_r$.

Ясно, что предыдущие определения являются симметричными относительно пары (A,V) и потому порождение «ошибок» и «исправление» ошибок имеют одинаковую природу.

Утверждение 1. Если код V исправляет ошибки аддитивного канала A, то код A исправляет ошибки аддитивного канала V.

Поскольку мощность окрестности t-ого порядка не зависит от вектора v, то обозначим $A^t = \left|A^t(v)\right|$.

Отметим теперь, что для мощности кода V, исправляющего ошибки аддитивного канала $A = \{y_0, y_1, ...y_m\}$, справедливы следующие границы [3]:

$$\frac{2^n}{A^2} \le |V| \le \frac{2^n}{A^1}.$$

При этом код V, на котором достигается верхняя граница, называется совершенным кодом, исправляющим ошибки аддитивного канала A.

Для описания «взаимоотношений» аддитивного канала A и кода V, исправляющего ошибки этого канала, удобно ввести следующий двухместный предикат *X(A,V):*

$$X(A,V) = \begin{cases} 1, \text{если код } V \text{ исправляет ошибки канала } A, \\ 0, \text{â ïðîòèâíîì ñëó÷àå} \end{cases}$$

Предикат *X(A,V)* обладает следующими свойствами:

а) $X(A,V) = X(V,A)$.

Это свойство сразу следует из «симметричности» условий исправления ошибок;

б) $X(A \oplus x, V \oplus y) = X(V,A)$, где x и y – произвольные векторы множества B^n;

в) $X(A,V) = X(TA,TV)$, где T – произвольное обратимое линейное преобразование $B^n \to B^n$ [1].

Свойство в) показывает, что аддитивные каналы A и TA для обратимого линейного преобразования T обладают одинаковыми свойствами в смысле коррекции ошибок, поэтому такие аддитивные каналы естественно считать неразличимыми.

Приведенные ниже рассуждения являются традиционными при изучении подобного рода эквивалентностей [7].

Пусть $\begin{pmatrix} B^n \\ |A| \end{pmatrix}$ – семейство всех $|A|$ элементных подмножеств B^n и $GL_2(n)$ – группа всех невырожденных матриц порядка n над полем B.

Если $T \in GL_2(n)$, то образ подмножества A – это множество $TA = \{y_0T, y_1T, ..., y_mT\}$, где $A = \{y_0, y_1, ..., y_m\}$.

Таким образом, группа $GL_2(n)$ действует на семейство $\begin{pmatrix} B^n \\ |A| \end{pmatrix}$, преобразуя множество A в $TA \in \begin{pmatrix} B^n \\ |A| \end{pmatrix}$.

Транзитивное множество $Z(A)$, определяемое подмножеством A, задается стандартным образом: $Z(A) = \{TA : T \in GL_2(n)\}$.

Если T_A стабилизатор множества A, т. е. $T_A = \{T \in GL_2(n) : TA = A\}$, то, как хорошо известно [7], $|Z(A)| = indT_A$. Мощность транзитивного множества Z(A) равна индексу подгруппы T_A.

Далее разложение

$$\begin{pmatrix} B^n \\ |A| \end{pmatrix} = \bigcup_A T_A$$

представляет разбиение всего семейства $\begin{pmatrix} B^n \\ |A| \end{pmatrix}$ на классы транзитивных множеств.

Формула для числа $r(n)$ транзитивных множеств определяется с помощью леммы Бернсайда [7].

Пусть $T \in GL_2(n)$, тогда $V_{|A|}(T)$ – число «неподвижных» точек преобразования T или число подмножеств из $\begin{pmatrix} B^n \\ |A| \end{pmatrix}$, не меняющихся при преобразовании T.

Лемма 1. *Справедливо соотношение*

$$r(n) = \frac{1}{\left|GL_2(n)\right|} \sum_{T \in GL_2(n)} V_{|A|}(T), \text{ где } \left|GL_2(n)\right| = \prod_{i=0}^{n-1} (2^n - 2^i).$$

Следствие. Справедливо неравенство

$$r(n) > \frac{\begin{pmatrix} 2^n \\ |A| \end{pmatrix}}{\left|GL_2(n)\right|} .$$

Пусть $V(A)$ код максимальной мощности, исправляющий все ошибки канала A.

