УДК 510

В.К.Леонтьев, Г.Л.Мовсисян

Об аддитивном канале связи

(Представлено академиком Ю.Г. Шукуряном 12/XII 2003)

Рассматривается аддитивный канал связи в следующей стандартной формулировке. В множестве B^n - двоичных наборов длины n выделено произвольное подмножество S, содержащее нулевой вектор, и любое кодовое слово v на выходе воспринимается как

$$v' = v + e, \qquad (1)$$

где $e \in S$, а $v \in B^n$. Таким образом S - это множество векторов ошибок в стандартных терминах теории корректирующих кодов. Многие классические каналы можно представить в форме (1), что и определяет интерес к этому достаточно универсальному каналу [1-3]. Классической задачей теории корректирующих кодов является построение кода максимальной мощности, исправляющего ошибки из множества S. Существуют два универсальных способа для оценки мощности такого кода: верхняя граница получается методом "плотной упаковки", а нижняя граница методом "насыщения" или процедурой Варшамова - Гилберта. Одна из известных проблем теории кодирования в содержательной формулировке звучит следующим образом: какая из двух упомянутых выше границ ближе к истинному значению максимальной мощности соответствующего кода [3]? Мы обсуждаем эту проблему в терминах "структуры" множества ошибок S, а также рассматриваем несколько отдельных примеров.

Определение [1]. *Код* $V \subseteq B^n$ *называется кодом, исправляющим ошибки канала* S, *если выполняется следующее условие:*

$$u + e_1 \neq v + e_2 \qquad (2)$$

для любых кодовых точек u *и* v *и для любых векторов ошибок* e_1 *и* e_2 *из* S.

Условие (2) действительно позволяет исправить все ошибки канала S с помощью обычной таблицы декодирования. Приведем нижнюю и верхнюю границы для мощности |V(S)| максимального кода, исправляющего все ошибки из S в терминах мощности окрестностей 1-го и 2-го порядка, индуцированных этим множеством.

Определение. *Окрестностью 1-го порядка точки* $v \in B^n$, *индуцированной множеством* S, *называется множество*

$$A_1(v) = \{v + e, e \in S\}. \qquad (3)$$

Окрестности следующих порядков определяются индуктивно, исходя из формулы (3)

$$A_2(v) = A_1(A_1(v)) = \{v_1 + e, v_1 \in A_1(v), e \in S\}. \qquad (4)$$

Ясно, что (4) эквивалентно следующей формуле:

$$A_2(v) = \{v + (e_i + e_j), e_i, e_j \in S\}.$$

Таким образом, если $S^2=\{(e_i+e_j), e_i, e_j \in S\}$ - "квадрат" множества S, то окрестность 2-го порядка $A_2(v)$ определяется формулой

$$A_2(v) = \{v + e, e \in S^2\}. \qquad (5)$$

Аналогично определяются окрестности любого порядка, индуцированные множеством S.

Примеры.

1. Если S - это шар радиуса t в метрике Хэмминга с центром в нуле, т.е. $S = \{ x, ||x|| \le t \}$, то S^2 - это шар радиуса 2t с этим же центром при $2t < n$.

2. Если S - подгруппа B^n, то $S^2 = S$.

Нетрудно понять, что все окрестности одного и того же порядка равномощны, т.е.

$$|A_k(v)| = |S_k| = |A_k| \quad k = 1,2,... \qquad (6)$$

Теорема 1. *Для мощности* $|V(S)|$ *максимального кода, исправляющего все ошибки из множества S, справедливы неравенства*

$$\frac{2^n}{|A_2|} \le |V(S)| \le \frac{2^n}{|A_1|}. \qquad (7)$$

Доказательство. Верхняя граница следует прямо из определения (2), которое утверждает, что окрестности 1-го порядка точек из кода V(S) не пересекаются.

Для доказательства нижней границы нужно лишь модифицировать процедуру Варшамова - Гилберта:

1. пусть v - произвольная точка из B^n. Положим $v_1 = v$ и рассмотрим окрестность 2-го порядка точки v_1, т.е. $A_2(v_1)$;

2. в качестве v_2 выбираем произвольную точку из $\{ B^n \backslash A_2(v_1)\}$;

3. в качестве v_3 выбираем произвольную точку из $\{ B^n \backslash (A_2(v_1) \cup A_2(v_2))\}$;

4. продолжаем эту процедуру до исчерпания всего B^n.

Относительно построенного кода $V(S) = \{v_1 v_2 ... v_N\}$ справедливы следующие утверждения.

I. Код V(S) исправляет все ошибки из S.

Действительно, если не так, то

$$v_\iota + e_1 = v_j + e_2$$

или

$$v_\iota = v_j + (e_1 + e_2),$$

т.е. $v_\iota \in A_2(v_j)$, что противоречит построению.

