Math-Net.Ru
All Russian mathematical portal

R. R. Varshamov, G. M. Tenengol'ts, Code Correcting Single Asymmetric Errors, *Avtomat. i Telemekh.*, 1965, Volume 26, Issue 2, 288–292

Use of the all-Russian mathematical portal Math-Net.Ru implies that you have read and agreed to these terms of use
http://www.mathnet.ru/eng/agreement

Download details:
IP: 86.48.7.223
January 16, 2023, 23:48:38

УДК 621.391.154

КОД, ИСПРАВЛЯЮЩИЙ ОДИНОЧНЫЕ НЕСИММЕТРИЧЕСКИЕ ОШИБКИ

Р. Р. ВАРШАМОВ, Г. М. ТЕНЕНГОЛЬЦ

(*Москва*)

Рассматривается бинарный корректирующий код, исправляющий одиночные несимметрические ошибки.

Введение

В технике связи представляет интерес исследование несимметрических систем кодирования, т. е. систем с несимметрическим каналом. Несимметрическим называется канал с неодинаковыми вероятностями повреждений различных элементарных посылок (импульсов). В бинарном случае, например, это означает, что вероятность перехода символа «1» в «0» в кодовом слове при прохождении его по каналу существенно меньше вероятности перехода «0» в «1» или наоборот. В такой ситуации обычно пренебрегают наименьшими вероятностями и пытаются защитить рабочие сигналы только от некоторых частичных ошибок, имеющих в данном случае наибольшую вероятность.

Отсюда возникает вопрос построения корректирующих кодов, способных исправлять любые $r > 0$ случайные и независимые несимметрические ошибки.

Задача построения такого кода [1] эквивалентна следующей математической задаче:

Выделить из G_n, n-мерного векторного пространства над полем G вычетов по модулю 2, максимальное (в смысле количества элементов) подмножество K, любая различная пара векторов которого удовлетворяла бы условию

$$\rho(x, y) = |x-y| + ||x| - |y|| \geqslant 2r+1, \tag{1}$$

где $|x| = \sum_{i=1}^{n} x_i$ — норма (вес) вектора x.

Как легко заметить, условие (1) слабее требования, предъявляемого к рабочим сигналам корректирующего кода, исправляющего то же количество r случайных и независимых симметрических ошибок, а именно:

$$|x-y| \geqslant 2r+1. \tag{2}$$

Поэтому априори можно было бы предполагать, что максимально возможная скорость передачи сообщения системы с несимметрическим каналом, вообще говоря, должна быть больше скорости передачи соответствующей ей системы с симметрическим каналом.

Однако, как показано в [1], в случае линейного кодирования несимметрический код не имеет ожидаемых преимуществ и почти всегда идентичен симметрическому. (Здесь и в дальнейшем при сравнении кодов основные их параметры, такие, как длина сигнала n и число исправляемых ошибок r, в обоих случаях подразумеваются одинаковыми).

В настоящей статье рассмотрен несимметрический код (вообще говоря, нелинейный), исправляющий одиночные ошибки, мощность (число сигналов) которого больше мощности соответствующего максимального симметрического кода, а также известного в литературе несимметрического кода Фреймана — Кима.

1. Корректирующий код, исправляющий одиночные несимметрические ошибки

Пусть требуется построить код с исправлением несимметрических одиночных ошибок при заданной длине кодовых слов n.

Рассмотрим сравнение

$$W = \sum_{i=1}^{n} i\alpha_i \equiv a \qquad (\operatorname{mod} n + 1), \tag{3}$$

где α_i — двоичные числа, a — произвольное целое, удовлетворяющее соотношению $0 \leqslant a < n + 1$.

Код, исправляющий одиночные несимметрические ошибки, представляется множеством K_a всевозможных бинарных последовательностей вида $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n)$, где $\alpha_1, \alpha_2, \ldots, \alpha_n$ — решение сравнения (3).

Например, в случае $n = 8$ одним из решений (3) при $a = 0$ будет:

$$\alpha = (1, 0, 0, 1, 1, 0, 0, 1),$$

так как $1 + 4 + 5 + 8 \equiv 0 \pmod 9$.

Соответственно кодовое слово имеет вид: 10011001.

Построение кода рассмотрим на одном частном примере.

