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

Հատոր Том Volume 120 2020 № 2

МАТЕМАТИКА

УДК 621.391.15

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

Алгебраические групповые каналы связи

(Представлено академиком Г. Г. Хачатряном 24/I 2020)

Ключевые слова: *алгебраические групповые каналы связи, максимальная мощность, коды, исправление ошибок.*

Введение. Семейство каналов связи довольно разнообразно, и подробное теоретическое изучение многих из них встречает серьезные математические трудности. В то же время целый ряд каналов связи в содержательном смысле похожи друг на друга и поэтому могут быть исследованы одинаковыми методами. Таковыми являются групповые каналы, для которых построение максимального кода имеет простое и прозрачное решение, формулируемое в классических теоретико-групповых терминах.

§1. Каналы связи и словарные функции. Пусть $B = \{a_1, a_2, \dots, a_p\}$ – конечный алфавит и B^* – множество всех слов конечной длины над алфавитом B. Словарная функция является произвольным частичным отображением ψ следующего вида:

$$B^* \xrightarrow{\psi} B^*.$$

Мы будем рассматривать канал как преобразователь информации, и если принять тезис о том, что в любом канале связи происходит преобразование одних слов в другие, то достаточно общий канал можно описать следующим образом.

Задано некоторое множество

$$\Psi = \{\psi_0, \psi_1, \dots, \psi_m\}$$

частичных словарных функций

$$B^* \xrightarrow{\psi_i} B^*, \qquad i = \overline{0, m}$$

и многозначное отображение

$$f(x) = (\psi_0(x), \psi_1(x), \dots, \psi_m(x)),$$

где $x \in W \subseteq B^*$. Содержательно это означает, что если $x \in W$, то после передачи по каналу $K(\Psi)$ это слово переходит в одно из слов $\{\psi_0(x), \psi_1(x), \dots, \psi_m(x)\} \subseteq W$.

Множество всех обратимых отображений $\{\psi_i\}$, $\psi_i(W) \subseteq W$ обозначим через Т. При этом все суперпозиции $\psi_{i_1} \psi_{i_2} \dots \psi_{i_k}$ функции ψ_{i_j} из множества Ψ определены на W.

Определение [1]. *Алгебраическим каналом связи* К(Ψ) *называется многозначное отображение*

$$f(x)=(\psi_0(x),\psi_1(x), \dots, \psi_m(x)), \tag{1}$$

где $\Psi \subseteq$ Т, *и если*

$$\psi_i \in \Psi \rightarrow \psi_i^{-1} \in \Psi. \tag{2}$$

Формулу (1) следует понимать следующим образом. На вход канала подается слово v. На выходе получается ровно одно из значений $\psi_0(v)$, $\psi_1(v), \dots, \psi_m(v)$. Фраза «одно из значений» интерпретируется в вероятностном смысле как равномерное распределение на всех словарных функциях $\psi_0(x),\psi_1(x), \dots, \psi_m(x)$. Точнее: если на вход канала подается слово v, то с вероятностью $\frac{1}{m+1}$ оно переходит в слово $\psi_i(v)$.

Условие (2) требует, чтобы любое «преобразованное» слово могло быть возвращено к исходному виду путем тех же самых трансформаций. Отметим, что любой аддитивный канал удовлетворяет условию (2) и является алгебраическим [2]. Однако не все матричные каналы являются алгебраическими, например, матричный канал с выпадением символов [3, 4]. Следовательно, на множестве B^n действует группа преобразования Т, которая переводит слово из B^n в слово из этого же множества. В дальнейшем мы всегда будем считать, что $\psi_0(x)= x$, что можно интерпретировать как возможность безошибочной передачи слова по этому каналу,

$$W = B^n \subseteq B^*, \text{где } B = \{0,1\}.$$

Подобные допущения упрощают многие технические детали и не влияют, как мы увидим далее, на ситуацию в целом. При этом изложенный материал становится более доступным для понимания.

