

В. К. Леонтьев¹, Г. Л. Мовсисян², Ж. Г. Маргарян³

Дизъюнктивные каналы

(Представлено академиком С. К. Шукурьяном 24/V 20022)

Ключевые слова: каналы связи, словарные функции, алгебраические каналы, дизъюнктивные каналы, коды.

Введение. Точная постановка задачи борьбы с помехами, происходящими в канале связи, принадлежит К. Шеннону и состоит в следующем: на входе канала известно некоторое множество слов, которое содержит все потенциально возможные сообщения, годные для передачи. Проблема кодирования состоит в выборе такого семейства сообщений, чтобы при получении на выходе канала сообщения было возможно однозначно восстановить (декодировать) переданное сообщение.

В предыдущих работах [1–3] мы рассматривали алгебраические каналы, в частности аддитивные и матричные каналы.

В данной работе изучается следующий класс комбинаторных неалгебраических каналов – дизъюнктивные каналы, которые по форме напоминают аддитивные каналы, но существенно отличаются от них.

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 – произвольное частичное отображение ψ следующего вида:

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

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

Заданы некоторое множество

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

частичных словарных функций

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

и многозначное отображение

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

где $x \in W \subseteq B^*$. Множество всех обратимых отображений $\{\psi_i\}, \psi_i(a) \subseteq W$ обозначим через T . При этом все суперпозиции $\psi_{i_1} \psi_{i_2} \dots \psi_{i_k}$ функций ψ_{i_j} из множества Ψ определены на W .

Определение [1]. Комбинаторным каналом связи $K(\Psi)$ называется многозначное отображение

$$f(x) = (\psi_0(x), \psi_1(x), \dots, \psi_m(x)). \quad (1)$$

Формулу (1) следует понимать следующим образом. На вход канала подается слово v . На выходе получается ровно одно из значений $\psi_0(v), \psi_1(v), \dots, \psi_m(v)$.

Определение [1]. Алгебраическим каналом связи $K(\Psi)$ называется многозначное отображение

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

где $\Psi \subseteq T$, и если

$$\psi_i^{-1} \in \Psi, \psi_i \in \Psi. \quad (2)$$

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].

В дальнейшем мы всегда будем считать, что $\psi_0(x) = x$, что можно интерпретировать как возможность безошибочной передачи слова по этому каналу, $W = B^n \subseteq B^*$.

Коды, исправляющие ошибки.

Определение [2]. Множество $V \subseteq B^n$ называется кодом, исправляющим ошибки канала $K(\Psi)$, если выполнено условие

$$\psi_i(u) \neq \psi_j(v) \quad (3)$$

для всех i и j и для всех слов $u, v \in V$.

Условие (3) означает, что последствия действий канала $K(\Psi)$ на кодовые слова различны и поэтому ошибки 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 – $\bar{V}(\Psi)$.

Итак, пусть опять $\Psi(0) = \{y_0, y_1, \dots, y_m\} \subseteq B^n$ и канал $K(\Psi)$ действует на слово $x \subseteq B^n$ следующим образом:

$$z = x \mathbf{V} y_i, \quad i = \overline{0, m},$$

и знак « \mathbf{V} » – словарная функция, определяемая стандартным образом: если $z = (\gamma_1 \gamma_2 \dots \gamma_n)$, $x = (\alpha_1 \alpha_2 \dots \alpha_n)$, $y = (\beta_1 \beta_2 \dots \beta_n)$, то

$$\gamma_i = \alpha_i \mathbf{V} \beta_i, \quad i = \overline{1, n}.$$

Таким образом, преобразование слов в дизъюнктивном канале – дизъюнкция соответствующих слов, а не сумма по mod 2, как в аддитивном канале.

Пример 1. Если $\Psi(0) = \{y_0 = (000), y_1 = (100), y_2 = (011), y_3 = (111)\}$, то при $x = (001)$ на выходе дизъюнктивного канала $K(\Psi)$ получается одно из следующих слов: $z_0=(001), z_1=(101), z_2=(011), z_3=(111)$. Если же $x=(110)$, то $z_0=(110), z_1=(101), z_2=(111), z_3=(111)$.