Пример. Пусть, как и раньше, $n = 8$. Полагая $a = 0$, сравнение (3) можно будет записать в виде

$$\sum_{i=1}^{8} i\alpha_i \equiv 0 \qquad (\operatorname{mod} 9),$$

все решения которого образуют код, содержащий 30 различных сигналов, имеющих вид:

00000000	00001110	11011100	
10000001	11000011	01010111	
01000010	10100101	00111011	
00100100	10010110	11110001	
00011000	10011001	11101010	
11000100	01011010	10111101	(I)
10101000	01101001	01111110	
01110000	01100110	11100111	
00100011	00111100	11011011	
00010101	10001111	11111111	

2. Коррекция одиночной ошибки

Для определенности в дальнейшем будем предполагать, что вероятность перехода символа «1» в «0» существенно больше вероятности перехода «0» в «1», т. е. ошибками вида $0 \to 1$ пренебрегаем. Это допущение несущественно и, как показано в [1], код, способный исправлять несимметрические ошибки вида $1 \to 0$, пригоден также и для коррекции ошибок вида $0 \to 1$.

Из дальнейшего будет видно, что номер позиции, в которой произошла ошибка в кодовом слове α, определяется как наименьшее положительное решение сравнения:

$$-l \equiv W' - a^* \qquad (\mathrm{mod}\ n+1). \tag{4}$$

Сказанное проиллюстрируем на примере.

Пусть передается один из возможных сигналов системы (I), а именно: $\alpha = 11101010$. Однако в результате прохождения его по каналу он терпит искажение и воспринимается на приемном конце в виде: $\alpha' = 11001010$ (ошибка произошла на третьей позиции сигнала).

Согласно определению для кодового слова α справедливо соотношение

$$W \equiv 0 \qquad (\mathrm{mod}\ 9),$$

где W — «обобщенный вес» сигнала α, определяемый формулой (3).

Между тем, в случае одиночной ошибки вида $1 \to 0$ «обобщенный вес» искаженного сигнала α' определится соотношением

$$W' = W - l,$$

где l — номер позиции сигнала α, в которой произошла ошибка.

Поэтому

$$W = W' + l \equiv 0. \qquad (\mathrm{mod}\ 9).$$

Откуда

$$l \equiv -W' \qquad (\mathrm{mod}\ 9).$$

В нашем случае

$$W' = \sum_{i=1}^{8} i\alpha_i = 1 + 2 + 5 + 7 = 15.$$

Следовательно,

$$l \equiv -15 \qquad (\mathrm{mod}\ 9)$$

или

$$l = 3.$$

Это означает, что ошибка произошла на третьей позиции (что в действительности имело место). Таким образом, исправленный сигнал имеет вид: 11101010.

3. Число кодовых слов

Общее число $M(n)$ кодовых слов длиной n в наилучшем из предлагаемых кодов, как нетрудно показать, связано неравенством

$$M(n) \geqslant \frac{2^n}{n+1}. \tag{5}$$

Поэтому при помощи несложного анализа можно установить, что максимальное число его сигналов во всяком случае не меньше общего числа сигналов $M_1(n) = 2^{n+[-\log_2(n+1)]}$ кода Хэмминга с коррекцией одиночных симметрических ошибок. Функция $[x]$ определена для любого вещественного x и является наибольшим целым, не превосходящим x.

В самом деле, этот факт непосредственно вытекает из очевидного неравенства

$$\frac{2^n}{n+1} \geqslant 2^{n+[-\log_2(n+1)]}, \tag{6}$$

откуда

$$\frac{1}{n+1} \geqslant 2^{[-\log_2(n+1)]}$$

или, что то же самое,

$$2^{-[-\log_2(n+1)]} \geqslant n+1$$

Знак равенства (т. е. $M(n) = M_1(n)$) имеет место лишь в случае $n = 2^k - 1$.

---

* Легко заметить, что в случае ошибок вида $0 \to 1$ правая часть выражения (4) берется со знаком минус.

Таким образом, установлено, что максимальное число сигналов в предлагаемом коде почти всегда больше общего количества сигналов в симметрическом коде Хэмминга и может совпадать с ним лишь при специальных значениях $n = 2^k - 1$.

4. Сравнение предложенного кода с несимметрическими корректирующими кодами

В настоящее время известен всего лишь один корректирующий код, исправляющий одиночные несимметрические ошибки. Этот код, предложенный Фрейманом и Кимом [2], образуется из кода Хэмминга, длина кодового слова которого соответственно равна $n - m$, причем $m = \left[\frac{n}{2}\right]$.

