ДИСКРЕТНЫЙ АНАЛИЗ И ИССЛЕДОВАНИЕ ОПЕРАЦИЙ
Октябрь—декабрь 1997. Серия 1. Том 4, № 4, 75–78

УДК 519.72

О НЕСИСТЕМАТИЧЕСКИХ СОВЕРШЕННЫХ КОДАХ ДЛИНЫ 15

А. М. Романов

Описываются несистематические совершенные двоичные коды длины 15.

Пусть E^n — векторное пространство размерности n над полем $GF(2)$. Код длины n рассматривается как подмножество векторов из E^n. Векторы, принадлежащие коду, называются кодовыми словами. Расстояние Хэмминга d между двумя векторами равно числу разрядов, в которых они различаются. Код C^n длины n называется совершенным $(n,3)$-кодом, если для любого вектора $\mathbf{a} \in E^n$ найдется единственное кодовое слово $\mathbf{c} \in C^n$ такое, что $d(\mathbf{a},\mathbf{c}) \leqslant 1$. Известно, что совершенные $(n,3)$-коды существуют лишь при $n = 2^p - 1$, где $p = 1, 2, \ldots$

Совершенный код C^n называется *систематическим*, если найдется $\log(n+1)$ таких разрядов (называемых проверочными), что после удаления этих разрядов из всех слов кода C^n получается множество всех слов длины $n - \log(n+1)$. Неудаленные разряды называются информационными.

Все не определяемые в статье понятия можно найти в [1].

Настоящая работа написана в связи с выходом статьи [2], в которой для $n \geqslant 255$ доказано существование несистематических совершенных двоичных кодов.

Ниже приводится конструкция несистематических совершенных двоичных кодов длины 15. При построении этих кодов использованы идеи из работы [4]. Несистематичность построенных кодов проверена при помощи компьютера. Автору стало известно, что несистематические совершенные двоичные коды предложены также в [3].

Пусть C^n — некоторый совершенный $(n,3)$-код. Кодовое слово $\mathbf{c}' = (c'_1, \ldots, c'_n) \in C^n$ назовем *соседним* с кодовым словом $\mathbf{c} = (c_1, \ldots, c_n) \in C^n$ по i-му разряду, если

$$d((c'_1, \ldots, c'_i, \ldots, c'_n), (c_1, \ldots, \bar{c}_i, \ldots, c_n)) = 2,$$

где $\bar{c}_i = 0$ при $c_i = 1$ и $\bar{c}_i = 1$ при $c_i = 0$.

© 1997 Романов А. М.

Подмножество I_i слов из C^n назовем *инвертируемым* по i-му разряду, если для каждого слова $\mathbf{c} \in I_i$ множеству I_i принадлежат все слова из C^n, соседние со словом $\mathbf{c}$ по i-му разряду.

Очевидно, что любое кодовое слово по каждому из своих разрядов порождает инвертируемое подмножество слов из C^n. Такое кодовое слово назовем *порождающим.*

Приведем ряд обозначений и два утверждения из работы [4], которые потребуются в дальнейшем.

Через $\bar{I}_i$ обозначим подмножество слов, которое получается в результате замены всех слов из I_i на слова с инвертированным i-м разрядом.

Утверждение 1. *Пусть подмножества I_i и I_j слов из C^n являются инвертируемыми по i-му и j-му разрядам соответственно и такими, что $I_i \cap I_j = \varnothing$. Тогда множество*

$$\bar{I}_i \cup \bar{I}_j \cup (C^n \setminus (I_i \cup I_j))$$

является совершенным $(n,3)$-кодом.

Пусть $\mathbf{u} = (u_1, \ldots, u_{i-1}, u_i, u_{i+1}, \ldots, u_n) \in E^n$, где символ $\oplus$ обозначает сложение по mod 2. Тогда положим

$$|\mathbf{u}| = u_1 \oplus \ldots \oplus u_n, \quad \lfloor \mathbf{u} \rfloor_i = (u_1, \ldots, u_{i-1}, u_{i+1}, \ldots, u_n).$$

Через $STS(\mathscr{H}^n)$ обозначим систему троек Штейнера, образованную словами веса 3 линейного кода Хэмминга $\mathscr{H}^n$.

При любых i и j, $1 \leqslant i \leqslant n+1$, $1 \leqslant j \leqslant n+1$, для пары (i,j) определим подмножества $A^n_{i,j}$, $B^n_{i,j}$ из $\mathscr{H}^n$.

При $i < n+1$, $j < n+1$ и $i \neq j$ положим

$$A^n_{i,j} = \{\mathbf{v} \mid \mathbf{v} \in \mathscr{H}^n,\ |\lfloor \mathbf{v} \rfloor_k| = 0\},$$
$$B^n_{i,j} = \{\mathbf{v} \mid \mathbf{v} \in \mathscr{H}^n,\ |\lfloor \mathbf{v} \rfloor_k| = 1\},$$

где k определяется из условия, что $\{i,j,k\} \in STS(\mathscr{H}^n)$.

При $i = n+1$ и $j < n+1$ положим

$$A^n_{i,j} = \{\mathbf{v} \mid \mathbf{v} \in \mathscr{H}^n,\ |\lfloor \mathbf{v} \rfloor_j| = 0\},$$
$$B^n_{i,j} = \{\mathbf{v} \mid \mathbf{v} \in \mathscr{H}^n,\ |\lfloor \mathbf{v} \rfloor_j| = 1\}.$$

При $i < n+1$ и $j = n+1$ положим

$$A^n_{i,j} = \{\mathbf{v} \mid \mathbf{v} \in \mathscr{H}^n,\ |\lfloor \mathbf{v} \rfloor_i| = 0\},$$
$$B^n_{i,j} = \{\mathbf{v} \mid \mathbf{v} \in \mathscr{H}^n,\ |\lfloor \mathbf{v} \rfloor_i| = 1\}.$$

При $i = j$ в качестве $A^n_{i,j}$ и $B^n_{i,j}$ берутся произвольные подмножества из $\mathscr{H}^n$, образующие его разбиение.