По аналогии с аддитивным каналом дизъюнктивный канал $K(\Psi)$, порождаемый множеством $\{y_0, y_1, \dots, y_m\}$, соответствует таблице декодирования $D(\Psi)$ при заданном коде $V = \{v_0, v_1, \dots, v_N\}$

v_0	v_1	...	v_N
$v_0 \vee y_0$	$v_1 \vee y_0$		$v_N \vee y_0$
$v_0 \vee y_1$	$v_1 \vee y_1$		$v_N \vee y_1$
...
...
$v_0 \vee y_m$	$v_1 \vee y_m$		$v_N \vee y_m$

Определение кода $V = \{v_0, v_1, \dots, v_N\}$, исправляющего ошибки дизъюнктивного канала $K(\Psi)$ с порождающим множеством $\Psi(0) = \{y_0, y_1, \dots, y_m\}$, копирует предыдущие определения аддитивного канала и состоит в следующем:

$$v_i \vee y_r \neq v_j \vee y_s.$$

В «физическом» смысле дизъюнктивный канал $K(\Psi)$ действует следующим образом: букву «1» он не меняет, а букву «0» может перевести в 0 или 1.

В стандартных терминах дизъюнктивный канал действует на букву «несимметричным» образом.

Замечание. Множество B^n с бинарной операцией *дизъюнкция* образует моноид с нейтральным элементом «0». Эта структура гораздо более бедная, чем группа $(B^n, +)$, и потому многие из свойств аддитивных каналов не выполняются для дизъюнктивных каналов. Так, если для аддитивного канала в каждом столбце таблицы декодирования $D(\Psi)$ содержится одно и то же число элементов, то для дизъюнктивного канала это вовсе не так.

Пример 2. Пусть $\Psi(0) = \{y_0 = (000), y_1 = (011), y_2 = (001)\}$,
 $V = \{v_0 = (000), v_1 = (100), v_2 = (010)\}$.

Тогда таблица декодирования $D(\Psi)$ дизъюнктивного канала $K(\Psi)$ имеет следующую форму:

000	100	010
000	100	010
011	111	011
001	101	011

Очевидно, что для канала $K(\Psi)$ и кода V условия (4) не выполняются.

Пример 3. Если в дизъюнктивном канале $K(\Psi)$ происходит не более одного «искажения», то формальная запись канала состоит в следующем:

$$\Psi(0) = \{e_0 = (00 \dots 0), e_1 = (10, \dots 0), \dots, e_n = (00 \dots 01)\}.$$

Если $V = \{v_0, v_1, \dots, v_N\}$, то таблица декодирования выглядит так:

v_0	v_1	...	v_N
$v_0 V e_0$	$v_1 V e_0$		$v_N V e_0$
$v_0 V e_1$	$v_1 V e_1$		$v_N V e_1$
...
...
$v_0 V e_n$	$v_1 V e_n$		$v_N V e_n$

Рассмотрим k -й столбец таблицы декодирования $D(\Psi)$. Если $\{l_1, l_2, \dots, l_r\}$ – номера нулей у слова v_k , то все элементы столбца – слова, отличающиеся от v_k в разрядах с номерами $\{l_1, l_2, \dots, l_r\}$. Поэтому общее число различных слов в столбце с учетом самого v_k равно $r+1 = n - \|v_k\| + 1$.

В общем виде, если D_1, D_2, \dots, D_N столбцы таблицы декодирования $D(\Psi)$, то справедлива следующая верхняя граница.

Утверждение 1. *Имеет место неравенство*

$$|D_k| \leq \min \{2^{n-\|v_k\|}, m\}.$$

Доказательство. Если $\{l_1, l_2, \dots, l_r\}$ – номера нулей у слова v_k , то к новым словам приводят изменения v_k в позициях $\{l_1, l_2, \dots, l_r\}$ и их общее количество равно $2^{n-\|v_k\|}$.

С другой стороны, по определению, общее число различных слов в D_k не превосходит m .

В качестве содержательного примера, завершающего этот параграф, рассмотрим канал из примера 3, в котором происходит не более одного искаженного символа в слове $x = (\alpha_1 \alpha_2 \dots \alpha_n)$.

Следующее утверждение содержит верхнюю границу для мощности кода V , исправляющего ошибки приведенного выше канала.

