

другие, то достаточно общий канал можно описать следующим образом.

Заданы некоторое множество $\Psi = \{\psi_0, \psi_1, \dots, \psi_m\}$ частичных словарных функций $B^* \xrightarrow{\psi_i} B^*$, $i = \overline{0, m}$, 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 T . 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. *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 $\psi_0(v), \psi_1(v), \dots, \psi_m(v)$. 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 $\psi_i(v)$.

§2. Восстановление искаженного сигнала. После передачи некоторого слова v по имеющемуся каналу связи на выходе мы получаем слово u . В классической постановке требуется восстановить исходное слово v по его искаженному образу u с максимально возможной достоверностью. Точная постановка задачи борьбы с искажениями, происходящими в канале связи, принадлежит К. Шеннону [2]: на входе канала известно некоторое множество слов из B^n , которое содержит все потенциально возможные сообщения, годные для передачи. Множество сообщений на выходе мы будем считать некоторым подмножеством из B^n . Проблема кодирования состоит в выборе такого семейства сообщений $V = \{v_0, v_1, \dots, v_N\}$, что при получении на выходе канала сообщения $u \in B^n$ мы можем однозначно декодировать переданное сообщение.

Следуя стандартным традициям, любое подмножество V из B^n мы будем называть кодом V , который и используется для связи, т.е. передаваться по каналу могут только слова кода V . Таким образом, каждое слово u , полученное на выходе канала, является образом кодового слова. И мы хотим восстановить исходное слово $v \in V$ по его образу. Здесь основное искусство состоит в правильном выборе кода V , позволяющего однозначно восстановить исходное сообщение по любому искаженному сигналу.

Что касается выбора кода V , то это фактически выбор необходимой избыточности в передаваемой информации для обеспечения нужной

достоверности. Поскольку избыточность приводит к увеличению времени работы канала и, следовательно, уменьшению скорости передачи информации в канале, то при принятии решения, учитывая как характеристики канала, так и способ декодирования, мы должны обеспечить баланс между необходимой достоверностью и скоростью передачи.

Возможность нахождения такого баланса основывается на теореме Шеннона: для определенного канала связи существуют коды со скоростью передачи, меньшей пропускной способности канала, обеспечивающие сколь угодно большую достоверность.

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

$$\psi_i(u) \neq \psi_j(v) \quad (2)$$

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

Условие (2) 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.

Ясно, что мощность кода $V(\Psi)$ зависит от «структуры» и мощности множества Ψ , «порождающего» канал $K(\Psi)$, и т.д. В других терминах, условие (2) можно естественным образом увязать с понятием «окрестности» и сформулировать эквивалентные понятия, используемые в дальнейшем.

Окрестность k -го порядка слова v определим следующим образом (индуктивно): $\Psi^k(v) = \Psi^1(x)$, $x \in \Psi^{k-1}(v)$, где $\Psi^0(v) = v$, $\Psi^1(v) = \Psi(v)$.

При этом выполняются включения $\Psi^0(v) \subseteq \Psi^1(v) \subseteq \dots \subseteq \Psi^k(v)$.

В терминах окрестностей условие, что код $V = \{v_0, v_1, \dots, v_N\}$ исправляет ошибки канала $K(\Psi)$, можно сформулировать следующим образом:

$$\Psi^1(v_i) \cap \Psi^1(v_j) = \emptyset, \quad i \neq j. \quad (3)$$

Нетрудно проверить, что условия (2) и (3) являются эквивалентными.

Определение кода V , исправляющего ошибки канала $K(\Psi)$, в значительной мере копирует классическое определение кода, исправляющего искажения типа $\mathbf{0} \rightarrow \mathbf{1}$, $\mathbf{1} \rightarrow \mathbf{0}$ в двоичном симметричном канале [2].

В содержательном смысле код V должен быть устроен так, чтобы по любому искаженному сигналу исходное сообщение восстанавливалось однозначно, т.е. предполагается существование однозначного декодирования. То обстоятельство, что код V исправляет ошибки канала $K(\Psi)$, можно формально записать двухместным предикатом:

$$X(\Psi, V) = \begin{cases} 1, & \text{если } V \text{ исправляет ошибки } K(\Psi), \\ 0, & \text{в противном случае.} \end{cases}$$

Предикат $X(\Psi, V)$ описывает «взаимоотношения» канала $K(\Psi)$ и кода V и обладает следующим свойством: $X(\Psi, V) = X(\varphi\Psi, V)$, где φ – произвольное обратимое преобразование из T .

