КОДЫ ГОППА

Стефан М. Додунеков

В работах [1] и [2] Гоппа построил класс линейных кодов, названные (L, g)-коды. Зная только степень порождающего многочлена $g(z)$, можно вывести границы для параметров кода — для корректирующих и информационных возможностей. Кроме того, коды Гоппа содержат как подкласс примитивных БЧХ-кодов [7], [8] и имеют алгоритм декодирования, аналогичный алгоритму Берлекэмпа для БЧХ-кодов.

Здесь мы исследуем некоторые свойства (L, g)-кодов, снова подчеркивающие их связь с БЧХ-кодами (§1 и §2). В §3 используем результаты [3], чтобы сконструировать (L, g)-коды, инвариантные относительно групп подстановок.

§ 1. ОПРЕДЕЛЕНИЕ И ОСНОВНЫЕ РЕЗУЛЬТАТЫ

Пусть

$$L \subset GF(q^m),\ L=\{\alpha_1, \alpha_2, \ldots, \alpha_n\},\ n \leqq q^m,$$

и V_n — n-мерное векторное пространство над полем $GF(q)$, q — простое число. Обозначим через R векторное пространство рациональных функций над $GF(q^m)$ вида

$$\zeta_x(z)=\sum_{i=1}^{n} \frac{b_i}{z-\alpha_i}, \quad x=(b_1, b_2, \ldots, b_n) \in V_n.$$

Если

$$\zeta_x(z)=\frac{\psi(z)}{\varphi(z)},$$

в R введем норму следующим образом:

$$\|\zeta_x(z)\|=\deg \varphi(z).$$

Соответствие

$$x \to \zeta_x(z)$$

порождает изометрию между V_n и R (если рассматривать V_n как метрическое пространство относительно метрики Хэмминга). Таким образом можно считать, что коды — подмножества R.

Пусть $g(z)$ многочлен над $GF(q)^m$, для которого $g(\alpha_i) \neq 0$, $i=1, 2, \ldots, n$. Линейное подпространство всех $\zeta_x(z) \in R$, для которых

(1) $$\zeta_x(z) \equiv 0 \pmod{g(z)},$$

называется (L, g)-кодом.

Определение корректно, так как для любого $\zeta_x(z) = \frac{\psi(z)}{\varphi(z)} \in R$ $(\varphi(z), g(z)) = 1$ и многочлен $\varphi(z)$ обратим в алгебре многочленов над $GF(q^m)$ по модулю $g(z)$.

Теорема 1. [1]. Вес произвольного элемента (L, g) — кода не меньше чем $\deg g(z) + 1$.

Теорема 2. [1]. (L, g)-код имеет не более $m \deg g(z)$ проверочных символов.

Известно [6], что для каждого линейного кода с блоковой длиной n, размерностью K и кодовым расстоянием d выполняется неравенство

(2) $$d \leqq n - k + 1.$$

Коды, для которых $d = n - k + 1$, называются кодами с достижимым максимальным расстоянием. В классе всех (n, k)-кодов они имеют наилучшие корректирующие возможности.

Теорема 3. Все (L, g)-коды над $GF(q)$ являются кодами с достижимым максимальным расстоянием.

Доказательство. Покажем сначала, что для числа r проверочных символов (L, g)-кода над $GF(q^m)$ выполняется неравенство

(3) $$l \leqq r \leqq ml,$$

где $l = \deg g(z)$. Действительно, так как (L, g)-код линеен, то из (2)

(4) $$d \leqq n - k + 1 \leqq r + 1.$$

Но по теореме 1 $r \leqq ml$, а по теореме 2 $d \geqq l + 1$. Из (4) и этих двух неравенств следует (3). Если $m = 1$, из (3) следует, что $r = l$. Теорема доказана.

Следствие. Коды Рида—Соломона являются кодами с достижимым максимальным расстоянием.