Определение. *Множество* $V \subseteq B^n$ *называется кодом, исправляющим ошибки канала* $K(\Psi)$, *если выполнено следующее условие:*

$$\psi_i(u) \neq \psi_j(v) \tag{3}$$

для всех $\boldsymbol{i}$ *и* $\boldsymbol{j}$ *и для всех слов* $\boldsymbol{u}, \boldsymbol{v} \in V$.

Условие (3) означает, что последствия действий канала $K(\Psi)$ на кодовые слова различны, и поэтому искажения могут быть обнаружены и исправлены.

В дальнейшем обозначим через $V(\Psi)$ код, исправляющий ошибки канала $K(\Psi)$. В терминах, введенных выше, основная задача при заданном канале состоит в построении кода $V(\Psi)$ максимальной мощности – $\overline{V}$ (Ψ).

Ясно, что мощность кода $V(\Psi)$ зависит от «структуры» и мощности множества Ψ, «порождающего» канал $K(\Psi)$, и т.д.

Определение. *Код $V(\Psi)$ называется совершенным для канала $K(\Psi)$, если*

$$B^n = \bigcup_{v \in V(\Psi)} \Psi(v).$$

В содержательном смысле код V должен быть устроен так, чтобы по любому искаженному сигналу исходное сообщение восстанавливалось однозначно, т.е. предполагается существование однозначного декодирования.

§2. Групповые каналы и коды. Существует один важный и полезный класс алгебраических групповых каналов, K (Ψ), $\Psi = (\psi_0,\ \psi_1,\ \ldots,\ \psi_m)$, на примере которого можно в определенном смысле до конца разобраться во всех отмеченных выше проблемах.

Определение. *Если множества словарных функций $\Psi = \{\psi_i\}$ образуют группу относительно операции суперпозиции, то такой канал $K(\Psi)$ называется* ***групповым****.*

Примеры. 1) Канал $K(\Psi)$, где $\psi_i(x) = x + y_i$, а множество $\{y_0,\ y_1, \ldots,\ y_m\}$ – подгруппа в B^n, является групповым, где $+$ – операция сложения по $mod2$. В частности, если $|\ y_i| \equiv 0(mod2)$ для $i = \overline{0, 2^{n-1} - 1}$, то канал $K(\Psi)$, где происходит любое четное число ошибок, является групповым.

2) Возьмем в качестве примера канал, порожденный «обобщенным кубом» $A = B^{n_1}(\ \lambda_1) \times B^{n_2}(\ \lambda_2) \times \ldots \times B^{n_k}(\ \lambda_k)$, где $n_1 + n_2 + \cdots + n_k = n$ и $B^{n_i}(\ \lambda_i) = \{\lambda_i^{n_i}, \lambda_i \in \{0,1\}\}$, т.е. $\psi_i(x) = x + y_i,\ \ y_i \in A$. Ясно, что $|A| = 2^k$ и канал $K(\Psi)$ является групповым. В содержательном смысле этот канал работает в так называемом «пакетном режиме»: меняются или не меняются одновременно все буквы в одном «пакете» кодового слова.

3) Если $M = \{M_0, M_1, \ldots, M_m\}$ – подгруппа группы $GL_2(n)$ невырожденных матриц порядка n над полем $F_2 = \{0,1\}$, то канал $K(\Psi)$, где $\Psi(x) = \{xM_1, xM_2, \ldots, xM_m\}$, является групповым.

4) Рассмотрим $S_n = \{g\}$, где g переставляет координаты

$$x = \left(\alpha_1\ \alpha_2, \ldots\ \alpha_n\right),$$

не меняя «состава» слова x. Пусть в этом примере $B = \left\{a_1,\ a_2\ \ldots\ a_p\right\}$ – произвольный алфавит, $B^n = (B)^n$. Тогда S_n – группа перестановок, действующих на B^n следующим образом:

$$g(\alpha_1\alpha_2 \ldots \alpha_n) = (\alpha_{g_{(1)}}\alpha_{g_{(2)}} \ldots \alpha_{g_{(n)}}),$$

где $g \in S_n$.