Если фиксировать мощность канала A, то существует $\begin{pmatrix} 2^n \\ |A| \end{pmatrix}$-различных аддитивных каналов и, как обычно, целесообразно рассмотреть нижнюю и верхнюю границы мощности соответствующих корректирующих кодов

$$\overline{D_k}(n) = \max_{|A|=k} \left|V(A)\right|, \quad \underline{D_k}(n) = \min_{|A|=k} \left|V(A)\right| .$$

Содержательный смысл этих функций, рассмотренных в работе [1] для класса групповых кодов, достаточно очевиден и вряд ли нуждается в дополнительных комментариях.

Ясно, что аддитивных каналов столько, сколько существует булевых функций, и, как показывает свойство б) и в), некоторые из них по существу не отличаются друг от друга. Как может выглядеть классификация таких каналов, неясно, но следующие определения соответствуют общепринятой точке зрения.

Определение. *Каналы A и C называются эквивалентными, если любой код, исправляющий ошибки аддитивного канала A исправляет ошибки канала C и наоборот.*

Формально можно описать, введя отношение частичного порядка

$$A \le C;\ X(C,V) = 1 \to X(A,V) = 1,\ \text{для всех}\ V \subseteq B^n.$$

Если $A \subseteq C$, то $A \le C$, что выглядит вполне естественно.

Это свойство позволяет для каждой $m < 2^n$ искать аддитивные каналы с «наилучшими» и «наихудшими» корректирующими свойствами.

Утверждение 2. *Аддитивные каналы* $(A \oplus u)$ *и* $(A \oplus v)$ *являются эквивалентными для любых* $u, v \in B^n$.

Утверждение 3. *Если* $X(A,V) = 1$, *то* $|A \cap V| \le 1$.

Из предыдущих утверждений следует, что без ограничения общности можно считать:

а) если $\{A\}$ – класс аддитивных каналов, эквивалентных A, то проблему кодирования достаточно решить для любого представителя этого класса;

б) аддитивный канал A содержит нулевой вектор, что можно интерпретировать как возможность безошибочной передачи сигнала по этому каналу.

Поскольку из $X(A,V) = 1$ следует $X(V,A) = 1$, то аналогичное утверждение верно и для кода V, т.е. достаточно рассматривать коды, содержащие нулевой вектор.

Таким образом, из $X(A,V) = 1$ следует, что множество A и V могут пересекаться только в нуле, а поиск кода V надо организовать в множестве $\{B^n \setminus A\} \cup \{(00...0)\}$. В дальнейшем $y_0 = (00...0) \in A$, $v_0 = (00...0) \in V$.

Метрики и коды. Стандартной и наиболее широко используемой в теории кодирования метрикой является метрика Хэмминга, т.е. следующая функция:

$$\|x\|_E = \|(x_1 x_2 ... x_n)\|_E = \sum_{i=1}^{n} x_i .$$

Можно считать, что эта метрика связана с «натуральным» базисом $E = (e_1, e_2, ..., e_n)$ следующим образом:

$$x = \sum_{i=1}^{n} \alpha_i e_i \to \|x\|_E = \sum_{i=1}^{n} \alpha_i .$$

Ясно, что при выборе другого базиса $M = \{y_1, y_2, ..., y_n\}$ мы порождаем другую метрику $x = \sum_{i=1}^{n} \beta_i y_i \to \|x\|_M = \sum_{i=1}^{n} \beta_i$.

Более общая процедура порождения метрик указанным выше способом состоит в следующем. Для заданного подмножества $M = \{y_1, y_2, ..., y_m\} \subseteq B^n$ и вектора $x \in B^n$ мы рассматриваем все «разложения» x по M, т.е. представления вида

$$x = \sum_{i=1}^{m} \alpha_i y_i , \qquad (1)$$

и каждому такому представлению сопоставляем число $\sum_{i=1}^{m} \alpha_i$.

