PLISKA
STUDIA MATHEMATICA BULGARICA
ПЛИСКА
БЪЛГАРСКИ МАТЕМАТИЧЕСКИ СТУДИИ

For further information on
Pliska Studia Mathematica Bulgarica
visit the website of the journal http://www.math.bas.bg/~pliska/
or contact: Editorial Office
Pliska Studia Mathematica Bulgarica
Institute of Mathematics and Informatics
Bulgarian Academy of Sciences
Telephone: (+359-2)9792818, FAX:(+359-2)971-36-49
e-mail: pliska@math.bas.bg

ВЫЧЕТНЫЕ КОДЫ

СТЕФАН М. ДОДУНЕКОВ

В работе показано, что вычетные коды с простой блоковой длиной можно рассматривать как специальный случай циклических кодов с произвольной, не объязательно простой блоковой длиной. Для конструкции и исследования этих кодов использована теория общих круговых полей.

1. Определение вычетных кодов. Пусть $m=p_1^{k_1}p_2^{k_2}\dots p_t^{k_t}$ — каноническое разложение натурального числа m и q — простое число, $q\neq p_i$, $i=1, 2, \dots, t$. Обозначим через f мультипликативный порядок числа q по модулю m. Тогда, если φ — функция Эйлера, а $Q^{(m)}(x)$ — круговой многочлен степени m, то $\varphi(m)=fg=\deg Q^{(m)}(x)$ и $x^m-1=(x-1)P(x)Q^{(m)}(x)$.

Согласно теореме Кумера [1, с. 83], над конечным полем $GF(q)$ имеет место разложение $Q^{(m)}(x)=F_1(x)F_2(x)\dots F_g(x)$, где $F_i(x)$, $i=1, 2, \dots, g$ — неприводимые над $GF(q)$ многочлены степени f.

Пусть G — мультипликативная группа вычетов по модулю m, взаимно простых с модулем. Минимальная подгруппа H группы G, содержащая q — это циклическая группа, порожденная q: $H=\{1, q, q^2, \dots, q^{f-1}\}$. Так как $(G:H)=g$, то пусть $G=H+x_2H+\dots+x_gH$ — разложение G по подгруппе H. Положим для краткости $H_i=x_iH$, $i=2, 3, \dots, g$ ($H_1=H$), и рассмотрим многочлены $P_i(x)=\Pi_{r\in H_i}(x-\zeta^r)$, где ζ — примитивный корень из единицы степени m в подходящем расширении $GF(q)$. Отметим, что такой корень существует тогда и только тогда, когда $(m, q)=1$.

Лемма 1. *С точностью до номерирования* $P_i(x)=F_i(x)$.

Доказательство. Ясно, что $P_1(x)P_2(x)\dots P_g(x)=Q^{(m)}(x)$ и $\deg P_i(x)=f$. Покажем, что $P_i(x)$ — многочлены над полем $GF(q)$. Действительно, $P_i^q(x)=\Pi_{r\in H_i}(x^q-\zeta^{qr})=\Pi_{r\in H_i}(x^q-\zeta^r)=P(x^q)$, чем лемма доказана.

Пусть $g=se$, $e\geq 2$ и R — подгруппа G индекса e. Положим $R=H_1+H_2+\dots+H_s$ и пусть $G=R+j_2R+\dots+j_eR$. Согласно лемме 1, многочлены $g^{(i)}(x)=\Pi_{r\in R_i}(x-\zeta^r)$, $i=1, 2, \dots, e$, делящие x^m-1, являются многочленами над полем $GF(q)$. Здесь $R_1=R$, $R_k=j_kR$, $k=2, \dots, e$.

Определение. *Циклические коды над* $GF(q)$ *с порождающими многочленами* $g^{(i)}(x)$ *и блоковой длиной* m *называются* e*-вычетными кодами.*

2. Ограничение весов. Пусть α — примитивный корень из единицы степени n в конечном поле $GF(q^l)$, K — подмножество чисел по модулю n, замкнутое относительно умножения на q и $q(x)=\Pi_{r\in K}(x-\alpha^r)$. Пусть j — произвольное число, взаимно простое с n и $g(x)=\Pi_{r\in K}(x-\alpha^{jr})=\Pi_{r\in jK}(x-\alpha^r)$. Пусть $c(x)=c_0+c_1x+\dots+c_{n-1}x^{n-1}$ — произвольный многочлен над $GF(q^l)$ сте-

ПЛИСКА Български математически студии. Том 2, 1981, с. 3—5.

пени $<n$, а $\breve{c}(x)=\breve{c}_0+\breve{c}_1x+\cdots+\breve{c}_{n-1}x^{n-1}$ — многочлен с коэффициентами $\breve{c}_r=c_m$, где $m\equiv jr \pmod n$. Тогда имеет место следующая лемма.

Лемма 2. *Многочлен $c(x)$ кратен $g(x)$ тогда и только тогда, когда $\breve{c}(x)$ кратен $\breve{g}(x)$.*

Доказательство леммы 2 аналогично доказательству ее двоичного варианта [2, с. 152].

Согласно лемме 2, идеалы $(g^{(i)}(x))$ $(i=1, 2, \ldots, e)$ алгебры $GF(q)[x]/(x^m-1)$ эквивалентны относительно метрики Хэмминга и, следовательно, имеют одинаковые кодовые расстояния.

Пусть $C^{(i)}(x)$ — многочлен минимального веса d в множестве многочленов идеала $(g^{(i)}(x))$, не делящихся на $x-1$.