Таким образом, на множество слов B^n действует группа $\Psi = \{\psi_0, \psi_1, \dots, \psi_m\}$.

Как обычно, транзитивные множества определяются как $\Psi(x) = \{\ \psi_i(x),\ \ \psi_i \in\ \Psi\}$ для $x \in B^n$, и имеет место разбиение

$$B^n = \bigcup_{x \in B^n} \Psi(x).$$

При этом $|\Psi(x)| = ind\Psi_x = \frac{|\Psi|}{|\Psi_x|}$ – индекс группы Ψ по подгруппе Ψ_x, где $\Psi_x = \{\ \psi_i \in\ \Psi\colon\ \psi_i(x) = x\}$ – стабилизатор слова $x \in B^n$.

Все коды, исправляющие ошибки канала $K(\Psi)$, описываются в следующем утверждении.

Утверждение 1. *Код* $V = \{v_0, v_1, \dots, v_N\}$ *исправляет ошибки группового канала* $K(\Psi)$ *тогда и только тогда, когда никакая пара* (v_i, v_j) *не принадлежит одному транзитивному множеству* $\Psi(x)$, $x \in B^n$.

Утверждение 2. *Для группового канала* $K(\Psi)$ *любой код* $V(\Psi)$, *содержащий по одному из представителей всех транзитивных множеств, является совершенным кодом, исправляющим ошибки канала* $K(\Psi)$.

Действительно, поскольку любые два транзитивных множества не пересекаются и для любых слов из B^n транзитивное множество и окрестность первого порядка совпадают, то, выбрав по одному представителю из каждого транзитивного множества, получим совершенный код $\overline{V}(\Psi)$ для канала $K(\Psi)$.

Из этого утверждения следует, что число элементов максимального по мощности кода, исправляющего ошибки группового канала $K(\Psi)$, равно числу транзитивных множеств. Следовательно, справедливо следующее утверждение , являющееся следствием классической леммы Бернсайда [5].

Следствие. *Совершенный код* $V(\Psi)$ *алгебраического группового канала* $K(\Psi)$ *является максимальным по мощности кодом, исправляющим ошибки любого алгебраического канала, эквивалентного* $K(\Psi)$ [6].

Пусть $x \in B^n$ и $N(\psi_i)$ – множество неподвижных слов преобразования ψ_i, т. е. множество решений уравнения

$$\psi_i(x) = x, \psi_i \in \Psi.$$

Утверждение 3. *Для мощности максимального кода* $V(\Psi)$ *справедлива формула*

$$\left|\overline{V}(\Psi)\right| = \frac{1}{m+1} \sum_{\psi_i \in \Psi} |N(\psi_i)|. \quad (4)$$

Воспользуемся теоремой и вычислим мощность кода $\overline{V}(\Psi)$ в следующих примерах.

Примеры. 5) Рассмотрим пример 2. Имеем

$$N(\psi_i) = \begin{cases} B^n, \text{если } i = 0 \\ \emptyset, i \neq 0 \end{cases}.$$

Следовательно, $\left|\overline{V}(\Psi)\right| = 2^{n-k}$.

6) Вернемся к примеру 4. Каждому слову $x \in B^n$ можно поставить в соответствие его состав или слово $\lambda = (\lambda_1\, \lambda_2 \dots \lambda_p)$, где λ_i – число вхождений буквы α_i в слово x. Ясно, что преобразование $g(x)$ не меняет состава слова x. При этом число слов состава λ равно

$$\binom{n}{\lambda_1}\binom{n-\lambda_1}{\lambda_2}\dots\binom{n-(\lambda_1+\lambda_2+\dots+\lambda_{p-1}}{\lambda_p} = \frac{n!}{t_1!\ t_2! \dots\ t_p!} = \binom{n}{t_1\, t_2 \dots t_p}$$