§ 2. (L, g)-КОДЫ, БЛИЗКИЕ К БЧХ-КОДАМ

Если $L = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$, то положим

$$F(z) = \prod_{i=1}^{n} (z - \alpha_i)^{q-1}$$

и пусть $x = (a_1, a_2, \ldots, a_n)$ принадлежит (L, g)-коду над $GF(q^m)$, q — простое число, с порождающим многочленом $g(z)$, делителем $F'(z)$. С каждым вектором x естественным образом связывается многочлен

$$f_x(z)=\prod_{i=1}^{n}(z-\alpha_i)^{a_i}.$$

Ясно, что

$$\zeta_x(z)=\frac{f_x'(z)}{f_x(z)}.$$

Пусть

(5) $$F(z)=f_x(z)h_x(z).$$

Дифференцируя (5), получим, что

(6) $$F'(z)=f_x'(z)h_x(z)+f_x(z)h_x'(z).$$

Так как $(F(z), g(z))=1$, то $F(z)$ обратим в алгебре многочленов по модулю $g(z)$ над $GF(q^m)$ и из (6) следует, что

$$\frac{h_x'(z)}{h_x(z)}\equiv\frac{F'(z)}{F(z)}\equiv 0 \pmod{g(z)}.$$

Следовательно, вектор $\bar{x}=(q-1-a_1,\ q-1-a_2,\ \ldots,\ q-1-a_n)$ принадлежит коду и если через $A_0, A_1, \ldots, A_n$ обозначим спектр кода (A_i — число векторов весом i), получим

Теорема 4. Если $g(z)/F'(z)$, то $A_n\geqq q-1$.

Следствие 1. Если $q=2$ и $g(z)/F'(z)$, то $A_{n-s}=A_j$ для каждого $j=0, 1, \ldots, n$.

Доказательство. Если $q=2$, единственный вектор x, вес которого равен n, это $x=(1, 1, \ldots, 1)$ и для каждого y веса j вектор $x-y$ имеет вес $n-j$.

Следствие 2. В двоичных примитивных БЧХ-кодах $A_{n-j}=A_j$ для, каждого $j=0, 1, \ldots, n$.

Доказательство. Здесь $n=2^m-1$, $L=\{1, \alpha, \ldots, \alpha^{n-1}\}$, α — примитивный корень из единицы степени n, $F(z)=z^n-1$, $g(z)=z^t$.

Пусть $\beta_1, \beta_2, \ldots, \beta_r$ — различные корни многочлена $g(z)$ и $\{\beta_1, \beta_2, \ldots, \beta_r\}\subset GF(q^m)$, $L=\{GF(q^m)\setminus\{\beta_1, \beta_2, \ldots, \beta_r\}\}$. Положим

$$L_\alpha=\{GF(q^m)\setminus\{\beta_1-\alpha, \ldots, \beta_r-\alpha\}\},\ \alpha\in GF(q^m).$$

Теорема 5. $(L_\alpha, g(z+\alpha))$-код и (L, g)-код эквивалентны.

Доказательство. Пусть

$$\zeta_x=\sum_{i=1}^{n}\frac{a_i}{z-\alpha_i}\equiv 0 \pmod{g(z)}.$$

Тогда

$$\zeta_x(z+\alpha)\equiv\sum_{i=1}^{n}\frac{a_i}{z-(\alpha_i-\alpha)}\equiv 0 \pmod{g(z+\alpha)}$$

и соответствие

$$\zeta_x(z)\to\zeta_x(z+\alpha)$$

индуцирует взаимно однозначное соответствие между (L, g) и $(L_\alpha, g(z+\alpha))$-кодами, сохраняющее вес.

Следствие. ([2], теорема 5). Любые два кумулятивных кода, порожденных многочленами одной и той же степени, эквивалентны. ((L, g)-коды с порождающим многочленом вида $g(z)=(z-\beta)^r$, $\beta \in GF(q^m)$, называются кумулятивными).

§ 3. КОНСТРУКЦИЯ (L, g)-КОДОВ, ИНВАРИАНТНЫХ ОТНОСИТЕЛЬНО ГРУПП ПОДСТАНОВОК

Сделаем несколко предварительных замечаний.

Пусть $S=\begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix}$ произвольная подстановка группы S_n и $L_s=\{\alpha_{i1}, \alpha_{i2}, \dots, \alpha_{in}\}$ — соответствующая ей перестановка L.

Лемма. (L, g)-код совпадает с (L_s, g)-кодом тогда и только тогда, когда (L, g)-код инвариантен относительно s.

