ДИСКРЕТНЫЙ АНАЛИЗ И ИССЛЕДОВАНИЕ ОПЕРАЦИЙ
Январь—март 1997. Том 4, № 1, 46–52

УДК 519.72

О ПОСТРОЕНИИ СОВЕРШЕННЫХ НЕЛИНЕЙНЫХ ДВОИЧНЫХ КОДОВ ИНВЕРСИЕЙ СИМВОЛОВ

А. М. Романов

Предлагается метод построения совершенных нелинейных двоичных кодов с исправлением одной ошибки, который заключается в инвертировании символов в словах кода Хэмминга и обобщает конструкцию Ю. Л. Васильева [1].

В множестве слов совершенного кода выделяются подмножества, которые называются *инвертируемыми*. В результате инверсии символов в некотором разряде в словах из инвертируемого подмножества получается совершенный код, отличный от исходного. В терминах инвертируемых подмножеств конструкцию из [1] можно представить как разбиение множества кодовых слов на попарно непересекающиеся инвертируемые подмножества, в каждом из которых допускаются инверсии символов в одном и том же фиксированном разряде. Ниже предлагается конструкция, в которой множество слов кода Хэмминга $\mathscr{H}^{2n+1}$ длины $2n+1$ разбивается на попарно непересекающиеся инвертируемые подмножества, отличные от подмножеств из [1]. В кодовых словах фиксируются разряды с номерами i и j. Инвертируемые подмножества из $\mathscr{H}^{2n+1}$ разделяются на две совокупности. В словах одной совокупности допускаются инверсии символов в i-м разряде, а в словах другой совокупности — в j-м разряде. Вопрос об эквивалентности предлагаемых кодов и кодов, построенных другими методами в [1, 3–8]), остается открытым.

Все неопределяемые в работе понятия можно найти, например, в [2]. Через E^n обозначается n-мерное векторное пространство над полем $GF(2)$. Векторы в этом пространстве называются *словами*. Далее будем считать, что $n = 2^p - 1$, $p = 2, 3, \ldots$, поскольку лишь при таких n существуют совершенные $(n, 3)$-коды.

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

$\mathscr{C}^n$ 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 d — расстояние Хэмминга, $\bar{c}_i=0$ при $c_i=1$ и $\bar{c}_i=1$ при $c_i=0$.

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

Положим

$$\bar{I}_i=\{(x_1,\ldots,\bar{x}_i,\ldots,x_n)\mid(x_1,\ldots,x_i,\ldots,x_n)\in I_i\}.$$

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

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

является совершенным $(n,3)$-кодом.

Доказательство. Докажем утверждение для первого множества, которое обозначим через $\mathscr{C}_1^n$. Для остальных множеств утверждение доказывается более просто. Мощность множества $\mathscr{C}_1^n$ равна мощности совершенного кода $\mathscr{C}^n$. Покажем, что расстояние между любыми двумя словами из $\mathscr{C}_1^n$ не менее 3. Пусть $\mathbf{c}\in\bar{I}_i$, $\mathbf{c}'\in\bar{I}_j$, $\mathbf{c}''\in(\mathscr{C}^n\backslash(I_i\cup I_j))$. Допустим, что $d(\mathbf{c},\mathbf{c}')=2$. Тогда в силу совершенности кода $\mathscr{C}^n$ найдется $\mathbf{x}\in\mathscr{C}^n$ такое, что $d(\mathbf{x},\mathbf{c})=2$ и $d(\mathbf{x},\mathbf{c}')=2$. Следовательно, $I_i\cap I_j\neq\varnothing$. Противоречие. Таким образом, $d(\mathbf{c},\mathbf{c}')\geqslant 3$. Неравенство $d(\mathbf{c},\mathbf{c}'')\geqslant 3$ (аналогично $d(\mathbf{c}',\mathbf{c}'')\geqslant 3$) справедливо, поскольку в противном случае $\mathbf{c}''\in I_i$. Утверждение доказано.

