

СОВЕРШЕННЫЕ ДВОИЧНЫЕ КОДЫ С ТРИВИАЛЬНЫМ ЯДРОМ

А. М. Романов

Предлагается конструкция совершенных двоичных кодов с тривиальным ядром для всех длин $n = 2^k - 1$, $k \geq 4$.

Пусть E^n — векторное пространство размерности n над полем Галуа $GF(2)$. Код C длины n рассматривается как подмножество векторов из E^n . Векторы, принадлежащие коду, называются *кодowymi словами*. Расстояние Хемминга $d(\mathbf{a}, \mathbf{b})$ между двумя векторами \mathbf{a} и \mathbf{b} равно числу координат, в которых \mathbf{a} и \mathbf{b} различаются. Код C длины n называется *совершенным двоичным $(n, 3)$ -кодом*, если расстояние Хемминга между любыми двумя векторами из C не меньше 3 и для любого вектора $\mathbf{a} \in E^n \setminus C$ найдется единственное кодовое слово $\mathbf{c} \in C$ такое, что $d(\mathbf{a}, \mathbf{c}) = 1$. Известно, что двоичные совершенные $(n, 3)$ -коды существуют лишь при $n = 2^k - 1$, $k = 1, 2, \dots$. Совершенные $(n, 3)$ -коды также называются *кодами Хемминга*. Существует единственный с точностью до изоморфизма (перестановки координат) линейный двоичный код Хемминга длины n . Подмножество $K \subseteq E^n$ называется *ядром* кода C (обозначается через $\ker C$), если $C + \mathbf{x} = C$ для любого вектора $\mathbf{x} \in K$. Через $\dim K$ обозначается размерность ядра K . Если $\dim K = 1$, то ядро называется *тривиальным*. Все не определяемые в статье понятия можно найти в [2].

В [5] предложен совершенный двоичный $(n, 3)$ -код длины 15 с тривиальным ядром. В [6] авторы, опираясь на мощностные оценки, доказали существование таких координат i_1, \dots, i_k и векторов $\mathbf{x}_1, \dots, \mathbf{x}_k$, принадлежащих линейному двоичному коду Хемминга H длины $n = 2^k - 1$, $k \geq 4$, что множество

$$H' = \left(H \setminus \left(\bigcup_{q=1}^k R_{i_q} + \mathbf{x}_q \right) \right) \cup \left(\bigcup_{q=1}^k R_{i_q} + \mathbf{x}_q + \mathbf{e}_{i_q} \right)$$

является нелинейным двоичным кодом Хемминга длины n и $\dim \ker H' = 1$.

При этом через R_{i_q} обозначено подпространство, порожденное векторами веса 3 кода H с единичной i_q -й координатой, а через e_{i_q} обозначен базисный вектор, в котором i_q -я координата равна 1.

В настоящей работе в явном виде найдены упомянутые выше координаты i_1, \dots, i_k и векторы x_1, \dots, x_k . Для этого используется достаточное условие непересекаемости смежных классов, образованных подпространствами R_{i_q} при разных i_q , которое было получено в [3]. Тем самым предложена конструкция совершенных двоичных $(n, 3)$ -кодов для всех допустимых длин начиная с $n = 15$.

Пусть H — линейный двоичный код Хемминга длины n , который строится по известной схеме [1]

$$H = \left\{ (u, |u|, u + v) \mid u \in E^{\frac{n-1}{2}}, v \in H^{\frac{n-1}{2}} \right\},$$

где $H^{\frac{n-1}{2}}$ — код длины $\frac{n-1}{2}$, построенный по этой схеме на предыдущем шаге.

Из n координат пространства E^n выберем k таких координат i_1, \dots, i_k , что $i_1 = 1, i_2 = 2, i_3 = 2^2, \dots, i_k = 2^{k-1}$.

Известно, что слова веса 3 кода Хемминга длины n соответствуют системе троек Штейнера порядка n . В случае, когда код Хемминга является линейным, система троек Штейнера, сопоставленная с кодом, является проективным пространством, а тройки — прямыми этого пространства. Проективное пространство, соответствующее коду H , обозначим через $PG(H)$.

Для любых целых p и s , $1 \leq p \leq n+1$, $1 \leq s \leq n+1$ и $p \neq s$, положим $T^n(p, s) = t$ при $\{p, s, t\} \in PG(H)$, $T^n(p, n+1) = p$ и $T^n(n+1, s) = s$.

Утверждение 1. Никакие три точки из множества $\{i_1, \dots, i_k\}$ не являются коллинеарными.

