ՀԱՅԱՍՏԱՆԻ ԳԻՏՈՒԹՅՈՒՆՆԵՐԻ ԱԶԳԱՅԻՆ ԱԿԱԴԵՄԻԱ
НАЦИОНАЛЬНАЯ АКАДЕМИЯ НАУК АРМЕНИИ
NATIONAL ACADEMY OF SCIENCES OF ARMENIA
ДОКЛАДЫ ԶԵԿՈՒՅՑՆԵՐ REPORTS

Հատոր 110 2010 № 4

МАТЕМАТИКА

УДК 621.391.15

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

Коды в аддитивных каналах

(Представлено академиком Г. Г. Хачатряном 18/III 2010)

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

Введение. Канал связи, или канал для передачи информации, изучался во многих математических работах. Стандартная точка зрения на канал связи включает в себя вероятностный язык, на котором описываются процессы, происходящие в этом канале. Мы придерживаемся более детерминистского взгляда и рассматриваем канал как преобразователь информации или, точнее, как некоторую словарную функцию, осуществляющую отображение одних слов в другие.

Аддитивный канал связи представляет достаточно простой пример такого преобразования, включающий, однако, в себя многие хорошо известные частные случаи.

Пусть $B = [0, 1]$ — поле Галуа и B^n — n-мерное векторное пространство над этим полем. Рассмотрим следующие преобразования B^n в себя:

$$T(x) - x + \lambda y, \quad \text{где} \quad x, y \in B^n \quad \text{и} \quad \lambda \in B.$$

Если $A = \{y_1, \ldots, y_m\}$ — произвольное подмножество B^n, то множество преобразований вида

$$Tp(x) = x + \lambda y_p$$

определяет аддитивный канал A в том смысле, что исходный вектор x преобразуется каналом A в один из векторов вида $Tp(x)$, где $p = \overline{1, m}$.

Определение кода, исправляющего ошибки аддитивного канала, копирует стандартное определение кода, исправляющего ошибки вида $0 \to 1$, $1 \to 0$.

Определение. Код $V = \{v_1, \ldots, v_N\} \subseteq B^n$ исправляет ошибки аддитивного канала $A = \{y_1, \ldots, y_m\}$, если выполняются условия

$$v_i + \lambda_1 y_p \neq v_j + \lambda_2 y_q, \tag{1}$$

где $v_i, v_j \in V$, $y_p, y_q \in A$; $\lambda_1, \lambda_2 \in B$, $i \neq j$, $p \neq q$.

При передаче по каналу A вектор $v \in V$ может перейти в один из векторов вида $\{v + \lambda y_p\}$, которые образуют окрестность вектора v. Условие (1) гарантирует, что эти окрестности не пересекаются и, тем самым, любой вектор $v \in V$ может быть однозначным образом восстановлен на выходе канала.

Приведем эквивалентное описание кодов, корректирующих ошибки аддитивного канала A, в терминах окрестностей [2].

Окрестность k-го порядка определим следующим образом:

$$A^k = \{v + \lambda y,\ v \in A^{k-1}, y \in A, \lambda \in B\}, \quad A^0 = \{(0, \ldots, 0)\}.$$

Утверждение. Код V исправляет ошибки аддитивного канала A тогда и только тогда, когда выполняется условие $V^2 \cap A^2 = A^0$.

Понятно, что

$$A^1 = A \cup A^0. \tag{2}$$

В терминах окрестностей классические оценки Хэмминга и Варшамова–Гильберта для мощности кода V, исправляющего ошибки аддитивного канала A, выглядят следующим образом:

$$\frac{2^n}{|A^2|} \leqslant |V| \leqslant \frac{2^n}{|A^1|}. \tag{3}$$

Таким образом, каждому аддитивному каналу A можно поставить в соответствие число $D_A(n)$ [3], равное максимальной мощности кода, исправляющего ошибки каналов A. Ясно, что $D_A(n)$ удовлетворяет неравенствам (3). Если фиксировать число $m = |A|$, то существует $\binom{2^n}{m}$ аддитивных каналов мощности m. При этом алгоритмы исправления ошибок в различных аддитивных каналах имеют разную сложность, зависящую от свойств аддитивного канала A. Это обстоятельство можно охарактеризовать следующим образом, введя на семействе подмножеств $\{A\} \subseteq B^n$ линейный порядок

$$A \leqslant C \longleftrightarrow D_A(n) \geqslant D_C(n). \tag{4}$$

Например, если $|A^1| = 2$, то $D_A(n) = 2^{n-1}$ и все аддитивные каналы являются эквивалентными в смысле (4).