Доказательство. Если $x \in (L, g)=(L_s, g)$, $x=(a_1, a_2, \dots, a_n)$, то одновременно выполняются сравнения

$$\sum_{i=1}^{n} \frac{a_i}{z-\alpha_i} \equiv 0 \pmod{g(z)} \tag{7}$$

и

$$\sum_{j=1}^{n} \frac{a_i}{z-\alpha_{i_j}} \equiv 0 \pmod{g(z)}. \tag{8}$$

Поэтому

$$\sum_{i=1}^{n} \frac{a_{s(i)}}{z-\alpha_i} \equiv 0 \pmod{g(z)} \tag{9}$$

и $s(x) \in (L, g)$-коду для всех x.

Пусть (L, g)-код инвариантен относительно S. Тогда из (7) и (9) следует (8). Лемма доказана.

Теорема 6. Над $GF(q)$ (q — простые число) существует многочлен степени m, инвариантный относительно группы T трансформаций вида $z \to z+\alpha$, $\alpha \in GF(q)$, тогда и только тогда, когда $m \equiv 0 \pmod q$.

Доказательство. Необходимость условия получаем легко, сравнивая коэффициенты перед z^{m-1} в равенстве $g(z)=g(z+\alpha)$.

Чтобы доказать достаточность, приведем эффективную конструкцию многочлена степени $m=qm_1$, инвариантного относительно T. Пусть $m=q^c p_1^{c_1} p_2^{c_2} \dots p_t^{c_t}=qm_1$ и пусть

$$m_1=\sum_{i=1}^{r} q_i,$$

где q_i — простые числа, $q_i \neq q$ для $i=1, 2, \dots, r$.

По следствию из теоремы 1 ([3]) можно выбрать нормированные неприводимые многочлены над $GF(q)$ $g_i(z)$ степени $q\,q_i$, инвариантные относительно T. Многочлен

$$g(z)=\prod_{i=1}^{r} g_i(z)$$

инвариантен относительно T и $\deg g(z)=m$.

Теорема доказана.

Пусть $g(z)$ инвариантный относительно T многочлен и $\beta_1, \beta_2, \ldots, \beta_r$ — корни $g(z)$, принадлежащие $GF(q^m)$. Положим

$$L=\{GF(q^m)\setminus\{\beta_1, \beta_2, \ldots, \beta_r\}\}=\{\alpha_1, \ldots, \alpha_n\}$$

и пусть α произвольный элемент поля $GF(q)$. Так как $\beta_1, \beta_2, \ldots, \beta_r \in GF(q^m)$, элементы $\beta_1-\alpha, \ldots, \beta_r-\alpha \in GF(q^m)$ и являются корнями $g(z)$. Следовательно, $\{\beta_1-\alpha, \ldots, \beta_r-\alpha\}=\{\beta_1, \ldots, \beta_r\}$ и $\{\alpha_1-\alpha, \ldots, \alpha_n-\alpha\}$ — перестановка элементов $\alpha_1, \ldots, \alpha_n$, например, $\alpha_{j_1}, \ldots, \alpha_{j_n}$. Подстановка $s_\alpha=\begin{pmatrix}1 & 2 \ldots n\\ j_1 & j_2 \ldots j_n\end{pmatrix}$ называется порожденной элементом α.

Если $x=(a_1, \ldots, a_n) \in (L, g)$-коду, т. е. если

$$\zeta_x(z)=\sum_{i=1}^{n} \frac{a_i}{z-\alpha_i} \equiv 0 \pmod{g(z)},$$

то

$$\zeta_x(z+\alpha)=\sum_{i=1}^{n} \frac{a_i}{z-\alpha_{j_i}} \equiv 0 \pmod{g(z)}$$

и $x \in (L_{s_\alpha}, g)$-коду. По лемме 4 следует

Теорема 7. Если многочлен $g(z)$ инвариантен относительно T и $\beta_1, \ldots, \beta_r$ — корни $g(z)$, принадлежащие полю $GF(q^m)$, а $L=\{GF(q^m)\setminus\{\beta_1, \ldots, \beta_r\}\}$, то (L, g)-код инвариантен относительно группы подстановок, порожденных элементами T.