полиномиальному коэффициенту, где

$$n = \sum_{i=1}^{p} t_i.$$

При этом число различных «составов» слов равно числу решений диофантова уравнения

$$\sum_{i=1}^{p} t_i = n, \quad t_i \geq 0, \quad i = \overline{1,p}$$

и, значит, равно

$$\binom{p+n-1}{p-1}.$$

Любой код V, исправляющий ошибки канала $K(S_n)$, содержит не более чем одно слово из семейства всех слов, имеющих одинаковый состав. Поэтому максимальная мощность такого кода $V(S_n)$ задается формулой

$$\left|\overline{V}(S_n)\right| = \binom{p+n-1}{p-1},$$

в частности, при $p = 2$: $\left|\overline{V}(S_n)\right| = n + 1$. Любой максимальный по мощности код, исправляющий ошибки канала $K(S_n)$, содержит только одно слово из каждого слоя $B_0^n, B_1^n, \dots B_n^n$. Число таких кодов равно

$$\prod_{k=0}^{n} \binom{n}{k}.$$

Рассмотрим канал, определяемый следующим образом:

если $x = (\alpha_1\, \alpha_2\, \dots\, \alpha_n)$, то при передаче по каналу позиции с номерами $\{i_1, i_2, \dots i_{n-k}\}$ не меняются, а в остальных -позициях могут происходить любые перестановки букв. Формально ситуация описывается следующим образом. На всех словах $(\alpha_1\, \alpha_2\, \dots\, \alpha_n) \in B^n$ действует подгруппа $S(i_1, i_2, \dots i_{n-k})$ группы S_n, сохраняющая позиции с номерами $\{i_1, i_2, \dots i_{n-k}\}$.

Орбита слова x – это множество всех слов, совпадающих с x в позициях $\{i_1, i_2\,, \dots i_{n-k}\}$ и получающихся перестановками во всех остальных - позициях.

Примеры. 7) Если $i_1 = 1, i_2 = 2, \dots i_{n-k} = n-k$, то орбита слова

$x = (\alpha_1\,\alpha_2\,\ldots\,\alpha_n)$ – это множество слов, получающихся из x перестановкой последних в k-позиции. Если $\left|\alpha_{n-k+1}\,\alpha_{n-k+2}\,\ldots\,\alpha_n\right| = r$, то число таких слов равно $\binom{k}{r}$ – мощности проекции k слоя в B_r^k. Мощность оптимального кода V равна $2^{n-k}(k+1)$, и любой такой код устроен следующим образом: произвольно выбираются первые $(n-k)$-позиции, а остальные k – это произвольный набор с фиксированным числом единиц $0,1\ldots k$.

8) Если $n = 4,\; k = 2$, то код V имеет вид

0000	0100	1000	1100
0010	0110	1010	1110
0011	0111	1011	1111

.

В общем виде, если перестановка g разбивается в произведение k-независимых циклов, т.е. $g = z^1 z^2 \ldots z^k$, то число слов из B^k, инвариантных относительно g, равно 2^k. Теперь для мощности кода V из леммы Бернсайда получаем выражение

$$|V| = \frac{2^{n-k}}{k}\sum_{g\in S} N(g) = \frac{2^{n-k}}{k}\sum_{k=1}^{n} C(n,k)2^k,$$

где $C(n,k)$ – число Стирлинга первого рода или число перестановок из S_n, имеющих ровно k независимых циклов. Так как в нашем случае $n = k$ и $C(n,k)$= $C(n,r)$, то

$$|V| = \frac{2^{n-k}}{k}\sum_{r=1}^{k} C(k,r)2^r = \frac{2^{n-k}}{k}(k+1)! = 2^{n-k}(k+1),$$

так как имеет место классическая формула $\{\psi^k\}$ – множество циклических сдвигов порядка n, действующее на B^n следующим образом: для слова $x = \left(\alpha_1\,\alpha_2\,\ldots\,\alpha_n\right) \in B^n$ $\psi^0(x) = x\,, \psi^1\left(\alpha_1\,\alpha_2\,\ldots\,\alpha_n\right) = \alpha_2\,\alpha_3\,\ldots\,\alpha_n\,\alpha_1$, $\psi^k(x) = \psi\psi^{k-1}(x)$, $k = 0,1,\ldots n-1$. $\sum_{k=1}^{n} C(n,k)\,x^k = x(x+1)\ldots(x+n-1)$. Интересным примером группового канала является канал циклических сдвигов.