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

Для любых i и j, $1\leqslant i\leqslant n+1$, $1\leqslant j\leqslant n+1$, положим

$$\pi_{i,j}^{n+1}=\begin{cases}k & \text{при } \{i,j,k\}\in STS(\mathscr{H}^n),\\ i & \text{при } j=n+1,\\ j & \text{при } i=n+1,\\ n+1 & \text{при } i=j.\end{cases}$$

Для любого i, $1\leqslant i\leqslant n+1$, определим перестановку π_i^{n+1} координат в E^{n+1}:

$$\pi_i^{n+1}=(\pi_{i,1}^{n+1},\pi_{i,2}^{n+1},\ldots,\pi_{i,n+1}^{n+1}).$$

Через $\pi_i(\mathbf{u})$ обозначим слово, которое получается из слова $\mathbf{u} = (u_1, u_2, \ldots, u_{n+1}) \in E^{n+1}$ после применения к буквам слова $\mathbf{u}$ перестановки π^{n+1}. Пусть $\mathbf{u} = (u_1, \ldots, u_{i-1}, u_i, u_{i+1}, \ldots, u_{n+1}) \in E^{n+1}$, символ $\oplus$ обозначает сложение по mod 2. Тогда положим

$$|\mathbf{u}| = u_1 \oplus \ldots \oplus u_{n+1}$$

и

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

Через H_l^n обозначим l-й смежный класс кода $\mathscr{H}^n$, $l = 0, 1, \ldots, n$. Положим

$$H_l^{n+1} = \{(\mathbf{v}, |\mathbf{v}|) \mid \mathbf{v} \in H_l^n\}.$$

Лемма 1. *При любых i и l, $1 \leqslant i \leqslant n+1$, $0 \leqslant l \leqslant n$, множество слов H_l^{n+1} инвариантно относительно перестановки π_i^{n+1}, т. е. перестановка π^{n+1} переводит множество в себя.*

Доказательство. Согласно [1] имеем

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

Отсюда следует, что система троек Штейнера $STS(\mathscr{H}^n)$ состоит из троек двух видов:

$$\left\{i, j, \pi_{i,j}^{(n+1)/2} + \frac{n+1}{2}\right\} \text{ при } i \leqslant \frac{n+1}{2}, j \leqslant \frac{n+1}{2}; \tag{2}$$

$$\left\{i + \frac{n+1}{2}, j + \frac{n+1}{2}, k + \frac{n+1}{2}\right\} \text{ при } \{i, j, k\} \in STS(\mathscr{H}^{(n-1)/2}). \tag{3}$$

Далее непосредственно из (2), (3) и определения перестановки π_i^{n+1} следует, что

$$\pi_i^{n+1} = \left(\pi_i^{(n+1)/2} + \frac{n+1}{2}, \pi_i^{(n+1)/2}\right) \text{ при } i \leqslant \frac{n+1}{2}, \tag{4}$$

$$\pi_i^{n+1} = \left(\pi_i^{(n+1)/2}, \pi_i^{(n+1)/2} + \frac{n+1}{2}\right) \text{ при } i > \frac{n+1}{2}, \tag{5}$$

где

$$\pi_i^{(n+1)/2} + \frac{n+1}{2} = \left(\pi_{i,1}^{(n+1)/2} + \frac{n+1}{2}, \ldots, \pi_{i,(n+1)/2}^{(n+1)/2} + \frac{n+1}{2}\right).$$

Из (1) следует, что для любых $l = 0, 1, ..., n$ и $\mathbf{x} \in H_l^{n+1}$ справедливо равенство

$$\mathbf{x} = (\mathbf{v}, \mathbf{w}), \tag{6}$$

где $\mathbf{v} \in H_p^{(n+1)/2}$, $\mathbf{w} \in H_g^{(n+1)/2}$, $0 \leqslant p \leqslant \frac{n+1}{2}, 0 \leqslant q \leqslant \frac{n+1}{2}$. Кроме того, из (1) следует, что

$$\{(\mathbf{v}, \mathbf{w}) \mid \mathbf{v} \in H_p^{(n+1)/2}, \mathbf{w} \in H_q^{(n+1)/2}\} \in H_l^{n+1}. \tag{7}$$

Очевидно, что лемма справедлива при $n = 3$. Предположим, что лемма справедлива при $(n+1)/2$. Тогда из (4)–(7) следует, что лемма справедлива при $n+1$. Лемма 1 доказана.

Для любого i, $1 \leqslant i \leqslant n+1$, определим перестановку σ_i^{2n+1} координат в E^{2n+1}. Положим

$$\sigma_i^{2n+1} = (\pi_i^{n+1}, n+2, \ldots, 2n+1).$$

Лемма 2. *При любом i, $1 \leqslant i \leqslant n+1$, код $\mathscr{H}^{2n+1}$ инвариантен относительно перестановки σ_i^{2n+1}.*

Доказательство. Согласно [1] имеем

$$\mathscr{H}^{2n+1} = \{(\mathbf{u}, |\mathbf{u}|, \mathbf{u} \oplus \mathbf{v}) \mid \mathbf{u} \in E^n, \mathbf{v} \in \mathscr{H}^n\}. \tag{8}$$