Теперь, выбрав из этих чисел минимальное, мы определим следующую норму (норма МЛМ), связанную с M :

$$\|x\|_M = \begin{cases} \min\left\{\sum \alpha_i\right\} \text{ по представлениям (1)}, \\ \infty, \text{если таких представлений нет.} \end{cases}$$

Лемма 2. *Функция* $\| \ \|_M$ *является метрикой (в дальнейшем метрикой МЛМ) для произвольного подмножества* $M \subseteq B^n$.

Определение. *Метрика МЛМ называется базисной, если* $M \subseteq B^n$ *является базисом.*

На языке теории графов описанная ситуация выглядит следующим образом.

На множестве вершин B^n зададим бинарное отношение

$$x \sim y \leftrightarrow x + y = y_i \text{ для некоторого } y_i \in M .$$

Это отношение определяет смежность, и мы получаем граф $\left(B^n, E_M\right)$. Расстояние между вершинами этого графа задается стандартным образом: минимальное число ребер в цепи, соединяющей эти вершины, и бесконечность, если такой цепи не существует.

Лемма 3. *Для базисных метрик справедливы соотношения*

$$\rho_M(u,v) = \rho_E\left(u\ H_M^{-1}\ ,\ v\ H_M^{-1}\ \right),$$

$$\rho_E(u,v) = \rho_M\ \left(u\ H_M\ ,\ v\ H_M\ \right), \qquad (2)$$

где H_M *– матрица перехода от базиса* M *к базису* E.

Несмотря на то, что метрики в различных базисах могут сильно различаться, спектр расстояний пространства B^n всегда один и тот же.

Лемма 4. *Пусть* $t_k(M)$ *– число точек из* B^n *с* $\|x\|_M = k$. *Тогда* $t_k(M) = \binom{n}{k}$, $k = \overline{0,n}$ *для произвольного базиса* M.

При заданной метрике МЛМ все стандартные определения теории корректирующих кодов можно трансформировать, заменяя метрику Хэмминга на любую базисную метрику МЛМ. В частности, совершенный код V с расстоянием $d = 2t+1$ – это разбиение множества B^n в объединение шаров радиуса t в метрике МЛМ. В силу формулы (2) совершенные коды в одной метрике переходят в совершенные коды в другой метрике. Формально эта ситуация выглядит следующим образом.

Пусть $Q = \{y_1, y_2, ..., y_n\}$ – произвольное подмножество B^n и C – произвольная невырожденная матрица порядка n над полем B. Рассмотрим линейное преобразование

$$f(u) = u \cdot C$$

пространства B^n в себя.

Образ множества Q при этом преобразовании мы обозначим через $f(Q)$, т.е.

$$f(Q) \overset{def}{=} \{f(u) : u \in Q\}.$$

При этом $|f(Q)| = |Q|$, а спектры $\{\rho_M(u,v): u,v \in Q\}$ и $\{\rho_M(f(u),f(v)),\ f(u),f(v) \in f(Q)\}$ не имеют какой-то простой связи. Ситуация несколько изменится, если рассмотреть различные МЛМ метрики и ввести ограничения на рассматриваемые преобразования.

Пусть $C = H_M$ – матрица перехода от базиса M к базису E. В этих условиях справедлива.

Лемма 5. *Для базисных метрик верна формула*

$$\rho_M(u,v) = \rho_E(f(u),f(v)) \qquad (3)$$

Здесь $u,v \in B^n$.

Обоснование формулы (3) следует из формул (2).

Формула (3) допускает много различных интерпретаций геометрического характера. Мы приведем два факта, которые будут использоваться в дальнейшем.

а) Подмножество $A \subseteq B^n$ с базисной метрикой ρ_M и подмножество $f(A)$ с базисной метрикой ρ_E являются шарами радиуса t одновременно.

