

УДК 519.72

## О РАЗБИЕНИИ КОДОВ ХЕММИНГА НА НЕПЕРЕСЕКАЮЩИЕСЯ КОМПОНЕНТЫ<sup>\*)</sup>

С. А. Малюгин, А. М. Романов

Получены необходимые и достаточные условия непересекаемости компонент двоичного кода Хемминга. Найдены новые разбиения кодов Хемминга на непересекающиеся компоненты, дающие более общую конструкцию нелинейных кодов.

### Введение

В  $n$ -мерном векторном пространстве  $E^n$  над полем Галуа  $GF(2)$  рассматривается подмножество векторов  $C$ , которое называется *кодом длины  $n$* . Векторы, принадлежащие коду, называются *кодowymi словами*. Расстояние Хемминга  $d(\mathbf{x}, \mathbf{y})$  между векторами  $\mathbf{x} \in E^n$  и  $\mathbf{y} \in E^n$  равно числу координат, в которых векторы  $\mathbf{x}$  и  $\mathbf{y}$  различаются. Наименьшее возможное расстояние  $d$  между двумя кодowymi словами называется *минимальным кодowym расстоянием*. Код  $C$  с минимальным кодowym расстоянием  $d = 2e + 1$  называется *совершенным*, если для любого вектора  $\mathbf{x} \in E^n$  существует единственное кодowoе слово  $\mathbf{c} \in C$  такое, что  $d(\mathbf{x}, \mathbf{c}) \leq e$ .

В статье рассматриваются совершенные двоичные коды с минимальным кодowym расстоянием 3. Известно, что такие коды существуют лишь при  $n = 2^k - 1$ , где  $k = 1, 2, \dots$ . Код называется *линейным*, если его слова образуют линейное подпространство в  $E^n$ . Линейные совершенные коды с минимальным кодowym расстоянием 3 называются *кодами Хемминга*. Существует единственный с точностью до изоморфизма (перестановки координат) код Хемминга длины  $n$ . Известны также нелинейные совершенные коды с параметрами кода Хемминга. Впервые такие коды были предложены в [3]. Имеются и другие способы построения нелинейных совершенных кодов [2, 4, 5, 12, 14–16, 19, 20].

---

<sup>\*)</sup> Исследование первого автора выполнено при финансовой поддержке Российского фонда фундаментальных исследований (проект 99-01-01531) и Федеральной целевой программы «Интеграция» (объединенный проект АО-110).

В [2, 6, 8] получена более общая конструкция, чем в [3], что дало возможность повысить нижнюю оценку числа нелинейных кодов. Но коды, получаемые с помощью конструкций из [2, 6, 8], имеют ранг, не превышающий  $n - \log(n + 1) + 2$  (рангом кода  $C$  называется размерность наименьшего подпространства, содержащего  $C$ ). Поэтому в серию, содержащую большую часть известных в настоящее время нелинейных кодов, не попадают такие интересные коды, как коды полного ранга (ранга, равного  $n$ ) [16], коды с тривиальным ядром [11, 17, 21], коды с тривиальной группой автоморфизмов [13, 18], несистематические коды [1, 10, 22]. В настоящей статье предлагается более общая конструкция, содержащая указанные выше типы нелинейных кодов.

### 1. Обозначения и основные определения

Пусть  $H^n$  — код Хемминга длины  $n$ . Сумму векторов  $\mathbf{u}, \mathbf{v} \in E^n$  будем обозначать через  $\mathbf{u} \oplus \mathbf{v}$ . Базисный вектор, в котором  $i$ -я координата равна единице, обозначаем через  $\mathbf{e}_i$ ,  $i = 1, \dots, n$ . Символом  $\mathbf{0}$  обозначаем нулевой вектор. Множество ненулевых координат вектора  $\mathbf{u} \in E^n$  будем называть *носителем* этого вектора и обозначать через  $[\mathbf{u}]$ . Количество элементов в  $[\mathbf{u}]$  называем *весом* вектора  $\mathbf{u}$ .

