ՀԱՅԿԱԿԱՆ ՍՍՀ ԳԻՏՈՒԹՅՈՒՆՆԵՐԻ ԱԿԱԴԵՄԻԱՅԻ ԶԵԿՈՒՅՑՆԵՐ
ДОКЛАДЫ АКАДЕМИИ НАУК АРМЯНСКОЙ ССР

LXX 1980 4

УДК 5198

МАТЕМАТИКА

Д. Н. Геворкян, А. Г. Мхитарян

Класс кодов, исправляющих большие одиночные несимметрические ошибки

(Представлено чл.-корр. АН Армянской ССР Р. Р. Варшамовым 30/I 1980)

Как выяснилось в последнее время, в некоторых устройствах хранения и передачи информации наиболее типичны искажения, имеющие несимметрический характер. Примером реального устройства с несимметрическими искажениями может служить система с мультипликативной помехой, когда уровень сигнала в посылке падает ниже порогового значения, установленного в решающем устройстве, запоминающее устройство — на ферритах или на магнитной ленте в больших ЭВМ и др. В релейных же устройствах это искажение типа обрыва или короткого замыкания ([1, 2]). В связи с этим большой интерес представляет исследование несимметрических систем кодирования.

Обозначим через $B_q^n = \{b = (b_1, b_2, \ldots, b_n) : b_i \in \{0, 1, \ldots q-1\}\}$ — множество всех последовательностей длины n с символами из множества $Q = \{0, 1, \ldots, q-1\}$. Пусть при передаче (или хранении) в i-ой позиции вектора $b = (b_1, b_2, \ldots, b_n)$ произошла ошибка величины e, т. е. $b_i \to b_i + e$. В случае симметрической ошибки b_i' — произвольный элемент множества Q и величина e не зависит от b_i. В случае несимметрических искажений различают два вида ошибок: 1) малые искажения типа $e = +1$ (или $e = -1$), когда каждый символ b_i (за исключением тех, которые равны $q-1$) подвержен искажению типа $b_i \to b_i + 1$ (или $b_i \to b_i - 1$); 2) большие искажения типа (+) (или (−)), когда каждый символ, кроме $b_i = q-1$, подвержен искажению типа $b_i \to b_i + e$, $e = 1, 2, \ldots, q-1-b_i$ (или $b_i \to b_i - e$, $e = -1, -2, \ldots, -b_i$). Очевидно, что в случае $q = 2$ эти два вида несимметрических ошибок совпадают. В отличие от кодов, исправляющих большие несимметрические ошибки, кодам, исправляющим малые несимметрические ошибки, посвящен целый ряд работ, из которых следует особо выделить код Варшамова—Тененгольца ([2]), исправляющий одиночную малую несимметрическую ошибку над произвольным основанием $q \geqslant 2$.

В настоящей работе построен класс кодов, исправляющих одиночные большие несимметрические ошибки. Приведенная средняя оценка мощности этих кодов является оптимальной.

Пусть $p = 2q + 1$, где p — простое число, $\alpha = g^{\frac{p-1}{2}}$, g — примитивный элемент поля Галуа $GF(p^m)$. Тогда имеет место

Теорема. *Множество $M_{n,q}$ всех решений уравнения*

$$\sum_{i=1}^{n} x_i \alpha^i = a, \quad x_i \in \{0, 1, \ldots, q-1\}, \; a \in GF(p^m),$$

является q-ичным кодом длины $n = 2(p^m - 1)(p-1)^{-1}$, исправляющим одиночные большие несимметрические ошибки тогда и только тогда, когда $(m, q-1)^* = 1$.

Доказательство. Обозначим через $|\alpha^t|$ циклическую подгруппу поля $GF(p^m)$, образованную последовательными степенями элемента $\alpha \in GF(p^m)$. Рассмотрим разложение мультипликативной группы поля $GF(p^m)$ на смежные классы по циклической подгруппе $|\alpha^t = g^{\frac{p-1}{2}}|$. Утверждение теоремы эквивалентно тому, что при условии $(m, q-1) = 1$ все числа $1, 2, \ldots, q-1 = \frac{p-1}{2}$ лежат в различных смежных классах. Произвольный элемент r, принадлежащий простому полю $GF(p)$, можно представить в виде

$$r = g^{k\frac{p^m-1}{p-1}}, \qquad k = 0, 1, \ldots, p-2.$$

Два числа $\beta, \gamma \in GF(p)$ лежат в одном смежном классе тогда и только тогда, когда $\beta \cdot \gamma^{-1} \in |\alpha^t|$, откуда следует, что

$$g^{k\frac{p^m-1}{p-1}} \cdot g^{l\frac{p-1}{2}}, \quad k = 1, 2, \ldots, p-2; \qquad l = 1, 2, \ldots, 2\frac{p^m-1}{p-1}$$

или, что то же,

$$k\frac{p^m-1}{p-1} \equiv l\frac{p-1}{2} \pmod{p^m-1}. \tag{1}$$

Из условия $\left(m, \frac{p-1}{2}\right) = 1$ следует, что $\left(\frac{p^m-1}{p-1}, \frac{p-1}{2}\right) = 1$ и сравнение (1) имеет единственное решение при $k = \frac{p-1}{2}$ и $l = \frac{p^m-1}{p-1}$. Это означает, что в каждом смежном классе лежат ровно два числа r и $-r$ простого поля $GF(p)$ и, следовательно, все числа $\left|1, 2, \ldots, q-1 = \frac{p-1}{2}\right|$ лежат в различных смежных классах. Что и требовалось доказать.

---

* (x, y)—наибольший общий делитель чисел x и y.

Для мощности $M_{n,q}$ наилучшего, в смысле количества векторов, кода справедлива следующая оценка:

$$M_{n,q} > \frac{q^n}{(q-1)n+1},$$

являющаяся, как легко видеть, оптимальной.

Вычислительный центр Академии наук
Армянской ССР и Ереванского
государственного университета

Գ. Ն. ԳԵՎՈՐԳՅԱՆ, Ա. Հ. ԻԽԻԹԱՐՅԱՆ

Եզակի մեծ ոչսիմետրիկ սխալներ ուղղող կոդերի դաս

Ստացված է կամայական q հիմք ունեցող կոդերի դաս, որոնք ուղղում են եզակի մեծ ոչսիմետրիկ սխալներ և կարծես հանդիսանում են Հեմինգի ընդհանրացված կոդերի անալոգ ոչսիմետրիկ կապուղիների համար:

Կոդը որոշվում է որպես $GF(p^m)$ դաշտում

$$\sum_{i=1}^{n=2\frac{p^m-1}{p-1}} x_i g^{i(q-1)} = \alpha$$

հավասարման լուծումների բազմություն: Այստեղ $x_i \in \{0, 1, \ldots, q-1\}$, $\alpha \in GF(p^m)$, իսկ g-ն՝ $GF(p^m)$ դաշտի պրիմիտիվ տարրն է:

Հիշյալ կոդերի հզորության համար բերված է միջին գնահատականը, որը հավասար է՝

$$M_{n,q} > \frac{q^n}{(q-1)n+1}.$$

ЛИТЕРАТУРА — ԳՐԱԿԱՆՈՒԹՅՈՒՆ

[1] *W. H. Kim.*, IRE Trans. on Information Thebry, vol. IT—5 (1959). [2] *D. Constantin, T. R. N. Rao.* Inform. Contr., vol. 40 (1979). [3] *Р. Р. Варшамов, Г. М. Тенengольц,* Автоматика и телемеханика, т. 26 (1965).