Следовательно, код V исправляет или не исправляет ошибки каналов $K(\Psi)$ и $K(\varphi\Psi)$ одновременно, т.е. каналы $K(\Psi)$ и $K(\varphi\Psi)$ для обратимого преобразования φ обладают одинаковыми свойствами в смысле коррекции ошибок, поэтому каналы $K(\Psi)$ и $K(\varphi\Psi)$ естественно считать неразличимыми, и в дальнейшем мы всегда будем считать, что $\psi_0(x) = x$, что можно интерпретировать как возможность безошибочной передачи слова по этому каналу, $W = B^n \subseteq B^*$, где $B = \{0, 1\}$. Следовательно, на множестве B^n действует группа преобразования T , которая переводит слово из B^n в слово из этого же множества. 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.

В основе понятия классификации семейства каналов $\{K(\Psi)\}$ лежит соотношение канала $K(\Psi)$ и кода V , т.е. значение предиката $X(\Psi, V)$. Следующее определение представляет один из вариантов разбиения каналов связи на классы эквивалентности.

Введем на множестве каналов бинарное отношение

$$K(\Psi) \leq K(\Phi) \tag{4}$$

следующим образом:

$K(\Psi) \leq K(\Phi)$, если $(X(\Phi, V) = 1) \rightarrow (X(\Psi, V) = 1)$ для всех $V \subseteq B^n$.

Определение. Канал $K(\Psi)$ слабее канала $K(\Phi)$, если любой код V , исправляющий ошибки канала $K(\Phi)$, исправляет и ошибки канала $K(\Psi)$.

Это бинарное отношение $K(\Psi) \leq K(\Phi)$ определяет отношение предпорядка на множестве всех каналов $\{K(\Psi)\}$. Однако отношения $K(\Psi) \leq K(\Phi)$, $K(\Phi) \leq K(\Psi)$ не влекут $K(\Psi) = K(\Phi)$, т.е. отношение (4) не является частичным порядком.

Ясно, что всегда имеет место $\Psi \subseteq \Phi \rightarrow K(\Psi) \leq K(\Phi)$. При этом из $K(\Psi) \leq K(\Phi)$ не всегда следует, что $\Psi \subseteq \Phi$.

Пример 1. Рассмотрим каналы $K(\Phi_1), K(\Phi_2), K(\Phi_3)$, где $\Phi_1(x) = \{x + y_0, \dots, x + y_m\}$, $\Phi_2(x) = \{x + y_0, \dots, x + y_m, x + y_{m-1} + y_m\}$, $\Phi_3(x) = \{x + y_0, \dots, x + y_m, x + y_{m+1}\}$.

Нетрудно убедиться, что $K(\Phi_3) \leq K(\Phi_2) \leq K(\Phi_1)$ и $K(\Phi_2) \leq K(\Phi_3)$. Однако в общем случае ни одно из следующих соотношений не имеет места: $\Phi_1 = \Phi_2$, $\Phi_2 = \Phi_3$, $\Phi_2 \subseteq \Phi_3$, $\Phi_3 \subseteq \Phi_2$.

Определение. Если $K(\Psi) \leq K(\Phi)$ и $K(\Phi) \leq K(\Psi)$, то каналы $K(\Psi)$ и $K(\Phi)$ называют эквивалентными и обозначают $K(\Psi) \sim K(\Phi)$.

Формально отношение эквивалентности каналов $K(\Psi)$ и $K(\Phi)$ можно записать так: $K(\Psi) \sim K(\Phi) \Leftrightarrow X(\Psi, V) = X(\Phi, V)$ для любого $V \subseteq B^n$.

Класс эквивалентности $M(\Psi)$ определяется как множество $M(\Psi) = \{K(\Phi); K(\Phi) \sim K(\Psi)\}$.

Ясно, что для любых каналов $K(\Psi), K(\Phi)$ из одного класса эквивалентности имеет место равенство $M(\Psi) = M(\Phi)$.

§3. Отношения между алгебраическими каналами связи. Определение [3]. Комбинаторный канал $K(\Psi)$ называется *алгебраическим каналом*, если выполняется условие

$$\psi_i \in \Psi \rightarrow \psi_i^{-1} \in \Psi. \quad (5)$$

Это условие требует, чтобы любое «преобразованное» слово могло быть возвращено к исходному виду путем тех же самых трансформаций. Отметим, что любой аддитивный канал удовлетворяет условию (5) и является алгебраическим [4-6]. Однако не все комбинаторные матричные каналы являются алгебраическими, например, матричный канал с выпадением символов [7, 8]. При этом матричный канал с инверсией является алгебраическим [7].