Определенные результаты, относящиеся к порядку (4), содержатся в [1]

ՀԻՄՆԱՐԱՐ ԳԻՏՈՒԹՅԱՆ
ԳՐԱԴԱՐԱՆ

Совершенные коды в аддитивных каналах. Пусть $M = \{z_1, \ldots, z_n\}$ – произвольный базис пространства B^n и $T = \|\tau_{ij}\|$ – матрица перехода от базиса $H = \{e_1 = (1, \ldots, 0), \ldots, e_n = (0, \ldots, 1)\}$ к базису $\{z_1, \ldots, z_n\}$

$$z_i = \sum_{j=1}^{n} \tau_{ij} e_j, \qquad i = \overline{1, n}.$$

Обратный переход осуществляется с помощью матрицы T^{-1}, т. е. при $x \in B^n$

$$x = \sum_{j=1}^{n} \lambda_j z_j,$$

где $(\lambda_1, \ldots, \lambda_n) = xT^{-1}$.

В случае, когда $z_i = 1^p 0^{n-p}$, получаем

$$T = \begin{Vmatrix} 10 & \ldots & 00 \\ 11 & \ldots & 00 \\ \ldots & \ldots & \ldots \\ 11 & \ldots & 11 \end{Vmatrix}, \qquad T^{-1} = \begin{Vmatrix} 10 & \ldots & 00 \\ 11 & \ldots & 00 \\ \ldots & \ldots & \ldots, \\ 00 & \ldots & 11 \end{Vmatrix}.$$

Ясно, что T реализует преобразование

$$xT = (x_1 \oplus x_2 \cdots \oplus x_n, x_2 \oplus x_3 \cdots \oplus x_n, \cdots, x_n),$$
$$xT^{-1} = (x_1 \oplus x_2, \cdots, x_2 \oplus x_3, \cdots, x_{n-1} \oplus x_n, x_n).$$

Представление вектора $x = (x_1, \ldots, x_n)$ в базисе $\{z_1, \ldots, z_n\}$ имеет вид

$$x = \sum_{i=1}^{n-1} (x_i \oplus x_{i-1}) z_j + x_n z_n.$$

Каждое подмножество $M = \{z_1 \ldots, z_m\} \subseteq B^n$, ранг которого равен n, порождает норму МЛМ, которая определяется следующим образом.

Если $u \in B^n$, то

$$\|u\|_M = \min \left\{ \sum_{i=1}^{m} \lambda_i \right\}, \quad \text{где } u = \sum_{i=1}^{m} \lambda_i z_i.$$

Очевидно, что когда $M = \{z_1 \ldots, z_n\}$ базис, то норма МЛМ

$$\|u\|_M = \sum_{i=1}^{n} \lambda_i, \tag{5}$$

где суммирование в (5) ведется в поле действительных чисел.

Лемма 1. *Если $M = \{z_1 \ldots, z_n\} \subseteq B^n$ и $\operatorname{rang} M = n$, то $\rho_M(u, v) = \|u + v\|_M$ $\forall u \in B^n$ является метрикой в B^n.*

Когда M базис в B^n, то метрика Хэмминга $\rho_H(u,v)$ и метрика МЛМ $\rho_M(u,v)$ связаны следующими соотношениями.

Лемма 2. *Справедливы формулы*

$$\rho_M(u,v) = \rho_H(uT^{-1}, vT^{-1}), \qquad \rho_H(u,v) = \rho_M(uT, vT). \tag{6}$$

Определим отображение $B^n \to B^n$ следующим образом:

$$f(u) = u\,C\,, \tag{7}$$

где C – произвольная невырожденная матрица порядка n.

Обозначим через $f(V)$ образ множества $V \subseteq B^n$ при отображении (7), т.е.

$$f(V) = \{f(u) : u \in V\}. \tag{8}$$

Теорема 1. *Если $V \subseteq B^n$ совершенный код в метрике Хэмминга, то $f(V)$ – совершенный код в МЛМ метрике ρ_M, где M множество строк матрицы C.*

Доказательство. Если $S_t(v)$ – шар радиуса t с центром в $v \in V$, то

$$f(S_t(v)) = \{f(u); u \in S_t(v)\}.$$

Если $a \in f(S_t(v))$, то с учетом (6) получаем

$$\rho_M(a, f(v)) = \rho_M(f(u), f(v)) = \rho_H(v,u) \leqslant t. \tag{9}$$

Из (9) следует, что образом шара радиуса t с центром в v по метрике Хэмминга является шар радиуса t с центром в $f(v)$ по метрике МЛМ. Далее, если u лежит в шаре радиуса t с центром $v \in V$, то по (9) $f(u)$ лежит в шаре радиуса t с центром $f(v)$. Таким образом, шары радиуса t с центрами $u \in f(V)$ покрывают множество B^n. Аналогичным образом показывается, что шары радиуса t с центрами $u \in f(V)$ не пересекаются. Лемма доказана.