Рассмотрим следующее представление кода Хемминга. Каждому номеру  $i = 0, \dots, n$  поставим в соответствие вектор  $(i_1, \dots, i_k) \in E^k$  ( $k = \log(n + 1)$ ), представляющий число  $i$  в двоичной системе счисления. Рассмотрим множество  $H^n$ , состоящее из всех векторов  $\mathbf{u} \in E^n$  таких, что  $\bigoplus \{i \mid i \in [\mathbf{u}]\} = 0$ . Известно, что  $H^n$  является кодом Хемминга. Пространство  $E^k \setminus \{\mathbf{0}\} = \{1, \dots, n\}$  можно рассматривать как конечную  $(k - 1)$ -мерную проективную геометрию  $PG_{k-1}(2)$ .

В коде  $H^n$  рассмотрим вектор  $\mathbf{h}$  такой, что носитель  $[\mathbf{h}]$  есть  $(k - 2)$ -мерная плоскость в  $PG_{k-1}(2)$ . Поэтому  $[\mathbf{h}]$  состоит из  $m = (n - 1)/2$  элементов и все такие множества образуют одну орбиту  $O_m^1$  длины  $n$  относительно группы перестановочных автоморфизмов кода  $H^n$ . Обозначим через  $H^m(\mathbf{h})$  множество всех векторов  $\mathbf{u} \in H^n$  таких, что  $[\mathbf{u}] \subseteq [\mathbf{h}]$ . Очевидно, что  $H^m(\mathbf{h})$  образует в  $H^n$  подкод Хемминга предыдущей размерности (в том смысле, что если во всех векторах из  $H^m(\mathbf{h})$  удалить координаты с номерами, не принадлежащими  $[\mathbf{h}]$ , то полученное множество векторов образует код Хемминга в пространстве размерности  $m = (n - 1)/2$ ).

В коде Хемминга  $H^n$  рассмотрим такое подпространство  $R_i$ , порожденное всеми векторами  $\mathbf{u}$  веса 3, что  $i \in [\mathbf{u}]$ . Всевозможные смежные классы вида  $R_i^{\mathbf{u}} = R_i \oplus \mathbf{u}$  ( $\mathbf{u} \in H^n$ ) представляют собой совокупность всех  $i$ -компонент кода Хемминга  $H^n$ ,  $i = 1, \dots, n$ .

Если  $S_1, \dots, S_m$  — попарно непересекающиеся подмножества кода  $C$  такие, что  $S_p$  является  $i_p$ -компонентой кода  $C$  при каждом  $p = 1, \dots, m$ , то множество

$$C' = \left( C \setminus \bigcup_{p=1}^m S_p \right) \cup \left( \bigcup_{p=1}^m (S_p \oplus \mathbf{e}_{i_p}) \right)$$

является совершенным кодом (см. [21]).

## 2. Условия непересекаемости компонент кода $H^n$

Пусть  $i \notin [\mathbf{h}]$ . Единственный вектор  $\mathbf{v} \in R_i \cap H^m(\mathbf{h})$  будем называть  $H^m(\mathbf{h})$ -представителем компоненты  $R_i$ . Это означает, что  $R_i \cap H^m(\mathbf{h}) = \{\mathbf{v}\}$ . Нашу основную задачу теперь можно переформулировать следующим образом. Какие координаты  $i_q \notin [\mathbf{h}]$  следует поставить в соответствие векторам  $\mathbf{u}_q \in H^m(\mathbf{h})$ , чтобы все компоненты  $R_{i_q}^{\mathbf{u}_q}$  ( $q = 1, \dots, p$ ) были попарно непересекающимися? Для решения этой задачи важно иметь критерий непересекаемости компонент в терминах координат  $i_q$  и  $H^m(\mathbf{h})$ -представителей  $\mathbf{u}_q$ .

**Лемма 1.** Для любых  $i, j \notin [\mathbf{h}]$  и  $\mathbf{u}, \mathbf{v} \in H^m(\mathbf{h})$  компоненты  $R_i^{\mathbf{u}}$  и  $R_j^{\mathbf{v}}$  не пересекаются тогда и только тогда, когда  $\mathbf{u} \oplus \mathbf{v} \notin R_k \cap H^m(\mathbf{h})$ , где  $k = i \oplus j$ .

