Р. Р. ВАРШАМОВ, Э. П. ЗОГРАБЯН

КЛАСС КОДОВ, ИСПРАВЛЯЮЩИЙ ДВЕ НЕСИММЕТРИЧНЫЕ ОШИБКИ

В последнее время некоторое внимание привлекли устройства хранения и передачи информации с несимметричной характеристикой повреждения (искажения), в связи с чем представляет интерес исследование несимметричных систем кодирования, устойчивых к искажениям, носящих специальный характер. Единичная ошибка, как бы она не определялась, изменит сигнал и переведет его в отличный от него другой сигнал. В случае двоичного канала дело обстоит сравнительно просто: ошибка приводит к тому, что „единица" переходит в „нуль" или наоборот. В случае же недвоичных кодов в принципе возможны несколько различных определений ошибок, например, неограниченные ошибки, меняющие символы на любое другое значение, или же малые ошибки с ограниченным диапазоном искажений.

Предположим, что каждая элементарная посылка кодовой последовательности длины n принимает q*) различных значений. Такой сигнал может быть обозначен последовательностью $x = (x_1, x_2, \cdots, x_n)$, где каждый знак x_i принимает соответственно одно из значений $0, 1, \cdots, q-1$. Совокупность $G_{n,q}$ из q^n последовательностей такого вида будем рассматривать как абелеву группу, определив сумму элементов x и y следующим образом:

$$x + y = (x_1 + y_1,\ x_2 + y_2,\ \cdots,\ x_n + y_n),$$

где сложение $x_i + y_i$ производится по модулю q.

В $G_{n,q}$ введем понятия нормы $|x|$, равное сумме элементов, входящих в последовательность x, т. е. $|x| = \sum_{i=1}^{n} x_i$. Математически под искажением сигнала x понимается обычное сложение его с некоторым элементом $y \in G_{n,q}$. Однако в случае несимметричных ошибок не каждый знак в сигнале одинаково подвержен искажению. Следовательно, не каждый элемент группы $G_{n,q}$ может быть выбран в качестве допустимой помехи y. Ясно, что элемент y выбирается из некоторого под-

*) Где q — любое целое $\geqslant 2$.

множества $E_x \subset G_{n,q}$. Для любого x определим E_x как совокупность элементов $y \in G_{n,q}$, удовлетворяющих условиям:

$$|x+y| = |x| + |y|, \tag{1}$$

или

$$|x-y| = |x| - |y|. \tag{1^1}$$

При этом, если $|y| = r$, то будем говорить, что произошла r-кратная ошибка.

В настоящей заметке предлагается новый класс кодов, исправляющих две*) несимметричные (удовлетворяющих условию (1) или (1^1)) ошибки.

Для всякого $x \in G_{n,q}$ обозначим через $W_m(f(z), x, \alpha)$ наименьший неотрицательный вычет по модулю m выражения $-\alpha + \sum_{i=1}^{n} f(i)\, x_i$, то есть

$$W_m(f(z), x, \alpha) \equiv -\alpha + \sum_{i=1}^{n} f(i)\, x_i \pmod m,$$

где $f(z)$ — любая целочисленная функция, определенная на заданном множестве, α — произвольное целое.

Пусть $p > 5$ — простое число, g — первообразный корень по модулю p и $n < p-1$.

Рассмотрим систему уравнений

$$\begin{aligned} W_{p-1}(z, x, \alpha) &= 0, \\ W_p(g^z - 1, x, \beta) &= 0, \end{aligned} \tag{2}$$

где α и β произвольные целые.

В дальнейшем мы покажем, что при любых α и β множество $H_{\alpha,\beta}$ всевозможных решений системы (2) является кодом, исправляющим две несимметричные (в смысле (1) или (1^1)) ошибки.

Действительно, пусть передается по каналу произвольный кодовый сигнал $x \in H_{\alpha,\beta}$. Допустим, что в процессе прохождения его по каналу он подвергся искажению помехой y ($|y| \leqslant 2$), в результате чего на приемный конец поступил искаженный сигнал $\gamma = y + x$. Подставляя γ в систему (2) (с учетом (1) или (1^1), в зависимости от того, какой тип помехи рассматривается), получим выражение

$$\theta_1 = W_{p-1}(z, \gamma, \alpha) = -\alpha + \sum_{i=1}^{n} i x_i \pm \sum_{i=1}^{n} i y_i \pmod{p-1},$$

---

*) То есть все одиночные и двойные ошибки.