Пусть $\Psi = \{\psi_0, \psi_1, \dots, \psi_{m_1}\}$, $\Phi = \{\varphi_0, \varphi_1, \dots, \varphi_{m_2}\}$.

Теорема 1. *Алгебраические каналы $K(\Psi)$ и $K(\Phi)$ эквивалентны тогда и только тогда, когда существует $\varphi \in T$ такое, что $K(\Phi_1)$ является алгебраическим и*

$$\Psi^2 = \Phi_1^2,$$

где $\Phi_1 = \{f_0, f_1, \dots, f_{m_2}\}$, $f_i = \varphi \varphi_i$.

Доказательство. Достаточность. Пусть для некоторых $\varphi \in T$ канал $K(\Phi_1)$ является алгебраическим и $\Psi^2 = \Phi_1^2$. Предположим, что код $V(\Psi)$ не исправляет ошибки канала $K(\Phi)$. Т.е. имеем $X(\Phi, V(\Psi)) = 0$.

Отсюда следует, что $\varphi_i(u) = \varphi_j(v)$ и поэтому $f_i(u) = f_j(v)$ для некоторых $0 \leq i, j \leq m_2$ и $u, v \in V(\Psi)$, $i \neq j$, $u \neq v$. Следовательно,

$$f_j^{-1} f_i(u) = v. \quad (6)$$

Поскольку $f_j^{-1} \in \Phi_1$ и $\Psi^2 = \Phi_1^2$, то из (6) следует, что $v = f_j^{-1} f_i(u) \in \Psi^2(u)$. Т.е. $v = \psi_r \psi_s(u)$ для некоторых $0 \leq r, s \leq m_1$. Следовательно $\psi_r^{-1}(v) = \psi_s(u)$.

Отсюда следует, что $X(\Psi, V(\Psi)) = 0$, что является противоречием.

Необходимость. Теперь предположим, что $K(\Psi) \sim K(\Phi)$, но для любого $\varphi \in T$, для которого $K(\Phi_1)$ является алгебраическим каналом, имеем $\Psi^2 \neq \Phi_1^2$.

Не нарушая общности, предположим, что существуют $u \neq x$, $u \in \Psi^2(x)$, $u \notin \Phi_1^2(x)$, и рассмотрим код $V = \{x, u\}$. Из условия $u \notin \Phi_1^2(x)$ следует, что $u \neq f_i f_j(x)$ для всех $0 \leq i, j \leq m_2$. Значит, $f_i^{-1}(u) \neq f_j(x)$, и, следовательно, поскольку канал $K(\Phi_1)$ алгебраический, то $f_l = f_i^{-1} \in \Phi_1$ и $f_l(u) \neq f_j(x)$, поэтому $\varphi_l(u) \neq \varphi_j(x)$ для всех $0 \leq l, j \leq m_2$, т.е.

$$X(\Phi, V) = 1. \quad (7)$$

Далее, поскольку $y \in \Psi^2(x)$, то $y = \psi_r \psi_s(x)$ для некоторых $0 \leq r, s \leq m_1$.

Значит, $\psi_r^{-1}(y) = \psi_s(x)$ или $\psi_r^{-1}(y) = \psi_l(y) = \psi_s(x)$ для некоторых $0 \leq l, s \leq m_1$. Следовательно $X(\Psi, V(\Psi)) = 0$, что с учетом (7) противоречит условию $K(\Psi) \sim K(\Phi)$. Теорема доказана.

Следствие. Для алгебраических каналов $K(\Psi)$ и $K(\Phi)$ справедливо:

а) $\Psi^2 = \Phi^2 \rightarrow K(\Psi) \sim K(\Phi)$;

б) $K(\Psi) \leq K(\Phi) \Leftrightarrow \Psi^2 \subseteq (\varphi\Phi)^2$ для некоторого $\varphi \in T$.

Следствие. Для класса эквивалентности алгебраического канала $K(\Psi)$ имеет место

$$M(\Psi) = \{K(\varphi\Phi); \Psi^2 = \Phi^2, \varphi \in T\}.$$

Пример 2. Рассмотрим каналы из примера 1 при $m = 4$, $y_0 = (0000)$, $y_1 = (1000)$, $y_2 = (0100)$, $y_3 = (0110)$, $y_4 = (1010)$. Для алгебраического канала $K(\Phi_4)$ с порождающим множеством

$$\Phi_4(x) = \{Ax, Ax + (0001), Ax + (0010), Ax + (0110), Ax + (0101)\},$$

где

$$A = \begin{pmatrix} 0001 \\ 0010 \\ 0100 \\ 1000 \end{pmatrix}$$

имеем $M(\Phi_1) = M(\Phi_2) = M(\Phi_3) = M(\Phi_4)$.