§3. Групповой канал циклических сдвигов. Пусть $B^n = \{0,1\}^n$ и $\Psi = \{\psi^k\}$ – множество циклических сдвигов порядка n, действующее на B^n следующим образом: для слова $x = \left(\alpha_1\,\alpha_2\,\ldots\,\alpha_n\right) \in B^n$

$$\psi^0(x) = x\,, \psi^1\left(\alpha_1\,\alpha_2\,\ldots\,\alpha_n\right) = (\alpha_2\,\alpha_3\,\ldots\,\alpha_n\,\alpha_1),\; \psi^k(x) = \psi\psi^{k-1}(x),$$
$$k = 0,1,\ldots n-1.$$

Ясно, что $|\Psi| = n$ и Ψ – циклическая группа порядка n, где окрестности слова $x \in B^n$ могут быть найдены с помощью стабилизаторов

$$\Psi_x = \{\psi^k : \ \psi^k x = x\}.$$

Ниже приведены соответствующие численные результаты некоторых n.

Примеры. 9) Для n=4 имеем:

$x = 0000 \quad \Psi_x = \{\psi^0, \psi^1, \psi^2, \psi^3\}, \Psi(x) = \{x\}$

$x = 0001 \quad \Psi_x = \{\psi^0\}, \Psi(x) = B_1^4 = \{0001, 0010, 0100, 1000\}$

$x = 1010 \quad \Psi_x = \{\psi^0, \psi^2\}, \Psi(x) = \{1010, 0101\}$

$x = 1100 \quad \Psi_x = \{\psi^0\}, \Psi(x) = \{1100, 0110, 0011, 1001\}$

$x = 1110 \quad \Psi_x = \{\psi^0\}, \Psi(x) = \{1110, 0111, 1011, 1101\} = B_3^4$

$x = 1111 \quad \Psi_x = \{\psi^0, \psi^1, \psi^2, \psi^3\}, \Psi(x) = \{x\}.$

Таким образом, куб B^4 разбивается на два транзитивных множества мощности 1; 1 – транзитивное множество мощности 2; 3 – транзитивное множество мощности 4. Естественным следствием проделанных вычислений является возможность нахождения функции $N\ (\psi)$ для всех преобразований ψ. В случае $n = 4$ имеем

$$N(\psi^0) = 2^4, \ N(\psi^1) = 2, \ N(\psi^2) = 4, \ N(\psi^3) = 2.$$

Отсюда число транзитивных множеств согласно утверждению 3 равно

$$\frac{16 + 4 + 2 + 2}{4} = 6,$$

что совпадает с результатом непосредственного вычисления.

Далее, код $V(\Psi) = \{(0000), (1111), (1010), (1100), (1110), (0001)\}$, собранный из представителей транзитивных множеств, является одним из максимальных кодов. Декодирование слов на выходе канала производится с помощью стандартной таблицы декодирования, которая в нашем случае имеет вид

0000	**1111**	**1010**	**1100**	**1110**	**0001**
		0101	0110	0111	1000
			0011	1011	0100
			1001	1101	0010

10) Для $n = 6$ картина следующая:

$x = 000000 \quad \Psi_x = \{\psi^0, \psi^1, \psi^2, \psi^3, \psi^4, \psi^5\}, \ \Psi(x) = \{x\}$

$x = 111111 \quad \Psi_x = \{\psi^0, \psi^1, \psi^2, \psi^3, \psi^4, \psi^5\}, \ \Psi(x) = \{x\}$

$x = 100000 \quad \Psi_x = \{\psi^0\}, \qquad \Psi(x) = B_1^6$

$x = 100100, \quad \Psi_x = \{\psi^0, \psi^3\}$ и $|\Psi(x)| = 3.$

Если $|x| = 2$, но $x \notin \Psi(100100)$, то $\Psi_x = \{\psi^0\}$ и $|\Psi(x)| = 6$.

