

МАТЕМАТИКА

УДК 621.391.15

В. К. Леонтьев, Г. Л. Мовсисян

О каналах связи

(Представлено академиком Ю.Г. Шукуряном 23/Х 2007)

Ключевые слова: код, канал связи, защита информации, преобразование слов, алгоритм, максимальная мощность

Существует много различных определений каналов связи, моделирующих те или иные содержательные ситуации. Это и двоичный симметричный канал (Д.С.К.), стирающий канал, аддитивный канал, квантовый канал, канал передачи наследственной информации и т.д. Общим для всех этих каналов является то обстоятельство, что в них происходит преобразование одних слов в другие, т.е. реализуется некоторая словарная функция. Одной из целей "защиты информации" при передаче по каналу связи является возможность надёжного воспроизведения переданного сообщения на приёмном конце. Так возникает классическая ситуация кодирования с коррекцией ошибок.

Другая ситуация защиты информации связана с предотвращением возможности дезинформации, т.е. защитой приёмника от заведомо ложной информации, которая может появиться как в результате случайных искажений, так и при несанкционированном доступе к каналу. Таким образом, возможны различные определения кодирования с целью защиты информации.

Целью настоящей работы является рассмотрение довольно общей ситуации, связанной как с каналом связи, так и с защитой информации, передаваемой по этому каналу. Канал задаётся множеством преобразований, реализующих некоторые словарные функции, а защита информации связана с понятием "запретного множества", моделирующего ситуацию информационной угрозы.

Пример 1. Пусть $B = \{0, 1\}$ – двоичный алфавит, $B^n = \{0, 1\}^n$ и $t \leq n$. Предположим, что за время передачи слова длины n из B^n в нём происходит

не более чем t искажений вида: $0 \rightarrow 1, 1 \rightarrow 0$. Тогда каждое отображение T вида

$$B^n \xrightarrow{T} B^n$$

с условием $\rho(x, Tx) \leq t$, где $\rho(\cdot)$ — расстояние Хэмминга, является словарной функцией, соответствующей конкретному виду реализации обозначенных выше искажений. Ясно, что число таких словарных функций равно $(\sum_{i=0}^t \binom{n}{i})^{2^n}$.

Пример 2. Если $B = \{a_1, a_2, \dots, a_m\}$ — m -буквенный алфавит и S_m — симметрическая группа, действующая на B , то преобразование вида

$$b_1 b_2 \dots b_n \rightarrow g(b_1) g(b_2) \dots g(b_n),$$

где $b_i \in B$ и $g \in S_m$, является словарной функцией, осуществляющей стандартное криптографическое преобразование, являющееся шифром замены.

Пример 3. Пусть $A = \|\alpha_{ij}\|_{m \times n}$ — булева матрица из классического матричного кольца над полем Галуа $F_2 = \{0, 1\}$ и $x \in B^n = \{0, 1\}^n$. Для произвольной последовательности $\{A_i, b_i\}_1^N$ матриц и векторов "аффинный канал" определяется как преобразование вида

$$y = A_i x^T + b_i, \quad i = \overline{1, N}, \quad (1)$$

где $x \in B^n$. Если $A_i = E$, то преобразование (1) определяет обычный аддитивный канал (см. [1]).

В общем случае будем считать, что имеются конечный алфавит $B = \{a_1, a_2, \dots, a_m\}$, множество всех слов B^* конечной длины над алфавитом B , некоторое выделенное подмножество $M \subseteq B^*$ и группа преобразований $T = \{T_i\}$, действующая на M . При этом выполняется условие: $T_i(M) \subseteq M$ для $T_i \in T$.

Определение 1 (см. [2]). *Множество преобразований $T^* \subseteq T$ определяет алгебраический канал, если выполнено условие*

$$T_i \in T^* \rightarrow T_i^{-1} \in T^*. \quad (2)$$

Содержательно условие (2) означает, что любое преобразованное каналом T^* слово может быть возвращено к исходному виду путём "тех же самых" трансформаций.

Следующее понятие связано с определением кода с защитой информации.