Коды, инвариантные относительно группы подстановок координатных позиций, представляются весьма интересными и это не случайно. При действии группы на код в одну орбиту попадают слова одинакового веса и чтобы изучить весовую структуру такого кода, достаточно лишь найти представителей всех различных орбит. Для циклических кодов этот вопрос вполне решен в работах [9] и [10] — эффективно найдены представители циклов, а в [4] и [5] это представление использовано для определения спектров некоторых циклических кодов.

Единственный известный нам результат в этом направлении, связанный с (L, g)-кодами, получен в [11], но он относится к удлиненным (L, g)-кодам.

ЛИТЕРАТУРА

1. Гоппа, В. Д.: Новый класс линейных корректирующих кодов. Проблемы передачи информации, 3 (1970), 24—30.
2. Гоппа, В. Д.: Рациональное представление кодов и (L, g)-коды. Проблемы передачи информации, 3 (1971), 41—48.
3. Додунеков, С. М.: Существенно различные неприводимые многочлены над конечными полями. Год. Соф. унив., Мат. фак., 66 (1972), 169—175.
4. Оганесян, С. Ш., Ягджян, В. Г.: Класс оптимальных циклических кодов с основанием p. Проблемы передачи информации, 2 (1972), 109 — 110.
5. Оганесян, С. Ш., Ягджян, В. Г.: Объединение циклических представителей по одинаковым весам. Труды ВЦ АН Арм. ССР и Ер. ГУ, (1970), № 6, 39—48.
6. Берлекэмп, Е. Р.: Алгебраическая теория кодирования. М., Мир, 1971.
7. Bose, R. C., Ray-Chaudhuri, D. K.: On a class of error-correcting binary group codes. Inf. and Control, 3 (1960), 68—79, 279—290.
8. Gorenstein, D. C., Zierler, N.: A class of error-correcting codes in p^m symbols. J. Soc. Indus. Appl. Math., 9 (1961), 207—214.
9. Tavares, S. E., Allard, P. E., Shiva, S. G. S.: On the decomposition of cyclic codes into cyclic classes. Inf. and Control, 18 (1971), № 4, 342 — 354.
10. Tavares, S. E., Allard, P. E., Shiva, S. G. S.: A note on the decomposition of cyclic codes into cyclic classes. Inf. and Controll, 22 (1973), No. 1, 100—106.
11. Berlekamp, E. R., Moreno, O.: Extended double-error-correcting binary Goppa codes are cyclic. IEEE Trans. Inf. Theory, IT — 19 (1973), No. 6, 817 — 818.

Постъпила на 14. XII. 1974 г.

GOPPA CODES

S. M. Dodunekov

(SUMMARY)

Notations:

$GF(q^m)$ — finite field with q^m elements, q — prime number;

L — subset of $GF(q^m)$ with elements $\alpha_1, \alpha_2, \ldots, \alpha_n$, $n \leqq q^m$;

$g(z)$ — polynomial over $GF(q^m)$ with no zeros in L;

(L, g)-code — Goppa code with generator polynomial $g(z)$.

The following results are proved:

Theorem 3. All (L, g)-codes over $GF(q)$ are maximal.

Let $F(z)=\prod_{i=1}^{n}(z-\alpha_i)^{q-1}$ and A_i, $i=0, 1, 2, \ldots, n$, denotes the number of elements in a (L, g)-code of weight i.

Theorem 4. If $g(z)/F'(z)$, then $A_n \geqq q-1$.

Corollary 1. If $g(z)/F'(z)$ and $q=2$, then $A_{n-j}=A_j$ for every $j=0, 1, \ldots, n$.

Theorem 6. There exists a polynomial $g(z)$ over $GF(q)$ of degree m invariant under the group T of linear transformations $z \to z+\alpha$, $\alpha \in GF(q)$ iff $m \equiv 0 \pmod q$.

Theorem 7. If $g(z)$ is invariant under T and $L=\{GF(q^m)\setminus\{\beta_1, \ldots, \beta_r\}\}$, where $\beta_1, \beta_2, \ldots, \beta_r$ are the zeros of $g(z)$ in $GF(q^m)$, then the (L, g)-code is invariant under the group of permutations of coordinate positions, generated by T.