Таким образом, имеем одно транзитивное множество с тремя словами и два транзитивных множества по 6 слов в каждом. В целом $\left|B_6^2\right| = 2 \cdot 6 + 1 \cdot 3$

$$x = 101010 \quad \Psi_x = \{\ \psi^0, \psi^2, \psi^4\}, \ \Psi(x) = \{x, \overline{x}\}.$$

В этом случае имеем одно транзитивное множество с двумя словами.

Для остальных $x \notin \Psi(101010)$ с $|x| = 3$ $\ \Psi_x = \{\psi^0\}$ и $|\Psi(x)| = 6$.

Количество таких транзитивных множеств 3, следовательно, получаем

$\binom{6}{3} = \frac{6\cdot5\cdot4}{6} = 20 = 3\cdot6+2,$

$x = 110110,$ то $\Psi_x = \{\psi^0, \psi^3\}$ и $|\Psi(x)| = 3.$

Для остальных $x \notin \Psi(110110)$ и $|x| = 4$ $\Psi_x = \{\psi^0\},$ $|\Psi(x)| = 6.$

Таких транзитивных множеств два. Следовательно,

$\binom{6}{4} = 15 = 3 + 2\cdot6 <$

$|x| = 5$, $\Psi_x = \{\psi^0\}$ и $|\Psi(x)| = 6$>

В этом случае имеем одно транзитивное множество.

Таким образом, получаем разбиение B^6 на транзитивные множества и возможность нахождения функции N (ψ) для всех преобразований ψ: $N(\psi^0) = 2^6,$ $N(\psi^1) = 2,$ $N(\psi^2) = 4, N(\psi^3) = 8, N(\psi^4) = 4,$ $N(\psi^5) = 2.$

Отсюда число транзитивных множеств согласно утверждению равно

$$\frac{64+2+4+8+4+2}{6} = 14,$$

что совпадает с результатом непосредственного вычисления. Далее, код $V(\Psi) = \{$(000000), (111111), (100000), (100100), (101000), (110000), (101010), (111000), (110010), (110100), (110110), (111100), (101110), (111110)$\}$, собранный из представителей транзитивных множеств, является одним из максимальных кодов. Декодирование слов на выходе канала производится с помощью стандартной таблицы декодирования, которая в нашем случае $n = 6$ имеет вид

111000	**101010**	**110010**	**110110**	**110100**	**100000**	**111100**
011100	010101	011001	101101	011010	010000	011110
001110		101100	011011	001101	001000	001111
000111		010110	101101	100110	000100	100111
100011		001011		010011	000010	110011
110001		100101		101001	000001	111001

101110	**111110**	**101000**	**100100**	**010000**	**111111**	**000000**
010111	011111	010100	010010	011000		
101011	101111	001010	001001	001100		
110101	110111	000101		000110		
111010	111011	100010		000011		
011101	111101			100001		

В общем виде мощность кода для циклического канала может быть найдена с помощью хорошо известных комбинаторных результатов.

Определение. *Периодом слова* $a \in B^n$ *называется минимальное число* k *такое, что* $\psi^k(a) = a$.

Если период слова a равен k, то транзитивное множество $\Psi(a)$ имеет вид: $\{a, \psi(a) \dots \psi^{k-1}(a)\}$. Поэтому мощность транзитивного множества $\Psi(a)$ равна периоду слова a.