Пусть $V = \{v_1, v_2, \dots, v_N\}$ — код и $V \subseteq M$. Если по каналу T^* передаются слова из V , то на приёмном конце мы получаем преобразованные слова:

$v_i = T_i(v)$. Для того чтобы информация, связанная с v , была защищена, необходимо потребовать от преобразованного слова v' , чтобы оно не попало в "запретное" множество, зависящее от слова v , кода V и отношения запрета Vor . Это запретное множество мы обозначим через $Vor(M, V, v)$ или просто $Vor(v)$.

Определение 2. Код V защищает информацию от угрозы Vor , если выполнено соотношение

$$T_i(v) \cap Vor(v) = \emptyset \text{ для } v \in V. \quad (3)$$

Пример 4. Если в качестве канала T^* понимать стандартный двоичный канал из примера 1, а под защитой информации понимать возможность однозначно восстановить любое кодовое слово, в котором произошло не более чем t искажений, то мы приходим к стандартной задаче теории кодов, исправляющих ошибки. В этом случае

$$T_i(v) = v + x, \quad (4)$$

где $\|x\| \leq t$ и запретное множество $Vor(v_i)$ для $V = \{v_1, v_2, \dots, v_N\}$ выглядит следующим образом:

$$Vor(v_i) = \bigcup_{j \neq i} S_t(v_j),$$

где $S_t(v_j)$ — шар Хэмминга радиуса t с центром в точке $v_j \in B^n$. При этом условие (3) трансформируется следующим образом:

$$T(v_i) \cap \left\{ \bigcup_{j \neq i} S_t(v_j) \right\} = \emptyset \quad (5)$$

для любого преобразования T вида (4).

Геометрически условие (5) означает, что искажённое слово $v'_i = T(v_i)$ не попадает ни в одну из t -окрестностей кодовых точек, отличных от v_i . Стандартным образом условие (5) записывают в виде

$$T_i(v_s) \neq T_j(v_r).$$

Пример 5. Пусть $F(x) = F(x_1, x_2, \dots, x_n)$ — произвольная булева функция и $N_F = \{x : F(x) = 1\}$ — множество единиц функции $F(x_1, x_2, \dots, x_n)$. Через T^* мы обозначим канал связи, определённый множеством преобразований T^* .

Определение 3. Подмножество $V \subseteq N_F$ называется кодом без дезинформации (б.д.и.-кодом), если $T^*(V) \subseteq N_F$.

Содержательно это определение означает, что преобразования канала T^* не должны "истинные" утверждения (единицы булевой функции F)

переводить в "ложные", т.е. в нули этой функции. В частности, если $F(x)$ — самодвойственная функция, т.е. $\bar{F}(x) = F(\bar{x})$, то выполняется следующее соотношение: $x \in N_F \Leftrightarrow \bar{x} \in \bar{N}_F$.

Если $T^* = \{y_1, y_2, \dots, y_m\}$ — аддитивный канал и $V = \{v_1, v_2, \dots, v_N\}$ — б.д.и.-код, то выполняется условие $v_i + y_j \notin \bar{N}_F$.

Пусть $T^* = \{T_i^*\}$ — алгебраический канал.

Определение 4. *Окрестностью 1-го порядка слова $v \in M$ называется множество слов $S^1(v)$, порождаемых семейством преобразований T^* , т.е.*

$$S^1(v) = \{T_i^*(v), T_i^* \in T^*\}. \quad (6)$$

Замечание. В стандартных алгебраических терминах $S^1(v)$ — это транзитивное множество или орбита элемента v . Разница состоит лишь в том, что семейство преобразований T^* , вообще говоря, не является группой.

Окрестности высших порядков элемента $v \in M$ определяются индуктивно ("окрестность от окрестности"), исходя из (6) (см. [3,4]).

Первая классическая проблема, связанная с алгебраическим каналом T^* , состоит в построении кода максимальной мощности, исправляющего ошибки этого канала. Такую мощность мы обозначим через $A(M, T^*)$.

Следующая процедура построения кода, исправляющего ошибки алгебраического канала T^* , является прямым аналогом стандартного алгоритма Варшавова — Гилберта.

1) В качестве первой кодовой точки мы выбираем произвольное слово $v_1 \in M$.

2) Строим окрестность 2-го порядка точки v_1 , т.е. строим множество $S^2(v_1)$, и в качестве точки v_2 выбираем произвольный элемент множества $M_1 = M \setminus S^2(v_1)$.