Пусть $\mathscr{H}^{2n+1}$ — линейный код Хэмминга длины $2n+1$, который строится индуктивно по известной схеме [5]

$$\mathscr{H}^{2n+1} = \{(\mathbf{u}, |\mathbf{u}|, \mathbf{u} \oplus \mathbf{v}) \mid \mathbf{u} \in E^n, \mathbf{v} \in \mathscr{H}^n\}.$$

Через R_i обозначим инвертируемое по i-му разряду подмножество кода $\mathscr{H}^{2n+1}$, порожденное нулевым кодовым словом.

Поскольку $\mathscr{H}^{2n+1}$ содержит слова вида $(0, \mathbf{v})$, то подмножество $R_i \oplus (0, \mathbf{v})$ обозначим через $R_{i,\mathbf{v}}$.

Утверждение 2. *При любых i и j таких, что $1 \leqslant i \leqslant n+1$, $1 \leqslant j \leqslant n+1$, и любых $\mathbf{v} \in A^n_{i,j}$, $\mathbf{w} \in B^n_{i,j}$ справедливо соотношение*

$$R_{i,\mathbf{v}} \cap R_{j,\mathbf{w}} = \varnothing.$$

Пусть код $\mathscr{J}^7$ является ортогональным к коду $\mathscr{H}^7$. Рассмотрим кодовые слова из $\mathscr{H}^{15}$ вида $(\mathbf{0}, \mathbf{a}_i)$, где $\mathbf{0}$ — нулевое слово длины 8, $\mathbf{a}_i \in \mathscr{J}^7$. Нетрудно заметить, что для каждого слова $(\mathbf{0}, \mathbf{a}_i)$ можно указать разряд такой, что каждая пара слов вида $(\mathbf{0}, \mathbf{a}_i)$ с соответствующими разрядами будет удовлетворять условиям утверждения 2. Например, разряды могут быть выбраны следующим образом:

(000000001010101)-1-й разряд, (000000001100110)-2-й,
(000000001001011)-3-й, (000000000000000)-4-й,
(000000001111000)-5-й, (000000000101101)-6-й,
(000000000110011)-7-й, (000000000011110)-8-й.

Следовательно, в силу утверждения 2 инвертируемые подмножества, порождаемые словами $(\mathbf{0}, \mathbf{a}_i)$, попарно не пересекаются. Далее будем считать, что слову $(\mathbf{0}, \mathbf{a}_i)$ соответствует разряд с номером i. Через I_i обозначим инвертируемое по i-му разряду подмножество кода $\mathscr{H}^{15}$, порождаемое словом $(\mathbf{0}, \mathbf{a}_i)$.

В силу утверждения 1 справедлива следующая

Теорема 1. *Множества*

$$\mathscr{M}_1 = \bar{I}_1 \cup \bar{I}_2 \cup \bar{I}_3 \cup \bar{I}_4 \cup \bar{I}_5 \cup \bar{I}_6 \cup \bar{I}_7 \\ \cup (\mathscr{H}^{15} \setminus (I_1 \cup I_2 \cup I_3 \cup I_4 \cup I_5 \cup I_6 \cup I_7)),$$

$$\mathscr{M}_2 = \bar{I}_1 \cup \bar{I}_2 \cup \bar{I}_3 \cup \bar{I}_4 \cup \bar{I}_5 \cup \bar{I}_6 \cup \bar{I}_7 \cup \bar{I}_8 \\ \cup (\mathscr{H}^{15} \setminus (I_1 \cup I_2 \cup I_3 \cup I_4 \cup I_5 \cup I_6 \cup I_7 \cup I_8))$$

являются совершенными $(15,3)$-кодами.

Перебор всех вариантов разбиения разрядов на информационные и проверочные (осуществляемый на компьютере) показывает, что коды $\mathscr{M}_1$, $\mathscr{M}_2$ не являются систематическими.

Заметим, что коды $\mathscr{M}_1$, $\mathscr{M}_2$ являются неэквивалентными. При помощи компьютера проверяется, что инверсия символов в $\bar{I}_1$ переводит $\mathscr{M}_1$ в систематический код. С другой стороны, инверсия символов ни в одном из инвертируемых подмножеств кода $\mathscr{M}_2$ не переводит $\mathscr{M}_2$ в систематический код.

Автор выражает благодарность С. А. Малюгину за написание программ проверки кодов на несистематичность и неэквивалентность.

ЛИТЕРАТУРА

1. **Мак-Вильямс Ф., Слоэн Н. Дж.** Теория кодов, исправляющих ошибки. М.: Связь, 1979.
2. **Августинович С. В., Соловьева Ф. И.** О несистематических совершенных двоичных кодах // Проблемы передачи информации. 1996. Т. 32, вып. 3. С. 47–50.
3. **Phelps K. T., Le Van M.** Non-systematic perfect codes // SIAM J. Discrete Mathematics (в печати).
4. **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.
5. **Васильев Ю. Л.** О негрупповых плотно упакованных кодах // Проблемы кибернетики. М.: Физматгиз, 1962. Вып. 8. С. 337–339.

Адрес автора:

Институт математики
им. С. Л. Соболева СО РАН,
пр. Академика Коптюга, 4,
630090 Новосибирск,
Россия

Статья поступила
16 июля 1997 г.