**Доказательство.** Так как  $k = i \oplus j$ , то  $R_k \subset R_i \oplus R_j$  (см. [2]). Следовательно,  $R_k \cap H^m(\mathbf{h}) \subseteq (R_i \oplus R_j) \cap H^m(\mathbf{h})$ . Множество  $R_k \cap H^m(\mathbf{h})$  является  $k$ -компонентой в коде  $H^m(\mathbf{h})$ , которую обозначим через  $R_k(\mathbf{h})$ . Для любого  $\mathbf{v} \in H^m(\mathbf{h})$  множество  $R_i^{\mathbf{v}} \cap H^m(\mathbf{h})$  одноэлементное. Поэтому

$$R_i \oplus R_k(\mathbf{h}) = \cup \{R_i \oplus \mathbf{v} : \mathbf{v} \in R_k(\mathbf{h})\} \subseteq R_i \oplus R_k = R_i \oplus R_j$$

По формулам из [2] получаем равенство мощностей  $|R_i \oplus R_j| = |R_i| \times |R_k(\mathbf{h})| = 2^{\frac{3n-5}{4}}$ . Следовательно,  $(R_i \oplus R_j) \cap H^m(\mathbf{h}) = R_k(\mathbf{h})$ . Осталось только заметить, что компоненты  $R_i^{\mathbf{u}}$  и  $R_j^{\mathbf{v}}$  не пересекаются тогда и только тогда, когда  $\mathbf{u} \oplus \mathbf{v} \notin R_i \oplus R_j$ . Лемма 1 доказана.

Для  $n = 15$  критерий упрощается и в точности показывает, что условие непересекаемости Романова [9], которое является достаточным для всех  $n \geq 15$ , в этом случае является и необходимым. Теперь элемент  $\mathbf{h}$  следует брать из орбиты  $O_7^1$  кода  $H^{15}$ .

**Лемма 2.** Пусть  $\mathbf{u}, \mathbf{v} \in H^7(\mathbf{h})$  и  $i, j \notin [\mathbf{h}]$  ( $i \neq j$ ). Компоненты  $R_i^{\mathbf{u}}$  и  $R_j^{\mathbf{v}}$  имеют пустое пересечение тогда и только тогда, когда множество  $[\mathbf{u} \oplus \mathbf{v}] \setminus \{k\}$  содержит нечетное число элементов, где  $k = i \oplus j$ .

**Доказательство.** Достаточность условия непересекаемости компонент доказана в [9, лемма 4]. Поэтому проверим только необходимость этого условия.

Допустим, что множество  $[\mathbf{u} \oplus \mathbf{v}] \setminus \{k\}$  состоит из четного числа элементов. Тогда это множество является либо кодовой тройкой (т. е. носителем кодового слова веса 3), содержащей  $k$ , либо кодовой четверкой, не содержащей  $k$ , либо кодовой семеркой  $[\mathbf{h}]$ . Такой набор вместе с нулем представляет, очевидно,  $k$ -компоненту  $R_k(\mathbf{h})$  кода  $H^7(\mathbf{h})$ . В силу леммы 1 пересечение компонент  $R_i^{\mathbf{u}}$  и  $R_j^{\mathbf{v}}$  не пусто. Лемма 2 доказана.

### 3. Разбиения кодов Хемминга на непересекающиеся компоненты

Построим некоторые разбиения кода Хемминга  $H^n$  длины  $n = 2^k - 1$  ( $k \geq 5$ ) на непересекающиеся компоненты.

Пусть  $\mathbf{u} \in H^n$ ,  $i, j \in \{1, \dots, n\}$ ,  $i \neq j$ ,  $k = i \oplus j$ . Следуя [2], множество  $R_{i,j,k}^{\mathbf{u}} = R_i \oplus R_j \oplus \mathbf{u}$  будем называть  $(i, j, k)$ -компонентой. Известно, что это множество не зависит от перестановки индексов  $i$ ,  $j$  и  $k$ .

**Лемма 3.** Пусть вектор  $\mathbf{h} \in H^n$  принадлежит орбите  $O_m^1$  ( $m = (n-1)/2$ ), и пусть  $H^m(\mathbf{h})$  является подкодом кода  $H^n$  размерности  $m$ . Если в  $H^m(\mathbf{h})$  имеется система попарно непересекающихся компонент  $R_{i_q}^{\mathbf{u}_q}(\mathbf{h})$ ,  $\mathbf{u}_q \in H^m(\mathbf{h})$ ,  $i_q \in [\mathbf{h}]$ ,  $q = 1, \dots, p$ , то при фиксированной координате  $t \notin [\mathbf{h}]$  компоненты  $R_{i_q, j_q, t}^{\mathbf{u}_q}$ , где  $j_q = i_q \oplus t$ ,  $q = 1, \dots, p$ , тоже попарно не пересекаются.