Общее число кодовых слов длины n в коде Фреймана — Кима

$$M_2(n) = (h_{n-m} + 1)2^{m-1},$$

где h_p — число кодовых слов кода Хэмминга с длиной сигнала p.

Однако, как будет показано далее, мощность $M'(n)$ наилучшего из предлагаемых нами кодов значительно больше мощности кода Фреймана — Кима. Для этой цели в первую очередь докажем следующее неравенство, справедливое для любого $n > 6$:

$$\left(2^{n-[n/2]+[-\log_2(n-[n/2]+1)]} + 1\right) 2^{[n/2]-1} < \frac{2^n}{n+1}. \tag{7}$$

В справедливости (7) при $n = 7 \div 13$ убеждаемся непосредственным подсчетом (см. таблицу).

Число сигналов в коде, исправляющем одиночные ошибки

n	Код Хэмминга $M_1(n)$	Код Фреймана—Кима $M_2(n)$	Предлагаемый код $M'(n)$	n	Код Хэмминга $M_1(n)$	Код Фреймана—Кима $M_2(n)$	Предлагаемый код $M'(n)$
3	2	2	2	10	64	80	94
4	2	4	4	11	128	144	171
5	4	6	6	12	256	288	316
6	8	12	10	13	512	544	586
7	16	12	16	14	1024	1088	1093
8	16	24	30	15	2048	1088	2048
9	32	40	52	16	2048	2176	3856

Остается показать справедливость его при $n \geqslant 14$.

Преобразуем выражение (7) следующим образом:

$$2^{n-1+[-\log_2(n-[n/2]+1)]} + 2^{[n/2]-1} < \frac{2^n}{n+1},$$

откуда

$$2^{-1+[-\log_2(n-[n/2]+1)]} + 2^{[n/2]-n-1} < \frac{1}{n+1}$$

или

$$2^{[-\log_2(n/2+\varepsilon+1)]} + 2^{-n/2-\varepsilon} < \frac{2}{n+1},$$

где

$$\varepsilon = \frac{n}{2} - \left[\frac{n}{2}\right] \geqslant 0.$$

Далее имеем

$$2^{-\log_2(n/2+\varepsilon+1)-\log_2\varepsilon_1} + 2^{-(n/2+\varepsilon)} < \frac{2}{n+1},$$

т. е.

$$2^{-\log_2 (n/2+\varepsilon+1)\varepsilon_1} + 2^{-(n/2+\varepsilon)} < \frac{2}{n+1},$$

что в свою очередь дает

$$\frac{1}{\left(\frac{n}{2}+\varepsilon+1\right)\varepsilon_1} + \frac{1}{2^{n/2+\varepsilon}} < \frac{2}{n+1}. \qquad (8)$$

Здесь

$$\log_2 \varepsilon_1 = \left[-\log_2\left(\frac{n}{2}+\varepsilon+1\right)\right] + \log_2\left(\frac{n}{2}+\varepsilon+1\right) \geqslant 0, \qquad \varepsilon_1 \geqslant 1.$$

Напишем теперь неравенство более сильное, чем (8)

$$\frac{1}{\frac{n}{2}+1} + \frac{1}{2^{n/2}} < \frac{2}{n+1} \qquad (8a)$$

или

$$\frac{1}{2^{n/2}} < \frac{2}{(n+1)(n+2)}. \qquad (9)$$

Неравенство (9) имеет место при любом $n \geqslant 14$, откуда автоматически следует справедливость (8), а следовательно, и (7).

Приведенная выше таблица характеризует нижнюю оценку $M'(n) \leqslant \leqslant M(n)$ числа сигналов в наилучшем из предлагаемых кодов, $M_2(n)$ — в коде Фреймана — Кима и $M_1(n)$ — в симметрическом коде Хэмминга.

Поступила в редакцию
28 сентября 1963 г.

Цитированная литература

1. Варшамов Р. Р. Некоторые особенности линейных кодов, корректирующих несимметрические ошибки. Докл. АН СССР, т. 157, № 3, 1964.
2. Kim W. H. and Freiman C. V. Single Error-Correcting Codes for Asymmetric Binary Channels. IRE Transactions on information theory, v. IT-5, No. 2, June, 1959.

CODE CORRECTING SINGLE ASYMMETRIC ERRORS

R. R. VARSHAMOV, G. M. TENENGOL'TS

A binary correction code correcting single asymmetric errors is considered.