Доказательство. Поскольку код H строится по приведенной выше схеме, то проективное пространство $PG(H)$ содержит прямые двух видов:

$$\left\{ p, s, T^{\frac{n-1}{2}}(p, s) + \frac{n+1}{2} \right\} \text{ при } p \leq \frac{n+1}{2}, s \leq \frac{n+1}{2};$$

$$\left\{ p + \frac{n+1}{2}, s + \frac{n+1}{2}, t + \frac{n+1}{2} \right\} \text{ при } \{p, s, t\} \in PG(H^{\frac{n-1}{2}}).$$

Следовательно, любая прямая из $PG(H)$ содержит элемент, величина которого превосходит $\frac{n+1}{2} = 2^{k-1}$. Утверждение доказано.

Рассмотрим k векторов $(a_i \dots a_i)$ длины 2^{k-1} таких, что $a_1 = 0$, $a_2 = 10, a_3 = 1100, \dots, a_k = \underbrace{1 \dots 1}_{2^{k-2}} \underbrace{0 \dots 0}_{2^{k-2}}$. В векторах $(a_i \dots a_i)$ удалим последнюю координату и полученные векторы обозначим через v_1, \dots, v_k .

Пусть \mathbf{u} — вектор длины $\frac{n+1}{2}$, принадлежащий расширенному коду Хемминга $H^{\frac{n+1}{2}}$. Положим $\mathbf{x}_1 = (\mathbf{u}, \mathbf{v}_1), \dots, \mathbf{x}_k = (\mathbf{u}, \mathbf{v}_k)$. Легко заметить, что при $k \geq 4$ векторы $\mathbf{v}_1, \dots, \mathbf{v}_k$ принадлежат коду $H^{\frac{n-1}{2}}$, а векторы $\mathbf{x}_1, \dots, \mathbf{x}_k$ — коду H .

Утверждение 2. При $k \geq 4$ и $p \neq s$ имеет место соотношение

$$(R_{i_p} + \mathbf{x}_p) \cap (R_{i_s} + \mathbf{x}_s) = \emptyset.$$

Доказательство. При $k \geq 4$ векторы $\mathbf{v}_1, \dots, \mathbf{v}_k$ имеют четный вес. Следовательно, как показано в работе [3], для того чтобы пересечение подмножеств $R_{i_p} + \mathbf{x}_p$ и $R_{i_s} + \mathbf{x}_s$ было пусто, достаточно показать, что в векторах \mathbf{x}_p и \mathbf{x}_s значения координат с номером t различны, а номер t определяется при помощи функции $T^n(i_p, i_s)$. Выполнимость достаточного условия при начальных значениях n проверяется непосредственно. Пусть достаточное условие выполнено при $\frac{n-1}{2}$. Допустим, что $p \neq k, s \neq k$. Тогда из равенства $T^n(i_p, i_s) = T^{\frac{n-1}{2}}(i_p, i_s) + \frac{n+1}{2}$ и того, что векторы $\mathbf{v}_1, \dots, \mathbf{v}_k$ имеют периодическое строение, следует выполнимость этого условия при n . Пусть $p = k$ (при $s = k$ проводятся аналогичные рассуждения). Тогда $i_p = 2^{k-1} = \frac{n+1}{2}$ и $T^n(\frac{n+1}{2}, i_s) = T^{\frac{n-1}{2}}(\frac{n+1}{2}, i_s) + \frac{n+1}{2} = i_s + \frac{n+1}{2}$. Нетрудно заметить, что значение координаты $i_s = 2^{s-1}$ в векторе \mathbf{v}_s равно 0, а значение координаты i_s ($1 \leq i_s \leq 2^{k-2}$) в векторе \mathbf{v}_k равно 1. Утверждение доказано.

Теорема 1. Для кода H длины $n = 2^k - 1, k \geq 4$, множество

$$H' = \left(H \setminus \left(\bigcup_{q=1}^k R_{i_q} + \mathbf{x}_q \right) \right) \cup \left(\bigcup_{q=1}^k R_{i_q} + \mathbf{x}_q + \mathbf{e}_{i_q} \right)$$

является совершенным двоичным $(n, 3)$ -кодом и $\dim \ker H' = 1$.

Доказательство аналогично доказательству теоремы 3 из [6]. В силу утверждения 2 при $k \geq 4$ подмножества $R_{i_1} + \mathbf{x}_1, \dots, R_{i_k} + \mathbf{x}_k$ попарно не пересекаются. Отсюда и из [4, 6] следует, что множество H' является совершенным двоичным $(n, 3)$ -кодом.