Пусть $\{K(\Psi)\}$ – семейство всех алгебраических каналов. На этом множестве действует группа преобразования T следующим образом: для любых $K(\Psi)$ алгебраических каналов и $\varphi \in T$ преобразований $\varphi K(\Psi) = K(\varphi\Psi)$.

Таким образом, транзитивное множество, порожденное каналом $K(\Psi)$, выглядит стандартным образом: $G(\Psi) = \{K(\varphi\Psi); \varphi \in T\}$.

Пусть $\bar{G}(\Psi) \subseteq \{K(\Phi); \Phi^2 = \Psi^2\}$ – максимальное по мощности множество (одно из), состоящее из попарно неэквивалентных каналов.

Теорема 2. Семейство всех транзитивных множеств $\{G(\Psi), K(\Psi) \in \bar{G}(\Psi)\}$ порождает разбиение класса эквивалентности $M(\Psi)$. Т.е.

$$M(\Psi) = \bigcup_{K(\Psi) \in \bar{G}(\Psi)} G(\Psi).$$

При этом независимо от того, какие максимальные по мощности $\bar{G}(\Psi)$ выбраны, разбиение $M(\Psi)$ единственное.

Изучение каналов связи мы привели к изучению транзитивных множеств, а изучение транзитивных множеств – к изучению классов эквива-

лентности, которые в дальнейшем можно описать, введя отношения частичного порядка $M(\Psi) \leq M(\Phi)$, если $K(\Psi) \leq K(\Phi)$.

Следствие. Для алгебраических каналов $K(\Psi)$ и $K(\Phi)$ справедливо $M(\Psi) \leq M(\Phi) \Leftrightarrow \Psi^2 \subseteq (\varphi\Phi)^2$ для некоторого $\varphi \in T$. Следовательно, мы приходим к необходимости введения инварианта канала связи, характеризующего канал $K(\Psi)$ и как следствие класс эквивалентности $M(\Psi)$. Роль инварианта для любого $K(\Psi)$ играет множество $\Psi^2(x)$. К сожалению, вопрос «каждое ли подмножество из T является инвариантом какого-то канала» имеет отрицательный ответ. Достаточно рассмотреть следующий пример.

При $m=2$ или 4 для подмножеств $\{\varphi_0, \varphi_1, \dots, \varphi_m\} \subseteq T$, где $\varphi_i(x) = x + y_i$, не существует алгебраического канала с инвариантом $\{\varphi_0, \varphi_1, \dots, \varphi_m\}$.

Теорема 3. Если $K(\Psi)$ – алгебраический групповой канал, то:

1. Ψ является инвариантом для всех каналов из $M(\Psi)$;
2. канал связи $K(\varphi\Psi)$ для всех линейных преобразований φ из T является групповым;
3. $K(\Psi)$ имеет максимальную мощность в классе эквивалентности $M(\Psi)$;
4. $M(\Psi) = \{K(\varphi\Psi); \Psi^2 = \Psi, \varphi \in T\}$.

§4. Отношение между аддитивными каналами связи. Пусть $\Psi(0) = \{y_0, y_1, \dots, y_m\}$ – подмножество B^n . Тогда с порождающим множеством Ψ связывается понятие аддитивного канала $K(\Psi)$ следующим образом [9].

Любое из слов $x \in B^n$ в канале $K(\Psi)$ преобразуется в одно из слов вида

$$\psi_0(x), \psi_1(x), \dots, \psi_m(x), \psi_i(x) = x + y_i, i = \overline{0, m}. \quad (8)$$

Таким образом, каждое из преобразований вида (8) осуществляет «сдвиг» на слово y_i . В результате «сдвига» y_i слово x преобразуется в другое слово y_i , которое может совпадать с x , если $y_i = (0 \ 0 \ \dots \ 0)$.

Интерес к аддитивному каналу связи как некоторому преобразователю информации объясняется тем обстоятельством, что является естественным обобщением двоично симметричного канала с ограниченным числом искажений $0 \rightarrow 1, 1 \rightarrow 0$, с одной стороны, и освобожден от четких рамок ограниченного выбора, с другой стороны, что позволяет в ряде случаев лучше понять исходную ситуацию.

Предикат $X(\Psi, V)$ описывает «взаимоотношения» аддитивного канала $K(\Psi)$ и кода V и обладает следующими свойствами:

- а) $X(\Psi + u, V + v) = X(\Psi, V)$, где u и v – произвольные слова множества B^n ;
- б) $X(\Psi, V) = X(\varphi\Psi, V)$, где φ – произвольное обратимое преобразование из T ;
- в) $X(\Psi, V) = X(\Phi, \varphi V)$, где $\Phi = \varphi\Psi$, φ – произвольное линейное преобразование из T .