По определению перестановка σ_i^{2n+1} переводит слово $(\mathbf{u}', |\mathbf{u}'|, \mathbf{u}' \oplus \mathbf{v}') \in \mathscr{H}^{2n+1}$ в слово $(\pi_i(\mathbf{u}', |\mathbf{u}'|), \mathbf{u}' \oplus \mathbf{v}')$. Поскольку подмножества $H_0^{n+1}, \ldots, H_l^{n+1}$ образуют разбиение множества всех слов из E^{n+1} с четным весом, при некотором $l \in \{1, \ldots, n\}$ справедливо включение

$$(\mathbf{u}', |\mathbf{u}'|) \in H_l^{n+1}, \tag{9}$$

из которого получаем

$$(\mathbf{u}' \oplus \mathbf{v}') \in H_l^n. \tag{10}$$

Из (9) и леммы 1 следует, что

$$\pi_i(\mathbf{u}', |\mathbf{u}'|) \in H_l^{n+1}. \tag{11}$$

Учитывая (8), (10) и (11), имеем

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

Лемма 2 доказана.

Обозначим через E_0^{n+1} множество слов из E^{n+1} с четным весом.

Лемма 3. *Если $1 \leqslant i \leqslant n+1$ и $\mathbf{v} \in \mathscr{H}^n$, то множество*

$$R_i = \{(\mathbf{u}, \lfloor \pi_i(\mathbf{u}) \rfloor_{n+1}) \mid \mathbf{u} \in E_0^{n+1}\}$$

является подмножеством кода $\mathscr{H}^{2n+1}$, инвертируемым по i-му разряду.

Доказательство. Из [1] следует, что множество слов

$$R_{n+1} = \{(\mathbf{u}, \lfloor \mathbf{u} \rfloor_{n+1}) \mid \mathbf{u} \in E_0^{n+1}\}$$

является подмножеством кода $\mathscr{H}^{2n+1}$, инвертируемым по $(n+1)$-му разряду.

В силу леммы 2 код $\mathscr{H}^{2n+1}$ инвариантен относительно перестановки σ_i^{2n+1}, которая переводит $(n+1)$-ю координату в i-ю координату. Следовательно, перестановка σ_i^{2n+1} переводит подмножество R_{n+1} кода $\mathscr{H}^{2n+1}$ в подмножество R_i. А так как подмножество R_{n+1} может быть представлено в виде

$$R_{n+1} = \{(\pi_i(\mathbf{u}), \lfloor \pi_i(\mathbf{u}) \rfloor_{n+1}) \mid \mathbf{u} \in E_0^{n+1}\}$$

и перестановка π_i^{n+1} такова, что $\pi_i(\pi_i(\mathbf{u})) = \mathbf{u}$, то

$$R_i = \{\mathbf{u}, \lfloor \pi_i(\mathbf{u}) \rfloor_{n+1}) \mid \mathbf{u} \in E_0^{n+1}\}.$$

Лемма 3 доказана.

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

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

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

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

При $i = n+1$ и $j < n+1$ положим

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

При $i < n+1$ и $j = n+1$ положим

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

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

Поскольку код $\mathscr{H}^{2n+1}$ представим в виде

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

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

Лемма 4. *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*

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

Доказательство. Рассмотрим только такие пары (i,j), когда $i < n+1$, $j < n+1$, $i \neq j$. (Пары, когда имеет место по крайней мере одно из равенств $i = n+1$, $j = n+1$, рассматриваются аналогично.) Из определения инвертируемого подмножества и леммы 3 следует, что

$$R_{i,\mathbf{v}} = \{(\mathbf{u}, \lfloor \pi_i(\mathbf{u}) \rfloor_{n+1})\} \oplus (\mathbf{0}, \mathbf{v}) = \{(\mathbf{u}, \lfloor \pi_i(\mathbf{u}) \rfloor_{n+1}) \oplus \mathbf{v})\},$$
$$R_{j,\mathbf{w}} = \{(\mathbf{u}, \lfloor \pi_j(\mathbf{u}) \rfloor_{n+1})\} \oplus (\mathbf{0}, \mathbf{w}) = \{(\mathbf{u}, \lfloor \pi_j(\mathbf{u}) \rfloor_{n+1}) \oplus \mathbf{w})\}.$$

Допустим, что $R_{i,\mathbf{v}} \cap R_{i,\mathbf{w}} \neq \varnothing$. Тогда для некоторого $\mathbf{u} \in E^{n+1}$ справедливо равенство

$$\lfloor \pi_i(\mathbf{u}) \rfloor_{n+1} \oplus \mathbf{v} = \lfloor \pi_j(\mathbf{u}) \rfloor_{n+1} \oplus \mathbf{w}.$$