б) Код $V \subseteq B^n$ с базисной метрикой ρ_M и код $f(V)$ с базисной метрикой ρ_E являются совершенными с расстоянием $2t+1$ одновременно.

Предыдущие утверждения позволяют строить совершенные коды в B^n для произвольных базисных метрик, если удалось построить такой код хотя бы для одной базисной метрики. В частности, если $A \setminus y_0$ является базисом, справедливо следующее утверждение.

Теорема 1. *Нетривиальные совершенные коды, исправляющие ошибки аддитивного канала $A^t(y_0)$, существуют лишь только при следующих значениях n и t:*

а) $n = 2^e - 1,\ t = 1;$

б) $n = 23,\quad t = 3.$

Теорема 2. *Код V исправляет ошибки аддитивного канала A, если и только если выполняются условия*

$$\rho_A(v_i, v_J) \geq 3, \qquad i, j = 1, N.$$

Из теоремы 1 следует теперь, что для $n = 2^e - 1$ и произвольного базиса $A \setminus y_0$ существует совершенный код V, исправляющий ошибки канала A. Оптимальность кода V следует из верхней границы мощности кода

$$V \leq \frac{2^n}{A^1}.$$

Для того, чтобы в общем случае построить совершенный код, исправляющий ошибки канала A, где A/Y_0 базис, нужно взять совершенный код Хэмминга V и рассмотреть его образ при линейном преобразовании $f(u) = uH_A$, где H_A – матрица, строками которой служат векторы множества $A \setminus y_0$. Тогда $f(V)$ – это искомый совершенный код, который в силу леммы 5 и леммы 6 исправляет ошибки аддитивного канала A.

[1]Вычислительный центр РАН, Москва

[2]БИТ групп, Москва

[3]Ереванский государственный университет, e-mail: jiromr@mail.ru

В. К. Леонтьев, Г. Л. Мовсисян, Ж. Г. Маргарян

Геометрия аддитивного канала

Рассматривается класс метрик, связанных с подмножествами линейного пространства над *GF(2)*, и устанавливается ряд фактов, позволяющих выразить корректирующую способность кодов для аддитивных каналов в терминах этих метрик.

Վ. Կ. Լեոնտև, Ղ. Լ. Մովսիսյան, Ժ. Գ. Մարգարյան

Ադդիտիվ կապուղիների երկրաչափություն

Դիտարկվում են *GF(2)*-ի վրա որոշված գծային տարածությունում հեռավորությունների դասեր, որոնք սահմանվում են ըստ այդ տարածության տրված ենթաբազմության: Բերված են ադդիտիվ կապուղիներում կոդի սխալներն ուղղելու հնարավորություններն այդ հեռավորությունների տեսանկյունից:

V. K. Leont'ev, G. L. Movsissyan, Zh. G. Margaryan

Geometry of Additive Channels

The classes of distance defined in liner space over *GF(2)* have been studied. The mentioned classes of distance are characterized according to the given subset of the liner space. We have given the opportunities to correct the code errors in the additive channels considering those distances.

Литература

1. *Деза М.Е.* В сб.: Об исправлении произвольного шума и наихудшем шуме. Теория передачи информации. М. Наука. 1964. С. 26-31.
2. *Леонтьев В.К., Мовсисян Г.Л.* - Доклады НАН Армении. 2004. Т. 104. №1. С.23-27.
3. *Леонтьев В.К., Мовсисян Г.Л., Маргарян Ж.Г.* - Доклады РАН. 2006. Т. 411. №3. С. 306-309.
4. *Леонтьев В.К., Мовсисян Г.Л., Маргарян Ж.Г.* - Проблемы передачи информации. 2008. Т.44. Вып. 4. С. 12-19.
5. *Леонтьев В.К., Мовсисян Г.Л., Маргарян Ж.Г.* - Доклады НАН Армении. 2010. Т. 110. N 4. С. 334-339.
6. *Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А.* Теории кодов, исправляющих ошибки. М. Связь. 1979.
7. *Сачков В.Н.* Комбинаторные методы дискретной математики. М. Наука. 1977.