Способность кода $V = \{v_1, \ldots, v_N\} \subseteq B^n$ исправлять ошибки аддитивного канала A в терминах метрики МЛМ может быть сформулирована следующим образом.

Лемма 3. *Если $\operatorname{rang} M = n$, то код $V = \{v_1, \ldots, v_N\}$ исправляет ошибки аддитивного канала $A = M$ тогда и только тогда, когда выполняется условие*

$$\rho_M(v_i, v_j) \geqslant 3, \qquad i \neq j.$$

Предыдущие утверждения позволяют построить совершенные коды для аддитивных каналов вида $A = M$, где M – базис пространства B^n.

Теорема 2. *Если $n = 2^m - 1$ и A является базисом пространства B^n, то существует совершенный код, исправляющий ошибки аддитивного канала A^1.*

Доказательство. Для $n = 2^m - 1$ можно построить совершенный код Хэмминга V с минимальным кодовым расстоянием, равным трем. Рассмотрим матрицу перехода $T = \|\tau_{ij}\|$ от базиса $H = \{e_1, \ldots, e_n\}$ к базису $A = \{y_1, \ldots, y_n\}$. Пусть $f(u) = uT$, где $u \in B^n$. По теореме образом совершенного кода V при преобразовании (7) является совершенный код $f(V)$ в метрике МЛМ и минимальное расстояние в коде $f(V)$ равно трем; по лемме код $f(V)$ исправляет ошибки аддитивного канала A^1 и имеет ту же мощность, что и код Хэмминга, т. е.

$$|f(V)| = \frac{2^n}{n+1}.$$

Отсюда с учетом (2) и (3) следует, что $f(V)$ является совершенным кодом, исправляющим ошибки аддитивного канала A^1, что и требовалось доказать.

Следствие. Если $n = 23$ и A — базис пространства B^n, то существует совершенный код, исправляющий ошибки аддитивного канала A^3.

В доказательстве этого следствия используется факт существования совершенного кода Голея с радиусом три в метрике Хэмминга.

Полученные результаты являются естественным развитием исследований, представленных в работах [1-4]. Однако многие вопросы, относящиеся к указанной проблематике, в настоящей статье затронуты лишь косвенно или не затронуты вовсе. Например, в теореме 1 фактически установлено, что все аддитивные каналы A, являющиеся базисом линейного пространства B^n, являются эквивалентными в смысле возможности исправления ошибок. Как далеко можно продвинуться в этом направлении и будут ли эквивалентными каналы A и $\overline{A}$ с $|A| = |\overline{A}|$ и $rang(A) = rang(\overline{A})$, уже не совсем ясно. Еще более сложной является проблема классификации всех аддитивных каналов.

[1] Computing Center, Russian Academy of Sciences

[2] BIT GROUP, Moscow

[3] Yerevan State University

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

Коды в аддитивных каналах

Для аддитивных каналов, с множеством ошибок $A \subseteq B^n$ (B^n — n-мерное векторное пространство над полем GF (2)), в пространстве B^n определено новое расстояние МЛМ, которое является обобщением расстояния Хэмминга. Описаны семейства совершенных кодов, которые по новому расстоянию МЛМ аналогичны совершенным кодам Хэмминга и Голея.

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

Կոդերն ադդիտիվ կապուղիներում

Մխալների $A \subseteq B^n$ (B^n – n-չափանի վեկտորական տարածություն է GF (2) վրա) բազմությունով ադդիտիվ կապուղիների համար B^n-ում սահմանված է նոր MΛM հեռավորություն, որը Հեմմինգի հեռավորության բնական ընդհանրացումն է: Նկարագրված են կատարյալ կոդերի դասեր A սխալներով ադդիտիվ կապուղիների համար, որոնք Հեմմինգի և Գոլեյի կատարյալ կոդերի նմանատիպն են ըստ նոր MΛM հեռավորության:

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

On Codes in Additive Channels

A new MLM distance has been defined for additive channels, with the set of errors $A \subseteq B^n$ (B^n – n is vectorial space on GF (2)) in B^n space. The new MLM distance is the natural generalization of Hamming's distance. Classes of perfect codes have been described which are analogues of Golay's and Hamming's perfect codes according to the MLM distance.

Литература

1. *Деза М.Е.* Проблемы передачи информации. 1965. Т. 1. N3. С. 29-39.

2. *Леонтьев В.К., Мовсисян Г.Л.* - Доклады НАН Армении. 2004. Т. 104. N1 С. 23-27.

3. *Леонтьев В.К., Мовсисян Г.Л., Маргарян Ж.Г.* - Доклады РАН. 2006. Т. 411. N3. С. 306-309.

4. *Леонтьев В.К., Мовсисян Г.Л., Маргарян Ж.Г.* - Проблемы передачи информации. 2008. Т. 44. N 4. С. 12-19.