Обозначим число транзитивных множеств мощности d через $\lambda_n(d)$. Так как транзитивные множества производят разбиение B^n, то справедливо соотношение

$$\sum_{d/n} d\lambda_n\,(d) = 2^n. \tag{5}$$

При этом код максимальной мощности $\overline{\mathrm{V}}\,(\Psi)$ – это любое множество всех представителей транзитивных множеств, и его мощность задается формулой (4), которая в данном случае имеет вид:

$$\left|\overline{\mathrm{V}}(\Psi)\right| = \sum_{d/n} \lambda_n(d). \tag{6}$$

Из формул (5) и (6) с использованием стандартной теоретико-числовой техники получается следующее хорошо известное выражение:

$$\left|\overline{\mathrm{V}}(\Psi)\right| = \frac{1}{n}\sum_{d/n} 2d\varphi(n/d) = \frac{1}{n}\sum_{d/n} 2^{n/d}\varphi(d)$$

или

$$\left|\,\overline{V}(\Psi)\right| = \sum_{k/n} 2^k \varphi\left(\frac{n}{k}\right), \tag{7}$$

где $\varphi(q)$ − функция Эйлера − количество чисел меньших q и взаимнопростых с ним, вычисляемая по формуле

$$\varphi(n) = n\prod_{p/n}\left(1 - \frac{1}{p}\right).$$

Формула (7) представляет собой мощность максимального кода, исправляющего ошибки циклического канала $K(\Psi)$. Если $n = pq$, где p, q – простые числа, то

$$\left|\,\overline{V}(\Psi)\right| = \frac{2^{pq} + 2^p(q-1) + 2^p(p-1) + 2(p-1)(q-1)}{p\mathrm{q}}.$$

Для $n = p$ все значительно проще:

$$\left|\,\overline{V}(\Psi)\right| = \frac{2^p - 2}{p} + 2.$$

Приведенные выше примеры показывают, что в случаях, когда канал $K(\Psi)$ является групповым, задача о построении максимального по мощности кода $\overline{V}(\Psi)$, исправляющего ошибки канала $K(\Psi)$, может быть решена до конца. Соответствующая формула для мощности максимального кода

(4) – это классическая лемма Бернсайда для числа транзитивных множеств в условиях действия группы Ψ на некотором множестве слов.

[1] ФИЦ ИУ РАН, Москва
[2] Группа Бит, Москва
[3] Ереванский государственный университет
e.mails: vkleontiev@yandex.ru, garib@hkzap.ru,
j.margaryan@ysu.am

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

Алгебраические групповые каналы связи

Исследуются групповые алгебраические каналы связи. Основной результат работы позволяет построить коды максимальной мощности, исправляющие ошибки групповых каналов.

Վ. Կ. Լեոնտիև, Գ. Լ. Մովսիսյան, Ժ. Գ. Մարգարյան

Հանրահաշվական խմբային կապի ուղիներ

Ուսումնասիրվում են հանրահաշվական խմբային կապի ուղիներ: Աշխատանքի հիմնական արդյունքը թույլ է տալիս կառուցել մաքսիմալ հզորության կոդեր, որոնք ուղղում են սխալները խմբային կապի ուղիներում:

V. K. Leontiev, G. L. Movsissian, J. G. Margaryan

A Group Communication Channels

The present paper explores group algebraic communication channels. The main result allows to build maximum power codes that corrects errors of the group channels.

Литература

1. *Леонтьев В. К., Мовсисян Г. Л.* В кн.: The First International. Algebra and Geometry Conference 16-20 May 2007, Yerevan, Armenia.
2. *Леонтьев В. К., Мовсисян Г. Л.* – ДНАН Армении. 2004. Т. 104. № 1. С. 23-27.
3. *Леонтьев В. К., Мовсисян Г. Л., Осипян А. А.* В кн.: Материалы XI междунар. семинара «Дискретная математика и ее приложение». Изд-во МГУ. 2012. С. 415-416.
4. *Левенштейн В. И.* – ДАН СССР. 1965. Т. 163. №4. С. 845-848.
5. *де Брейн Н. Дж.* В сб.: Прикладная комбинаторная математика. М. Мир. 1968. С. 61-106.
6. *Леонтьев В. К., Мовсисян Г. Л., Маргарян Н. Г.* – ДНАН Армении. 2019. Т. 119. № 3. С. 195-203.