$$\delta_2 = W_p(g^z - 1,\ z,\ \beta) = -\beta + \sum_{i=1}^{n} (g^i - 1)\, x_i +$$

$$+ \sum_{i=1}^{n} (g^i - 1)\, y_i \pmod p,$$

из которого, принимая во внимание, что $x \in H_{n,3}$, будем иметь

$$W_{p-1}(z,\ y,\ \pm \delta_1) = 0,$$

$$W_p(g^z - 1,\ y,\ \pm \delta_2) = 0. \tag{3}$$

Код $H_{n,3}$, по утверждению, исправляет все одиночные и двойные ошибки, а это означает, что ни одна из допустимых помех (отличная, разумеется, от y), не является решением системы (3). Чтобы в этом убедиться, достаточно показать, что ни одна из различных пар элементов группы $G_{n,q}$, x' и x'' ($|x'|,\ |x''| \leqslant 2$) не удовлетворяет соотношению

$$W_{p-1}(z,\ x',\ W_{p-1}(z, x'', 0)) = 0,$$

$$W_p(g^z - 1,\ x',\ W_p(g^z - 1,\ x'', 0)) = 0. \tag{4}$$

В самом деле, норма каждого элемента x' и x'' в отдельности не превышает 2, а поэтому выражение (4) эквивалентно системе сравнений

$$a + b \equiv c + d \pmod{p-1},$$

$$g^a + g^b \equiv g^c + g^d \pmod p, \tag{5}$$

где a, b, c и d неотрицательные целые $< p - 1$, причем $a \neq c$ и, следовательно, $b \neq c$.

Но так как

$$d = a + b - c + (p-1)\,h,$$

то

$$g^a + g^b \equiv g^c + g^{a+b-c} \pmod p,$$

откуда

$$g^a - g^c \equiv g^{a+b-c} - g^b \pmod p,$$

и

$$(g^c - g^b)(g^{a-c} - 1) \equiv 0 \pmod p. \tag{6}$$

Однако, согласно условию $a \not\equiv c$, $b \not\equiv c \pmod{p-1}$. А это значит, что сравнение (6) невыполнимо ни при каких значениях a, b и c и, следовательно, неразрешимо соотношение (5), а также и эквивалентная система (4).

Этим завершается доказательство того, что код $H_{n,3}$ исправляет две несимметричные ошибки.

Аналогичным образом, несколько изменив рассуждения, можно показать, что множество $\overline{H}_{\alpha,\beta}$ — всевозможное решение системы

$$W_p(z, x, \alpha) = 0,$$

$$W_p(z^2, x, \beta) = 0,$$

где $p > n$, α и β любые целые числа, также является кодом, исправляющим две несимметричные ошибки.

Ռ. Ռ. ՎԱՐՇԱՄՈՎ, Է. Գ. ՋՈՀՐԱԲՅԱՆ

ԵՐԿՈՒ ՈՉ ՍԻՄԵՏՐԻԿ ՍԽԱԼՆԵՐԻ ՈՒՂՂՈՂ ԿՈԴԵՐԻ ԴԱՍ

Ամփոփում

Դիտարկվում է $G_{n,q}$ բազմությունը, որը բաղկացած է $x = (x_1\ x_2, \ldots, x_n)$ տեսքի բոլոր հնարավոր հաջորդականություններից, որտեղ յուրաքանչյուր x_i նշան ընդունում է $0, 1, \ldots, q-1$ արժեքներից որևէ մեկը (q — կամայական ամբողջ թիվ է $\geqslant 2$)։

$G_{n,q}$ բազմության մեջ մտցվում է նորմայի՝ $|x|$ հասկացությունը որպես x հաջորդականության մեջ մտնող էլեմենտների գումար ($|x| = \sum_{i=1}^{n} x_i$)։ x ազդանշանի r բազմապատիկ ոչ սիմետրիկ աղավաղման տակ հասկացվում է նրա սովորական գումարը $y \in G_{n,q}$, ($|y| \leqslant r$) վեկտորի հետ, որը բավարարում է

$$|x + y| = |x| + |y|$$

կամ

$$|x - y| = |x| - |y|$$

պայմաններից որևէ մեկին։

Ցույց է տրվում, որ $H_{\alpha,\beta} \in G_{n,q}$ բազմությունը, որը բաղկացած է

$$\sum_{i=1}^{n} i x_i \equiv \alpha \quad (\mathrm{mod}\, p-1),$$

$$\sum_{i=1}^{n} (g^i - 1) x_i \equiv \beta \quad (\mathrm{mod}\, p)$$

համեմատության սիստեմի բոլոր հնարավոր լուծումներից (որտեղ α և β կամայական ամբողջ թվեր են, $p > 5$ - պարզ թիվ է, g-նախասկզբնական արմատ է՝ p մոդուլով, $n < p-1$), հանդիսանում է միալնակ և կրկնակի ոչ սիմետրիկ սխալների ուղղող կոդ։

Հոդվածի վերջում հաստատվում է, որ $\overline{H}_{\alpha,\beta} \in G_{n,q}$ բազմությունը, որը բաղկացած է

$$\sum_{i=1}^{n} i x_i \equiv \alpha \quad (\mathrm{mod}\, p),$$

$$\sum_{i=1}^{n} i^2 x_i \equiv 3 \pmod{p}$$

համեմատության սխալների բոլոր հնարավոր յուծումներից. նույնպես հաղորդառում է երկու ոչ սիմետրիկ սխալներ ուղղող կոդ։

ЛИТЕРАТУРА

1. *W. H. Kim* and *C. V. Freiman*. Single Error-Correcting Codes for Asymmetric Binary Channels. IRE Transactions on information theory, v. IT-5, № 2, June, 1959.
2. *Р. Р. Варшамов, Г. М. Тенгольц*. Код, исправляющий одиночные несимметрические ошибки. „Автоматика и телемеханика", т. XXVI, № 2, 1965.