Словесное описание этих свойств предиката $X(\Psi, V)$ состоит в следующем:

а) любые «сдвиги» канала $K(\Psi)$ или кода V не нарушают «взаимоотношения» между ними;

б) код V исправляет или не исправляет ошибки каналов $K(\Psi)$ и $K(\varphi\Psi)$ одновременно. Т.е. каналы $K(\Psi)$ и $K(\varphi\Psi)$ для обратимого преобразования φ обладают одинаковыми свойствами в смысле коррекции ошибок, поэтому аддитивный канал $K(\Psi)$ и канал $K(\varphi\Psi)$ естественно считать неразличимыми;

в) коды V и φV одновременно исправляют или не исправляют ошибки аддитивных каналов, порожденных соответственно Ψ и $\varphi\Psi$.

Теорема 4. Для произвольных аддитивных каналов $K(\Psi)$ и $K(\Phi)$ справедливо следующее:

$$K(\Psi) \sim K(\Phi) \Leftrightarrow \Psi^2 = \Phi^2.$$

Пример 3. Рассмотрим аддитивные каналы, порождающие множества которых имеют разные мощности: $K(\Phi_1)$, $K(\Phi_2)$, $K(\Phi_3)$ из примера 2.

Нетрудно убедиться, что эти каналы эквивалентны, хотя $|\Phi_1|=5$, $|\Phi_2|=6$, $|\Phi_3|=6$. На самом деле в общем случае мощность канала не является помехой для классификации, а в определенных случаях однозначно определяет класс эквивалентности канала.

Следствие. Для любого аддитивного канала $K(\Psi)$, удовлетворяющего условию $|\Psi| > 2^{n-1} + 1$, имеет место $M(\Psi) = M(\Phi)$, где $\Phi(0) = B^n$.

Следствие. $K(\Psi) \sim K(\Phi)$ тогда и только тогда, когда $\Psi^2 = \Phi^2$.

¹ Московский государственный университет

² Группа Бит, Москва

³ Ереванский государственный университет

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

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

Отношения между каналами связи

Введено понятие эквивалентности каналов связи с точки зрения исправления возможных ошибок в данных каналах связи. Для алгебраических каналов связи приведены необходимые и достаточные условия эквивалентности. Описаны классы эквивалентности алгебраических каналов.

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

Հարաբերություններ կապուղիների միջև

Ներմուծված է կապուղիների համարժեքության հասկացությունը կապուղիներում հնարավոր սխալներ ուղղելու տեսանկյունից: Հանրահաշվական կապուղիների

համար տրվում են անհրաժեշտ և բավարար համարժեքության պայմաններ: Նկարագրված են հանրահաշվական կապուղիների համարժեքության դասերը:

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

Channel Relations between Channels

The notion of equivalence of communication channels has been introduced in terms of correcting possible errors in these communication channels. For algebraic communication channels, necessary and sufficient equivalence conditions are given. The equivalence classes of algebraic channels are described.

Литература

1. *Мальцев А. И.* Алгоритмы и рекурсивные функции. М. Наука, Физматлит. 1986. 368 с.
2. *Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А.* Теории кодов, исправляющих ошибки. М. Связь. 1979. 744 с.
3. *Леонтьев В. К., Мовсисян Г. Л.* В кн.: The First International. Algebra and Geometry Conference 16-20 may 2007. Yerevan. Armenia.
4. *Леонтьев В. К., Мовсисян Г. Л.* – Доклады НАН Армении. 2004. Т. 104. № 1. С. 23-27.
5. *Леонтьев В. К., Мовсисян Г. Л., Маргарян Ж. Г.* – Доклады РАН. 2006. Т. 411. № 3. С. 306-309.
6. *Леонтьев В. К., Мовсисян Г. Л., Маргарян Ж. Г.* – Доклады НАН Армении. 2010. Т. 110. № 4. С. 334-339.
7. *Леонтьев В. К., Мовсисян Г. Л., Осипян А.А.* В кн.: Матер. XI междунар. семинара «Дискретная математика и ее приложение». М. Изд-во МГУ. 2012. С. 415-416.
8. *Левенштейн В. И.* – ДАН СССР. 1965. Т. 163. № 4. С. 845-848.
9. *Leontiev V., Movsisyan G., Osipyanyan A.* – Open Journal of Discrete Mathematics (OJDM). 2014. 4. P. 67-76.