II. Мощность $|V(S)|$ кода $V(S)$ удовлетворяет неравенству

$$|V| \geq \frac{2^n}{|A_2|}.$$

Эта граница сразу следует из очевидных неравенств

$$|A_2(v_1) \cup A_2(v_2) \cup \ldots \cup A_2(v_N)| \leq \sum_{i=1}^{N} |A_2(v_\iota)| \leq N|A_2|$$

Следствие 1. *Если* S - *группа, то*

$$|V(S)| = \frac{2^n}{|S|}. \tag{8}$$

Неравенства (7) показывают, что точность границ Хэмминга и Варшамова - Гилберта определяется отношением $|A_2|/|A_1|$, которое удовлетворяет очевидным неравенствам

$$1 \leq \frac{|A_2|}{|A_1|} \leq |S|. \tag{9}$$

В частности, если $S = U_1 \cup U_2$, где U_1, U_2 - подгруппы B^n и $|U_2| \leq c$, то при больших n

$$|S^2| \leq c|S|$$

и границы в (7) отличаются в константу раз.

Таким образом алгебраическая структура множества S сильно влияет на точность границ в (7).

Примеры.

1. Пусть в канале происходит любое, но четное число ошибок. Тогда $|S| = 2^{n-1}$ и $|V(S)| = 2$. Действительно, точки a = (11...1) и b = (0...0) образуют код, который исправляет все ошибки из S. Если же в коде V(S) имеется не менее трех точек, то хотя бы две из них имеют вес одинаковой "четности" и не могут быть правильно идентифицированы на приемном конце.

2. Рассмотрим канал с "разделением ошибок", т.е. после искажения канал некоторое время передает символы безошибочно.

Определение. *Канал* S *называется каналом с разделением ошибок уровня* k, *если любое слово* $x = (x_1x_2...x_n) \in S$ *удовлетворяет следующим неравенствам:*

$$\begin{cases} x_1+x_2+...+x_k \le 1 \\ x_2+x_3+...+x_{k+1} \le 1 \\ ... \\ x_{n-k+1}+x_{n-k+2}+...+x_n \le 1, \end{cases} \qquad (11)$$

$$x_\iota=\{0,1\}.$$

Следующее утверждение нужно для оценки мощности |S|.

Теорема 2. *Если* S(n,k) - *число ненулевых решений системы* (11), *то*

$$S(n,k) = \sum_{m=1}^{\infty} \binom{n-(m-1)(k-1)}{m} + 1. \qquad (12)$$

Доказательство. Пусть $x = (x_1x_2...x_n)$ - произвольное решение системы (11) и $y_1 < y_2 < ... < y_m$ - номера всех единичных координат вектора x. Тогда

$$y_s - y_{s-1} \ge k, \qquad s = 2,3,...m$$

и если $y_1=y$, то

$$y_2 = k + y + z_1$$

...

$$y_m = (m-1)k + y + (z_1 + z_2 ... + z_{m-1}),$$

где $z_\iota \ge 0$ и

$$z_1 + z_2 ... + z_{m-1} \le n - (m-1)k + y,$$

Если $e_m(t)$ - число решений уравнения

$$z_1 + z_2 + ... + z_{m-1} = t,$$

то $e_m(t) = \binom{m+t-2}{m-2}$ и для числа $S_m(n,k)$-решений уравнения (11) с $||x|| = m$ получаем формулу

$$S_m(n,k) = \sum_{t=0}^{N} e_m(t) = \binom{m+N-1}{N},$$

где $N = n - (m-1)k - y$.

Для получения финального результата осталось "освободить" y и просуммировать $S_m(n,k)$ по всем m.

В терминах производящих функций искомый результат выглядит так.

Пусть

$$F_k(z) = \sum_{n=1}^{\infty} S(n,k) z^n.$$

Следствие.

$$F_k(z) = \frac{z}{1-z}(z^k + z - 1). \tag{13}$$

Для исправления ошибок в канале S можно использовать код Хэмминга для коррекции одной ошибки в каждом подслове длины k. Таким образом, мы получили код мощности (для больших n и k) порядка

$$|V(S)| \gtrsim 2^{n(1-[\ln k/k])}. \tag{14}$$

Использование (7) и (13) приводит к следующей верхней границе:

$$|V(S)| \lesssim 2^{n(1-[(\lambda)/k])}, \tag{15}$$

где $\lambda = \log_2 e$.

Вычислительный центр РАН

Литература

1. *Деза М.Е.* - Проблемы передачи информации. 1965. Т. 1. N3. С. 29-39.
2. *Гоппа В.Д.* - Успехи мат. наук. 1984. N1(35). С. 77-120.
3. *Кричевский Р.Е.* Сжатие и поиск информации. М. Радио и связь. 167 с.

Վ.Կ. Լեոնտև, Ղ.Լ. Մովսիսյան

Ադդիտիվ կապի գծերի վերաբերյալ

Աշխատանքում դիտարկվում են ադդիտիվ կապի գծերում սխալներ ուղղող կոդեր: Սխալների տրված բազմության համար բերված են կոդի մաքսիմալ հզորության վերին և ստորին գնահատականներ: Դիտարկված են նաև այսպես կոչված սխալները տրոհող կապի գծերում մեկ սխալ ուղղող կոդեր և այդ կոդերի հզորության համար բերված են վերին և ստորին ասիմպտոտիկ գնահատականներ: