Доклады Академии наук СССР
1975. Том 221, № 4

УДК 621.391.15 *КИБЕРНЕТИКА И ТЕОРИЯ РЕГУЛИРОВАНИЯ*

И. М. БОЯРИНОВ, Г. А. КАБАТЯНСКИЙ

АРИФМЕТИЧЕСКИЕ (n, A)-КОДЫ НАД ПРОИЗВОЛЬНЫМ ОСНОВАНИЕМ

(Представлено академиком А. И. Бергом 5 V 1974)

При сложении (вычитании) чисел в ЭВМ происходят ошибки. Для обнаружения или исправления ошибок числа кодируют арифметическим кодом. В работе строятся новые классы арифметических кодов и изучаются их корректирующие свойства.

1. Пусть Z_M — кольцо вычетов целых чисел по модулю M. Будем обозначать одними и теми же буквами как элементы кольца, так и соответствующие им целые числа. Любое $B \in Z_{r^n-1}$, $r>1$ и n — натуральные числа, единственным образом представимо в виде

$$B=b_{n-1}r^{n-1}+b_{n-2}r^{n-2}+\ldots+b_0, \quad 0\leqslant b_i<r. \tag{1}$$

Лемма 1. *Коэффициенты b_i представления* (1) *вычисляются из соотношения*

$$b_i=(Br^{n-i} \bmod (r^n-1)) \bmod r, \tag{2}$$

где $c \bmod d$ обозначает наименьший неотрицательный вычет c по модулю d.

B можно представить также в виде

$$B=a_{n-1}r^{n-1}+a_{n-2}r^{n-2}+\ldots+a_0, \quad 0\leqslant|a_i|<r. \tag{3}$$

Такое представление уже не будет единственным.

Весом представления (3) будем называть число ненулевых коэффициентов. Арифметическим циклическим весом $W_n(B)$ элемента B называется вес представления с минимальным весом. Легко показать, что $W_n(B)$ обладает следующими двумя важными свойствами:

$$W_n(rB)=W_n(B), \quad W_n(-B)=W_n(B). \tag{4}$$

Арифметическим циклическим расстоянием $d_n(B_1, B_2)$ между B_1, $B_2 \in Z_{r^n-1}$ назовем $W_n(B_1-B_2)$. Введенное расстояние будет метрикой.

Теорема 1. *Для любого $B \in Z_{r^n-1}$ существует представление* (3) *такое, что:*

1) *если $a_i<0$, то $a_{(i+1) \bmod n}=0$;*

2) *если $a_i \equiv -1 \pmod r$, то $a_{(i-1) \bmod n}=0$.*

Это представление, называемое циклическим каноническим представлением, всегда единственно, исключая случай, когда n четное и представления $B'=\pm((1-r)0\ldots(1-r)0)$ и $B'=\pm(0(r-1)\ldots0(r-1))$ имеют одинаковый вес и оба удовлетворяют условиям 1), 2). *Вес циклического канонического представления B равен $W_n(B)$.*

2. Арифметическим циклическим (n, A)-кодом, A делит r^n-1, будем называть ненулевой идеал $\mathfrak{A}=(A)$ в кольце Z_{r^n-1} вычетов целых чисел по модулю r^n-1. Обозначим $A^*=(r^n-1)/A$, тогда (n, A^*)-код, $\mathfrak{A}^*=(A^*)$, называется двойственным к (n, A)-коду (заметим, что $\mathfrak{A}\cdot\mathfrak{A}^*=0$ в кольце Z_{r^n-1}). Вектор (слово) B (n, A)-кода будем представлять как $B=b_{n-1}b_{n-2},\ldots, b_0$. Длина (n, A)-кода равна n, мощность (число

кодовых векторов) — A^*. Минимальным кодовым расстоянием $d_n(A)$-кода называется $d_n(A)=\min d_n(B_1, B_2)$ по всем $B_1, B_2\in\mathfrak{A}$, $B_1\neq B_2$. Очевидно, $d_n(A)=\min W_n(B)$ по всем ненулевым $B\in\mathfrak{A}$.

Пусть $B=lA=b_{n-1}b_{n-2}\ldots b_0$ — произвольный вектор (n, A)-кода. Тогда из леммы 1 вытекают следующие утверждения.

Лемма 2. *Коэффициенты b_i кодового вектора $B=lA$ удовлетворяют соотношению*

$$b_i=Ax_i(l) \bmod r, \quad x_i(l)=lr^{n-i} \bmod A^*. \tag{5}$$

Лемма 3. *Вес $B=lA$ равен числу $x_i(l)$ таких, что*

$$\frac{A^*}{r+1}\leqslant x_i(l)<\frac{rA^*}{r+1}. \tag{6}$$

Обозначим $\delta(x)$ количество целых чисел в $\left[\frac{x}{r+1}\ \frac{rx}{r+1}\right)$ Тогда

$$\delta(x)=\left[\frac{rx}{r+1}\right]-\left[\frac{x}{r+1}\right], \tag{7}$$

где $[a]$ — наибольшее целое, не большее a.

Теорема 2. *Сумма $\sigma_n(A)$ весов арифметического циклического (n, A)-кода равна произведению числа целых точек $\delta(A^*)$ в $\left[\frac{A^*}{r+1}, \frac{rA^*}{r+1}\right)$ на длину кода n:*

$$\sigma_n(A)=n\delta_n(A^*). \tag{8}$$

3. Введем нумератор весов (n, A)-кода

$$P(A, t)=\sum p_i t^i,$$

где p_i — число слов кода веса i.

Сопоставим каждому слову $B=lA$ (n, A)-кода элемент l кольца Z_{A^*} и определим $\omega(l)=W_n(lA)$. Тогда из (4) следует

$$\omega(\pm r^i l)=\omega(l). \tag{9}$$

Назовем орбитой множество F_l,

$$F_l=\{x\in Z_{A^*}:\ x=\pm r^i l\}.$$

Кольцо Z_{A^*} разбивается на непересекающиеся орбиты и функция $\omega(x)$ постоянна на них в силу (9). Обозначим $Z_{A^*}^{-1}$ группу обратимых (взаимно простых с A^*) элементов Z_{A^*} и рассмотрим подгруппу $H=\{\pm r^i\}$ в $Z_{A^*}^{-1}$. Разбиение Z_{A^*} на орбиты есть частный случай действия группы на множестве, а именно, множество — Z_{A^*}, группа — H, действие задается формулой $h(\alpha)=h\cdot\alpha$, $h\in H$, $\alpha\in Z_{A^*}$.

Пусть $A^*=\prod_{i=1}^{m} p_i^{\alpha_i}$, $\alpha_i>0$, p_i — простые, тогда

$$Z_{A^*}=\oplus Z_{p_i^{\alpha_i}}=\bigcup_{\beta}\left\{\prod_{i=1}^{m} p_i^{\alpha_i-\beta_i}\cdot Z_{A^*}^{-1}\right\}=\bigcup_{\beta} M_\beta,$$

$$\beta=\{\beta_i\},\quad 0\leqslant\beta_i\leqslant\alpha_i,\quad i=1, \ldots, m.$$

Теорема 3. *Если $\omega(\cdot)$ на каждом M_β постоянна, то нумератор весов (n, A)-кода равен*

$$P(A, t)=\sum_{\beta}\varphi\left(\prod_{i=1}^{m} p_i^{\beta_i}\right) t^{\omega_\beta} \tag{10}$$

и значение ω *на* M_β

$$\omega_\beta=\Big\{\sum_{\varepsilon}(-1)^{\sum_{i=1}^{m}\varepsilon_i}\cdot\delta\Big(\prod_{i=1}^{m}p_i^{\beta_i-\varepsilon_i}\Big)\Big\}\frac{n}{\varphi(\prod p_i^{\beta_i})} \tag{11}$$

где сумма берется по $\varepsilon=\{\varepsilon_i\}$; $\varepsilon_i=0$ *или* 1; $i=1,\ldots,m$; $\beta_i-\varepsilon_i\geqslant 0$.

В частности, ω *постоянна на* M_β, *если каждое* M_β *состоит из одной орбиты, а для этого, в свою очередь, необходимо и достаточно, чтобы* $M_\alpha=Z_{A^*}^{-1}$ *состояло из одной орбиты.*

Теорема 4. *Пусть* $A^*=\prod p_i^{\alpha_i}$. $Z_{A^*}^{-1}$ *состоит из одной орбиты тогда и только тогда, когда выполнено одно из следующих условий:*

I. 1) $A^*=p_1^{\alpha_1}p_2^{\alpha_2}$, $p_i>2$, $i=1, 2$.

а) r *— первообразный корень по модулю* $p_i^{\alpha_i}$, $(\varphi(p_1^{\alpha_1}), \varphi(p_2^{\alpha_2}))=2$ *и одно из* $p_i\equiv 1 \pmod 4$ *или*

б) r *— первообразный корень по модулю* $p_2^{\alpha_2}$,

$$\Big(\frac{\varphi(p_1^{\alpha_1})}{2}, \varphi(p_2^{\alpha_2})\Big)=1, \quad e(r, p_1^{\alpha_1})=\frac{\varphi(p_1^{\alpha_1})}{2},$$

где $e(x, N)$ *— показатель, которому принадлежит* x *по модулю* N.

I. 2) $A^*=p^\alpha$, $p>2$.

а) r *— первообразный корень по модулю* p^α *или*

б) $e(r, p^\alpha)=\varphi(p^\alpha)/2$ *и* $p\equiv -1 \pmod 4$.

II. r *нечетное.*

1) $A^*=2A_1^*$ *и* A_1^* *удовлетворяет условию* I.

2) $A^*=2^\alpha$, $\alpha>2$, *и* $e(r, 2^\alpha)=2^{\alpha-2}$.

3) $A^*=2^2p^\alpha$.

а) r *— первообразный корень по модулю* p^α, $p\equiv 1 \pmod 4$ *или*

б) $e(r, p^\alpha)=\varphi(p^\alpha)/2$ *и* $p\equiv -1 \pmod 4$.

Во всех описанных случаях верна теорема 3 и нумератор весов (n, A)-кода вычисляется по формулам (10), (11). Длина кода n кратна $\varphi(A^*)/2$, за исключением случаев $A^*=p^\alpha$, $A^*=2p^\alpha$, p^α удовлетворяет I. 2а), когда n кратно $\varphi(A^*)$.

Следствие 1. При $r=2$ коды, удовлетворяющие условиям I, описаны в ([1], [2]), исключая случай I. 1б), который описан лишь при $\alpha_1=\alpha_2=1$.

Следствие 2. Коды $A^*=p^\alpha$, удовлетворяющие условию I. 2), при $p\equiv 1 \pmod{(r+1)}$, эквидистантные и $d_n(A)=\dfrac{r-1}{r+1}n$.

Следствие 3. Коды, удовлетворяющие условию I. 2) при $\alpha=1$, т. е. $A^*=p$, также эквидистантные и $d_n=\delta(p)n/(p-1)$.

4. Пусть $r>2$, $A^*=(r-1)p^\alpha$, r — первообразный корень по модулю p^α. Если $p\equiv 1 \pmod{(r+1)}$, то

$$P(A, t)=1+(r-1)(p^\alpha-1)t^{n(r-1)/(r+1)}+(r-2)t^n, \quad d_n(A)=n\frac{r-1}{r+1}$$

и код при том же расстоянии имеет в $r-1$ раз большую мощность, чем эквидистантный код с $A^*=p^\alpha$. Если $p\not\equiv 1 \pmod{(r+1)}$, то явная формула $P(A, t)$ также найдена, но ввиду громоздкости не приводится.

5. Ниже рассматриваются некоторые границы для минимального расстояния $d_n(A)$ (n, A)-кодов. Используя лемму 3, можно показать, что для произвольного (n, A)-кода циклическое каноническое представление любого его ненулевого слова не содержит более $\theta=\left]\log_r\dfrac{A^*}{r+1}\right[$ нулей подряд ($]a[$ — наименьшее целое, не меньшее a). Отсюда получается граница

для минимального расстояния (n, A)-кодов

$$d \geqslant \frac{n}{\left]\log_r A^* \cdot \frac{r}{r+1}\right[}.$$

Эта граница достигается, например, на кодах $A^*=r^s-1$, где $s \mid n$.

Из теоремы 3 следует, что

$$d_n(A) \leqslant n\frac{\delta(A^*)}{A^*-1}.$$

Так как $\delta(A^*) \leqslant \frac{r-1}{r+1}(A^*+1)$, то

$$d_n(A) \leqslant n\frac{r-1}{r+1}\frac{A^*+1}{A^*-1}. \qquad (12)$$

Назовем (n_0, A_0)-код оптимальным в классе (n, A)-кодов, если не существует отличного от него кода с не меньшими расстоянием и мощностью и не большей длиной. Можно показать, что коды, достигающие границы (12), оптимальны.

Коды следствия 3 теоремы 4 при $p \equiv -1 \pmod{(r+1)}$ оптимальны. Неоптимальность таких кодов при $p \equiv 1 \pmod{(r+1)}$ следует из п. 4.

Замечание. Если в каждом классе вычетов lA идеала $\mathfrak{A}=(A)$, являющегося по нашему определению (n, A)-кодом, выбрать наименьшее неотрицательное число lA, то множество таких чисел образует арифметический циклический AN-код, $0 \leqslant N < A^*$.

Если обозначить $W(lA)$ арифметический вес числа lA, тогда, как легко видеть, $W_n(lA)=\min\{W(lA), W(r^n-1-lA)\}$ и $W(l, A) \geqslant W_n(l, A)$. Отсюда следует, что минимальные кодовые расстояния AN-кода и соответствующего ему (n, A)-кода совпадают, однако нумераторы весов будут несколько отличаться, в частности, (n, A)-код с $A^*=p$ будет эквидистантным, а соответствующий ему AN-код уже не будет эквидистантным при $A^*>r^4$.

Научный совет по комплексной проблеме «Кибернетика»
Академии наук СССР
Москва

Поступило
5 V 1974

ЦИТИРОВАННАЯ ЛИТЕРАТУРА

[1] *N. T. Tsao-Wu, S. H. Chang,* IEEE Trans. Inform. Theory, v. 15, 5, 628 (1969).
[2] *Ю. Г. Дадаев,* Проблемы передачи информации, т. 6, 1, 45 (1970).