Из определения многочленов $g^{(i)}(x)$ и $C^{(i)}(x)$ следует, что

$$\prod_{i=1}^{e} C^{(i)}(x)\equiv 0 \pmod{Q^{(m)}(x)}. \tag{1}$$

Умножим сравнение (1) на $P(x)$. Получим

$$P(x)\prod_{i=1}^{e} C^{(i)}(x)\equiv 0 \left(\mathrm{mod}\sum_{i=0}^{m-1} x^i\right) \tag{2}$$

и, следовательно,

$$P(x)\prod_{i=1}^{e} C^{(i)}(x)=r(x)\sum_{i=0}^{m-1} x^i,$$

где $r(x)$ — многочлен, для которого $r(1)\neq 0$ в $GF(q)$. Кроме того,

$$P(x)\prod_{i=1}^{e} C^{(i)}(x)\equiv r(1)m \pmod{x-1}. \tag{3}$$

Многочлены $x-1$ и $1+x+\cdots+x^{m-1}$ взаимно просты и согласно китайской теореме об остатках, из (2) и (3) следует

$$P(x)\prod_{i=1}^{e} C^{(i)}(x)\equiv r(1)\, m\sum_{i=0}^{m-1} x^i \pmod{x^m-1}. \tag{4}$$

Следовательно, имеет место следующее утверждение.

Теорема 1. *Если d_p — вес многочлена $P(x)$, то $d_p d^e\geqq m$.*

В случае, когда $-1\notin R$, неравенство теоремы 1 можно улучшить.

Теорема 2. *Если $-1\notin R$, то $d_p d^{e-2}(d^2-d+1)\geqq m$.*

Доказательство. В этом случае для некоторого индекса $i\geqq 2$ можно выбрать $R_i=-R$ и $C^{(i)}(x)=x^{\deg C^{(1)}(x)}C^{(1)}(x^{-1})$. Требуемое неравенство следует из (4).

Пусть $m=p^\lambda$, a — первообразный корень по модулю m, $G=\{1, a, a^2, \ldots, a^{\varphi(m)-1}\}$ и пусть $R=\{1, a^e, a^{2e}, \ldots, a^{ke}\}$ — подгруппа e-тых степеней элемента a.

Следствие. *Если $k=2l$, то $d^{e-2}(d^2-d+1)\geqq p$.*

Доказательство. Так как $a^{e(2l+1)/2}=-1$, то ясно, что $-1\notin R$.

В этом случае

$$P(x)=\prod_{\nu=1}^{\lambda-1}Q^{(p^\nu)}(x)=\prod_{\nu=1}^{\lambda-1}Q^{(p)}(x^{p^{\nu-1}})$$

и, следовательно, $d_p=p^{\lambda-1}$. Применяя теорему 2, получаем искомое неравенство.

3. Вычетные коды с блоковой длиной $p_1 p_2 \dots p_t$. Пусть как и раньше $m=p_1^{k_1}p_2^{k_2}\dots p_t^{k_t}$ — каноническое разложение числа m, $n=p_1 p_2 \dots p_t$ и пусть над полем $GF(q)$

$$Q^{(n)}(x)=\Phi_1(x)\Phi_2(x)\dots\Phi_n(x), \tag{5}$$

где $\varphi(n)=hu$, h — мультипликативный порядок числа q по модулю n и $\Phi_i(x)$ $(i=1, 2, \dots, u)$ являются неприводимыми многочленами степени h над полем $GF(q)$.

Лемма 3. *Многочлен* $\Phi_i(x^{m/n})$ *неприводим над полем* $GF(q)$ *тогда и только тогда, когда* $f=hm/n$.

Доказательство. Из равенства

$$Q^{(m)}(x)=Q^{(m)}(x^{m/n})$$

и (5) следует, что $\Phi_1(x^{m/n})\Phi_2(x^{m/n})\dots\Phi_u(x^{m/n})=F_1(x)F_2(x)\dots F_g(x)$. Многочлены $F_i(x)$ — неприводимы над полем $GF(q)$, а степень каждого многочлена $\Phi_j(x^{m/n})$ равна hm/n. Поэтому $hm/n=vf$ и $\Phi_i(x^{m/n})$ являются неприводимыми над полем $GF(q)$ тогда и только тогда, когда $v=1$. Лемма доказана.

Отметим, что не всегда $f=hm/n$. Например, для $q=3$, $m=8$, $n=2$ получаем, что $h=1$, $f=2$, $hm/n=4$.

Пусть $f=hm/n$ и значит $u=g$. Отсюда ясно, что если существует e-вычетный код с блоковой длиной n, то существует и e-вычетный код с блоковой длиной m.

Теорема 3. *Если* $f=hm/n$, *то минимальный вес* e-*вычетного кода с блоковой длиной* m *не выше минимального веса* e-*вычетного кода с блоковой длиной* n.

Доказательство. Согласно лемме 3, можно положить $F_i(x)=\Phi_i(x^{m/n})$. Если через $h^{(i)}(x)$, $i=1, 2, \dots, e$, обозначим порождающие многочлены e-вычетных кодов с блоковой длиной n, то при подходящей номерации $g^{(i)}(x)=h^{(i)}(x^{m/n})$. Следовательно, если для многочлена $C(x)$ над $GF(q)$ степени $\leq n-1$ для некоторого $i=1, 2, \dots, e$ выполняется сравнение $C(x)\equiv 0 \pmod{h^{(i)}(x)}$, то $C(x^{m/n})\equiv 0 \pmod{g^{(i)}(x)}$. Этим теорема доказана.

ЛИТЕРАТУРА

1. Г. Вейль. Алгебраическая теория чисел. Москва, 1947.
2. Е. Р. Берлекэмп. Алгебраическая теория кодирования. Москва, 1971.

Единый центр математики и механики
1090 София П. Я. 373

Поступила 29. 1. 1975;
в переработанном виде 5. 11. 1976