Далее покажем, что $\ker H' = \bigcap_{q=1}^k R_{i_q}$. Предположим, что код H' содержит нулевой вектор. Тогда очевидно, что $\ker H' \subseteq H'$. Пусть $\mathbf{y} \in \ker H'$. Тогда либо $\mathbf{y} \in H$, либо $\mathbf{y} \in R_{i_q} + \mathbf{x}_q + \mathbf{e}_{i_q}$. Допустим, что $\mathbf{y} \in H$. Тогда $(R_{i_q} + \mathbf{x}_q + \mathbf{e}_{i_q}) + \mathbf{y} \subseteq H'$, так как $\mathbf{y} \in \ker H'$, и $(R_{i_q} + \mathbf{x}_q + \mathbf{y}) + \mathbf{e}_{i_q} \subseteq H + \mathbf{e}_{i_q}$, так как $\mathbf{y} \in H$ и H является линейным кодом. Поскольку $H' \cap H + \mathbf{e}_{i_q} = R_{i_q} + \mathbf{x}_q + \mathbf{e}_{i_q}$, то $R_{i_q} + \mathbf{x}_q + \mathbf{e}_{i_q} + \mathbf{y} = R_{i_q} + \mathbf{x}_q + \mathbf{e}_{i_q}$. Следовательно, $\mathbf{y} \in R_{i_q}$ при $q = 1, \dots, k$ и $\mathbf{y} \in \bigcap_{q=1}^k R_{i_q}$.

Пусть $y \in R_{i_s} + x_s + e_{i_s}$. Тогда $(R_{i_p} + x_p + e_{i_p}) + y \subseteq H'$ и $(R_{i_p} + x_p + e_{i_p}) + y \subseteq H + e_{i_p} + y = H + e_{i_p} + e_{i_s} = H + e_{i_t}$. Следовательно, $H' \cap H + e_{i_t} \neq \emptyset$ и, значит, $i_t \in \{i_1, \dots, i_k\}$. Так как $H + e_{i_p} + e_{i_s} = H + e_{i_t}$, то $H + e_{i_p} + e_{i_s} + e_{i_t} = H$ и $e_{i_p} + e_{i_s} + e_{i_t} \in H$. Таким образом, точки i_p, i_s, i_t принадлежат множеству $\{i_1, \dots, i_k\}$ и являются коллинеарными, что противоречит утверждению 1.

Известно [6], что подпространство $R_{i_1} \cap \dots \cap R_{i_r}$ имеет размерность 2^{k-r} . Следовательно, $\dim \ker H' = 1$. Теорема 1 доказана.

В работе [6] для доказательства существования множества векторов x_{i_1}, \dots, x_{i_k} используются следующие рассуждения. Число смежных классов $R_j + x$, образованных подпространством R_j в коде H , равно $2^{\frac{n+1}{2} - \log(n+1)}$. Поскольку множество $R_i \cap R_j$ является подпространством и $|R_i \cap R_j| = 2^{\frac{n+1}{4}}$, то число смежных классов $R_j + x$, имеющих непустое пересечение с подпространством R_i , равно $2^{\frac{n-3}{4}}$, что значительно меньше их общего числа. Следовательно, существует вектор x такой, что $R_i \cap R_j + x = \emptyset$. Продолжая эти рассуждения, можно доказать существование требуемого множества векторов.

ЛИТЕРАТУРА

1. Васильев Ю. Л. О негрупповых плотно упакованных кодах // Проблемы кибернетики. М.: Физматгиз, 1962. Вып. 8. С. 337–339.
2. Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А. Теория кодов, исправляющих ошибки. М.: Связь, 1979.
3. Романов А. М. О построении совершенных нелинейных двоичных кодов инверсией символов // Дискрет. анализ и исслед. операций. Сер. 1. 1997. Т. 4, № 1. С. 46–52.
4. Etzion T., Vardy A. Perfect binary codes: construction, properties and enumeration // IEEE Trans. Inform. Theory. 1994. V. 40, N 3. P. 754–763.
5. Heden O. A binary perfect code of length 15 and codimension 0 // Designs, Codes and Cryptography. 1994. V. 4, N 3. P. 213–220.
6. Phelps K. T., LeVan M. Kernels of nonlinear Hamming codes // Designs, Codes and Cryptography. 1995. V. 6, N 3. P. 247–257.

Адрес автора:

Институт математики
им. С. Л. Соболева СО РАН,
пр. Академика Коптюга, 4,
630090 Новосибирск, Россия.
E-mail: rom@math.nsc.ru

Статья поступила

27 сентября 1999 г.