Утверждение 2. *Справедливо неравенство*

$$|V| \leq \min_{\lambda} \left\{ \sum_{k \leq \lambda} \binom{n}{k} + \frac{2^n}{n - \lambda + 1} \right\}.$$

Доказательство. Пусть

$$V_1 = \{x \in V; \|x\| \leq \lambda\}, \quad V_2 = \{x \in V; \|x\| > \lambda\}.$$

Тогда

$$V = V_1 \cup V_2, \quad V = V_1 \cap V_2 = \emptyset \text{ и}$$

$$|V_1| \leq \sum_{k \leq \lambda} \binom{n}{k}, \quad |V_2| \leq \frac{2^n}{n - \lambda + 1}.$$

Первое неравенство следует из того, что общее число точек $x \in V$ с $\|x\| \leq \lambda$ не превосходит общего числа точек из B^n со свойством $\|x\| \leq \lambda$, т.е.

$$|V_1| \leq \sum_{k \leq \lambda} \binom{n}{k}. \quad (5)$$

Если $x \in V_2$, то в силу примера 3

$$|V_2| \leq \frac{2^n}{n - \lambda + 1}, \quad (6)$$

так как число элементов в любом столбце таблицы декодирования для V_2 не превосходит правой части (6).

Утверждение 3. *Справедливо неравенство*

$$|V| \lesssim \frac{2^{n+1}}{n}.$$

Доказательство. Так как [5]

$$\binom{n}{\lambda} \sim \frac{2^{n+1}}{\sqrt{2\pi n}} e^{-\frac{(2\lambda-n)^2}{2n}},$$

то при $\lambda = \frac{n}{2} - \omega\sqrt{n}$, $\omega(n) = o(\sqrt{n})$ имеем

$$\left(\frac{n}{\frac{n}{2} - \omega\sqrt{n}} \right) = O\left(\frac{2n}{\sqrt{n}} e^{-2\omega^2} \right)$$

Выбрав $\omega = \sqrt{\ln n}$, мы получим оценку

$$|V^1| \lesssim O\left(\frac{2^n}{n^2 \sqrt{n}} \right)$$

Следовательно, с учетом (5) и (6)

$$|V| \lesssim \frac{2^{n+1}}{n}$$

Исправление ошибок в дизъюнктивном канале. Если в дизъюнктивном канале происходит не более одного искажения, то для исправления ошибки можно использовать обычный код Хэмминга. Однако, используя специфику этого канала, можно предложить более эффективные способы борьбы с помехами. Одним из таких способов является использование кода Варшавова – Тененгольца [6].

Рассмотрим сравнения

$$\alpha_1 + 2\alpha_2 + 3\alpha_3 + \dots + n\alpha_n \equiv 0 \pmod{(n+1)}, \quad (7)$$

где $x = (a_1 a_2 \dots a_n) \in B^n$.

Множество решений сравнений (7) обозначим через S^n .

Утверждение 4. Код S^n исправляет все одиночные искажения канала.

Доказательство. Пусть $x = (a_1 a_2 \dots a_n) \in S^n$ и ошибка произошла в r -разряде слова x . По определению кода S^n , если на выходе мы получаем слово

$$z = (\gamma_1 \gamma_2 \dots \gamma_n), \text{ то}$$

$$l(z) = \sum_{i=1}^n i\gamma_i = \sum_{i=1}^n i\alpha_i + r. \quad (8)$$

Из (8) получим

$$l(z) \pmod{(n+1)} = \left(\sum_{i=1}^n i\alpha_i + r \right) \pmod{(n+1)}. \quad (9)$$

Из (9) получим $l(z) \pmod{(n+1)} = r$.

Таким образом, мы получаем номер разряда, в котором произошла ошибка.

Изменив значение этого разряда, мы исправляем искомую ошибку.

Пример 4. Если $n=4$, то исходное сравнение имеет вид

$$\alpha_1 + 2\alpha_2 + 3\alpha_3 + 4\alpha_4 \equiv 0 \pmod{5}.$$

Слово $x=(1001)$ принадлежит S^4 . Если ошибка произошла в 3-м разряде, то

$$z=(1011) \text{ и } l(z)=l(1011)=1+3+4=8.$$

Далее $l(z) \equiv 3 \pmod{5}$ и номер ошибочного разряда определен.

Отметим, что множество коэффициентов линейной формы $L(x)=\alpha_1 + 2\alpha_2 + \dots + n\alpha_n$ – кольцо классов вычетов по $\text{mod}(n+1)$, т.е. множество $\{0, 1, \dots, n\}$.

Это обстоятельство играет определенную роль при исследовании множества решений сравнения

$$L(x) \equiv 0 \pmod{(n+1)}.$$

Рассмотрим сравнения

$$c(\alpha_1\alpha_2\dots\alpha_n) = \sum_{i=1}^n d_i\alpha_i \equiv 0 \pmod{d}. \quad (10)$$

Здесь все параметры d_i, d – натуральные числа и $x=(\alpha_1\alpha_2\dots\alpha_n) \in B^n$.