3) В качестве v_k выбираем произвольный элемент из M_{k-1} , где

$$M_{k-1} = M \setminus \bigcup_{i=1}^{k-1} S^2(v_i).$$

4) Алгоритм заканчивает свою работу при отсутствии возможности выбора.

Пусть

$$S^1(M) = \min_{v \in M} |S^1(v)|,$$

$$S^2(M) = \max_{v \in M} |S^2(v)|.$$

Теорема 1. *Справедливы следующие оценки:*

$$\frac{|M|}{S^2(M)} \leq A(M, T^*) \leq \frac{|M|}{S^1(M)}.$$

Отметим, что мощность кода V , построенного путём применения алгоритма Варшамова – Гилберта, зависит от стратегии выбора точек на каждом шаге алгоритма. Однако существуют специальные классы каналов T^* , для которых изложенная выше процедура всегда приводит к коду одной и той же мощности, т.е. строит оптимальный код.

Теорема 2. *Если T^* – группа преобразований, то*

$$A(M, T^*) = \frac{1}{|T^*|} \sum_{T_i^* \in T^*} |N(T_i^*)|, \quad (7)$$

где $N(T_i^*)$ – множество неподвижных точек преобразования T_i^* , т.е.

$$N(T_i^*) = \{v : T_i^*(v) = v, v \in M\}.$$

Формула (7) является следствием классической комбинаторной леммы Бернсайда (см. [5]).

Следствие 1 (см. [3]). *Пусть $T^* = \{y_1, y_2, \dots, y_m\}$ – аддитивный канал, порождаемый группой $G = \{y_1, y_2, \dots, y_m\}$, где G – подгруппа группы B^n . Тогда справедливо равенство*

$$A(B^n, G) = \frac{2^n}{m}.$$

Следствие 2. *Пусть $M = B^n$ и $T^* = \{T^n\}$ – группа циклических сдвигов. Тогда*

$$A(B^n, T^*) = \frac{1}{n} \sum_{d|n} 2^d \varphi(n/d).$$

Здесь $\varphi(n)$ – функция Эйлера или число чисел, меньших n и взаимно простых с n .

Отметим, что в свете вышеизложенного вполне уместно рассмотреть каналы, в которых могут одновременно возникать как "локальные" ошибки типа стандартных искажений двоичных символов, так и "глобальные" изменения типа циклических сдвигов.

Вычислительный центр РАН

В. К. Леонтьев, Г. Л. Мовсисян

О каналах связи

Для определённых классов каналов связи приведены оценки мощности кода, аналогичные оценкам Варшамова – Гилберта и сферической упаковки. Доказано, что для специальных классов каналов связи код, построенный путём применения алгоритма Варшамова – Гилберта, оптимален.

Վ. Կ. Լեոնտև, Գ. Լ. Մովսիսյան

Կապի գծերի մասին

Կապի գծերի որոշակի դասերի համար բերված են կոդի հզորության Վարշամով – Շիրերտի և գնդային փաթեթավորման նմանապիսի գնահատականներ: Ապացուցված է, որ հարուկ տիպի կապի գծերի համար Վարշամով – Շիրերտի գնահատականի՝ ալգորիթմով կառուցված կոդը օպտիմալ է:

V. C. Leontev, Gh. L. Movsisyan

On Connection Channels

We have proposed the power limits of the code for the definite classes of connection channels which are analogical to those by Varshamov - Gilbert and to those of the spherical packing. It has been proved that the code built by applying the Varshamov - Gilbert algorithm is optimal for the special classes of connection channels.

Литература

1. Деза М.Е. - Проблемы передачи информации. М. 1965. Т. 1. N3. С. 29-39.
2. Леонтьев В.К., Мовсисян Г.Л. - The First International Algebra and Geometry Conference. Yerevan, Armenia. 2007. С. 16-20.
3. Леонтьев В.К., Мовсисян Г.Л. - ДНАН Армении. 2004. Т. 104. N1. С. 23-28.
4. Леонтьев В.К., Мовсисян Г.Л., Маргарян Ж.Г. - Докл. РАН. 2006. Т. 411. N3. С. 306-308.
5. де Брейн Н.Дж. В сб.: Прикладная комбинаторная математика. М. Мир. 1968. С. 61-106.
6. Margaryan Zh., Movsisyan G., Leont'ev V. In: Computer Science and Information Technologies. Yerevan. 2005.