Следовательно,

$$\mathbf{w} = \lfloor \pi_i(\mathbf{u}) \rfloor_{n+1} \oplus \lfloor \pi_j(\mathbf{u}) \rfloor_{n+1} \oplus \mathbf{v}.$$

Поскольку $\mathbf{v} \in A^n_{i,j}$, имеем $|\lfloor \mathbf{v} \rfloor_k| = 0$. По определению перестановок π_i^{n+1} и π_j^{n+1} для всех $\mathbf{u} \in E_0^{n+1}$ справедливо равенство

$$\left| \left\lfloor \lfloor \pi_i(\mathbf{u}) \rfloor_{n+1} \oplus \lfloor \pi_j(\mathbf{u}) \rfloor_{n+1} \right\rfloor_k \right| = 0.$$

Следовательно,

$$|\lfloor \mathbf{w} \rfloor_k| = \left| \left\lfloor \lfloor \pi_i(\mathbf{u}) \rfloor_{n+1} \oplus \lfloor \pi_j(\mathbf{u}) \rfloor_{n+1} \oplus \mathbf{v} \right\rfloor_k \right| = 0.$$

Таким образом, $\mathbf{w} \in A^n_{i,j}$. Получили противоречие. Лемма 4 доказана.

Пусть $\lambda(\mathbf{v})(\mu(\mathbf{w}))$ — произвольная булева функция, определенная на множестве $A^n_{i,j}(B^n_{i,j})$. Положим

$$R_{i,\lambda(\mathbf{v})} = \begin{cases} R_{i,\mathbf{v}} & \text{при } \lambda(\mathbf{v}) = 1, \\ \bar{R}_{i,\mathbf{v}} & \text{при } \lambda(\mathbf{v}) = 0. \end{cases}$$

Аналогичное обозначение $R_{j,\mu(\mathbf{w})}$ введем для функции $\mu(\mathbf{w})$. Положим

$$S^{2n+1} = \Big(\bigcup_{\mathbf{v} \in A^n_{i,j}} R_{i,\lambda(\mathbf{v})} \Big) \cup \Big(\bigcup_{\mathbf{w} \in B^n_{i,j}} R_{j,\mu(\mathbf{w})} \Big).$$

Теорема 1. *Для любых булевых функций λ и μ от n переменных множество S^{2n+1} является совершенным $(2n+1, 3)$-кодом.*

Доказательство. Очевидно, что $R_{i,\lambda(\mathbf{v}_1)} \cap R_{i,\lambda(\mathbf{v}_2)} = \varnothing$ при $\mathbf{v}_1 \neq \mathbf{v}_2$ и $R_{j,\mu(\mathbf{w}_1)} \cap R_{j,\mu(\mathbf{w}_2)} = \varnothing$ при $\mathbf{w}_1 \neq \mathbf{w}_2$. Из леммы 4 следует, что $R_{i,\lambda(\mathbf{v})} \cap R_{j,\mu(\mathbf{w})} = \varnothing$. Следовательно, в силу утверждения 1 множество слов S^{2n+1} является совершенным $(2n+1, 3)$-кодом. Теорема 1 доказана.

ЛИТЕРАТУРА

1. **Васильев Ю. Л.** О негрупповых плотно упакованных кодах // Проблемы кибернетики. М.: Физматгиз, 1962. Вып. 8. С. 337–339.
2. **Мак-Вильямс Ф., Слоэн Р. Дж.** Теория кодов, исправляющих ошибки. М.: Связь, 1979.
3. **Соловьева Ф. И.** О двоичных негрупповых кодах // Методы дискретного анализа в изучении булевых функций и графов: Сб. науч. тр. Новосибирск: Ин-т математики СО АН СССР, 1981. Вып. 37. С. 65–76.
4. **Bauer H., Ganter B., Hergert F.** Algebraic techniques for nonlinear codes // Combinatorica. 1983. V. 3, N 1. P. 21–33.
5. **Heden O.** A new construction of group and nongroup perfect codes // Inform. and Control. 1977. V. 34, N 4. P. 314–323.
6. **Mollard M.** A generalized parity function and its use in the construction of perfect codes // SIAM J. Algebraic Discrete Methods. 1986. V. 7, N 1. P. 113–115.
7. **Phelps K. T.** A combinatorial construction of perfect codes // SIAM J. Algebraic Discrete Methods. 1983. V. 4, N 3. P. 398–403.
8. **Phelps K. T.** A general product constraction for error correcting codes // SIAM J. Algebraic Discrete Methods. 1984. V. 5, N 2. P. 224–228.

Адрес автора:

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

Статья поступила
3 марта 1995 г.,
переработанный вариант —
12 ноября 1996 г.