ДОКАЗАТЕЛЬСТВО. Из доказательства леммы 1 имеем

$$R_{i_q, j_q, t}^{\mathbf{u}_q} = R_t \oplus R_{i_q}^{\mathbf{u}_q} = \cup \left\{ R_t \oplus \mathbf{v} : \mathbf{v} \in R_{i_q}^{\mathbf{u}_q}(\mathbf{h}) \right\}.$$

Отсюда непосредственно следует, что при различных  $q$  эти множества не пересекаются. Лемма 3 доказана.

Из леммы 3 следует, что, разбивая каждую из непересекающихся компонент  $R_{i_q, j_q, t}^{\mathbf{u}_q}$  либо на  $i_q$ -компоненты, либо на  $j_q$ -компоненты, либо на  $t$ -компоненты, мы получим в коде  $H^n$  новую систему попарно непересекающихся компонент по координатам  $i_q$ ,  $j_q$ ,  $t$  ( $q = 1, \dots, p$ ).

Назовем  $i$ -компоненту  $R_i^{\mathbf{u}}$  кода  $H^n$  *антиподальной*  $i$ -компоненте  $R_i^{\mathbf{v}}$ , если существует вектор  $\mathbf{w} \in R_i^{\mathbf{u} \oplus \mathbf{v}} \cap O_m^1$  такой, что  $i \notin [\mathbf{w}]$ . В [7] доказано, что если при  $i \neq j$  компоненты  $R_i^{\mathbf{u}}$  и  $R_j^{\mathbf{w}}$  кода  $H^n$  не пересекаются и компонента  $R_i^{\mathbf{v}}$  антиподальна к  $R_i^{\mathbf{u}}$ , то компоненты  $R_i^{\mathbf{v}}$  и  $R_j^{\mathbf{w}}$  тоже не пересекаются ([7, лемма 8]).

Добавляя при необходимости антиподальные компоненты к первоначальной системе непересекающихся компонент  $R_{i_q}^{\mathbf{u}_q}(\mathbf{h})$ , можно добиться, чтобы в новой системе компонент кода  $H^n$  присутствовали как  $i_q$ -компоненты, так и  $j_q$ -компоненты. Следовательно, в системе компонент кода  $H^n$  будет задействовано одновременно по крайней мере  $2p$

координат. Если же в исходной системе компонент кода  $H^m(\mathbf{h})$  для некоторого  $i = i_q$  существуют по крайней мере две неантисимметричные различные  $i$ -компоненты, то в коде  $H^n$  построим систему непересекающихся компонент, в которой задействованы все  $2p + 1$  координат  $i_q, j_q, t$  ( $q = 1, \dots, p$ ). Из этой же леммы и так называемых  $(8 \times 2)$ -разбиений,  $(4 \times 4)$ -разбиений,  $(2 \times 8)$ -разбиений кода  $H^{15}$  [7, 9, 10] легко получить серию разбиений кода  $H^n$  на компоненты для любого  $n = 2^k - 1$  ( $k \geq 5$ ).

**Теорема.** Для любого  $n = 2^k - 1$  ( $k \geq 4$ ) и любого  $l$  такого, что  $1 \leq l < k = \log(n + 1)$ , существует разбиение кода Хемминга  $H^n$  на  $i$ -компоненты ( $1 \leq i \leq 2^l$ ), в котором при каждом  $i$ ,  $1 \leq i \leq 2^l$ , имеется  $2^{\frac{n+1}{2} - k - l}$   $i$ -компонент.