Обозначим через $t_d(d_1d_2\dots d_n)$ число решений сравнения (10).

Утверждение 5. *Справедливо соотношение*

$$t_d(d_1d_2\dots d_n) = \frac{1}{d} \sum_{s=0}^{d-1} \prod_{r=1}^n \left(1 + e^{\frac{2\pi i}{d}sd_r}\right). \quad (11)$$

Доказательство. Используем известное соотношение, выражающее свойства делимости

$$\frac{1}{d} \sum_{s=0}^{d-1} e^{\frac{2\pi i}{d}xs} = \begin{cases} 1, & \text{если } d|x \\ 0, & \text{если } d \nmid x \end{cases}. \quad (12)$$

Если вместо x в формулу (12) подставить функцию $c(\alpha_1\alpha_2\dots\alpha_n)$, то после некоторых стандартных манипуляций получим

$$t_d(d_1d_2\dots d_n) = \frac{1}{d} \sum_{(\alpha_1\alpha_2\dots\alpha_n)} \sum_{s=0}^{d-1} e^{\frac{2\pi i}{d}c(\alpha_1\alpha_2\dots\alpha_n)s} = \frac{1}{d} \sum_{s=0}^{d-1} \left(1 + e^{\frac{2\pi i}{d}sd_1}\right)$$

... $\left(1 + e^{\frac{2\pi i}{d}sd_n}\right)$, что и доказывает (11).

Выделив в формуле (11) слагаемое, соответствующее $s = 0$, получим

$$t_d(d_1d_2\dots d_n) = \frac{2^n}{d} + \frac{1}{d} \sum_{s=1}^{d-1} \left(1 + e^{\frac{2\pi i}{d}sd_1}\right) \dots \left(1 + e^{\frac{2\pi i}{d}sd_n}\right),$$

отсюда, используя известные арифметические функции, имеем

$$|S_n| = t_{n+1}(1, 2, \dots, n) \gtrsim \frac{2^{n+1}}{n}.$$

¹ФИЦ ИУ РАН

²Группа Бит, Москва

³Ереванский государственный университет

e-mails: vkleontiev@yandex.ru, garib@hkzap.ru, j.margaryan@ysu.am

Վ. Կ. Լեոնտև, Գ. Լ. Մովսիսյան, Ջ. Գ. Մարգարյան

Дизъюнктивные каналы

Введено понятие дизъюнктивного канала связи, являющегося неалгебраическим комбинаторным каналом, по форме напоминающим аддитивный канал, а по существу отличающимся от него. Предложен способ исправления всех одиночных искажений, происходящих в данном канале связи.

Վ. Կ. Լեոնտև, Գ. Լ. Մովսիսյան, Ջ. Գ. Մարգարյան

Դիզյունկտիվ կապուղիներ


Ներմուծված են դիզյունկտիվ կապուղիներ, որոնք կոմբինատոր ոչ հանրահաշվական են: Դիզյունկտիվ կապուղիները ձևով նման են ադիտիվ կապուղիներին, բայց էսպես տարբերվում են նրանցից: Բերված է այդպիսի կապուղիներում բոլոր սխալներն ուղղելու եղանակ:

V. K. Leontiev, G. L. Movsisyan, Zh. G. Margaryan

Disjunctive Channels

The article introduces the concept of a disjunctive communication channel, which is a non-algebra combinatorial channel, though resembling an additive channel by its form, but different from it by its essence. A method for correcting all single distortions occurring in a given communication channel is proposed.

Литература

1. *Leontiev V. K., Movsisyan G. L.* In: The First International. Algebra and Geometry Conference 16-20 may 2007, Yerevan, Armenia. P. 16-20.
2. *Լեոնտև Վ. Կ., Մովսիսյան Գ. Լ.* – Доклады НАН РА. 2004. Т. 104. № 1. С. 23-27.
3. *Լեոնտև Վ. Կ., Մովսիսյան Գ. Լ., Օսիպյան Ա. Ա.* В: Матер. XI междунар. семинара «Дискретная математика и ее приложение». М. Изд-во МГУ. 2012. с.415-416. 
4. *Левенштейн В. И.* – ДАН СССР. 1965. Т. 163. № 4. С. 845-848.
5. *Гаврилов Г. П., Сапоженко А. А.* Сборник задач по дискретной математике. М. Наука. 1977. 368 с.
6. *Вариамов Р. Р., Тененгольц Г. М.* – Автоматика и телемеханика. 1965. Т. 26. № 2. С. 288-292.