**Доказательство.** Рассмотрим только случай  $l = k - 1$ . Доказывать будем индукцией по  $k$ . Для  $k = 4$  в качестве базы индукции рассмотрим любое  $(8 \times 2)$ -разбиение кода  $H^{15}$ . Пусть теперь дано любое  $k \geq 5$  и имеется разбиение кода  $H^m$  ( $m = (n - 1)/2$ ,  $n = 2^k - 1$ ) на компоненты по координатам  $p + 1, \dots, m$  ( $p = (m - 1)/2$ ). В коде  $H^n$  рассмотрим подкод  $H^m(\mathbf{h})$ , где  $[\mathbf{h}] = \{1, \dots, p\} \cup \{m + 1, \dots, m + p\}$ . Будем считать, что этот подкод разбит на компоненты  $R_{i_q}^{u_q}(\mathbf{h})$ , где  $i_q$  принимают значения из множества  $\{m + 1, \dots, m + p\}$ . Полагаем  $t = p + 1$ . Теперь для каждого  $i_q$  одну половину компонент  $R_{i_q, j_q, t}^{u_q}$  разбиваем на  $i_q$ -компоненты, а другую половину — на  $j_q$ -компоненты кода  $H^n$  ( $j_q = i_q \oplus t$ ). Получаем требуемое разбиение, так как  $j_q$  пробегает множество координат  $\{m + p + 1, \dots, n\}$ . Теорема доказана.

## ЛИТЕРАТУРА

1. **Августинович С. В., Соловьева Ф. И.** О несистематических совершенных двоичных кодах // Проблемы передачи информации. 1996. Т. 32, вып. 3. С. 47–50.
2. **Августинович С. В., Соловьева Ф. И.** Построение совершенных двоичных кодов последовательными сдвигами  $\tilde{\alpha}$ -компонент // Проблемы передачи информации. 1997. Т. 33, вып. 3. С. 15–21.
3. **Васильев Ю. Л.** О негрупповых плотно упакованных кодах // Проблемы кибернетики. М.: Физматгиз, 1962. Вып. 8. С. 75–78.
4. **Зиновьев В. А.** Коды для корреляционной многоадресной селекции: Дис. ... канд. техн. наук. М., 1970.
5. **Зиновьев В. А., Лобстейн А. С.** Об обобщенных каскадных конструкциях совершенных двоичных нелинейных кодов // Проблемы передачи информации. 2000. Т. 36, вып. 4. С. 59–73.

6. **Кротов Д. С.** Нижние оценки числа  $m$ -квазигрупп порядка 4 и числа совершенных двоичных кодов // Дискрет. анализ и исслед. операций. Сер. 1. 2000. Т. 7, № 2. С. 47–53.
7. **Малюгин С. А.** О перечислении совершенных двоичных кодов длины 15 // Дискрет. анализ и исслед. операций. Сер. 2. 1999. Т. 6, № 2. С. 48–73.
8. **Малюгин С. А.** О нижней оценке числа совершенных двоичных кодов // Дискрет. анализ и исслед. операций. Сер. 1. 1999. Т. 6, № 4. С. 44–48.
9. **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.
10. **Романов А. М.** О несистематических совершенных кодах длины 15 // Дискрет. анализ и исслед. операций. Сер. 1. 1997. Т. 4, № 4. С. 75–78.
11. **Романов А. М.** Совершенные двоичные коды с тривиальным ядром // Дискрет. анализ и исслед. операций. Сер. 1. 2000. Т. 7, № 2. С. 71–74.
12. **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.
13. **Avgustinovich S. V., Solov'eva F. I.** Perfect binary codes with trivial automorphism group // Proc. of IEEE Intern. Workshop on Inform. Theory. Killarney, Ireland, June 1998. P. 114–115.
14. **Cohen G. D., Honkala I., Litsyn S., Lobstein A.** Covering codes. Amsterdam: North-Holland Publ. Co., 1997.
15. **Etzion T., Vardy A.** Perfect binary codes: Constructions, properties and enumeration // IEEE Trans. Inform. Theory. 1994. V. 40, N 3. P. 754–763.
16. **Heden O.** A new construction of group and nongroup perfect codes // Inform. and Control. 1977. V. 34, N 4. P. 314–323.
17. **Heden O.** A binary perfect code of length 15 and codimension 0 // Designs, Codes and Cryptogr. 1994. V. 4, N 3. P. 213–220.
18. **Malyugin S. A.** Perfect codes with trivial automorphism group // Proc. Second Intern. Workshop on Optimal Codes and Related Topics. Sozopol, Bulgaria, June 1998. P. 163–167.
19. **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.
20. **Phelps K. T.** A general product construction for error correcting codes // SIAM J. Algebraic Discrete Methods. 1984. V. 5, N 2. P. 224–228.
21. **Phelps K. T., LeVan M. J.** Kernels of nonlinear Hamming codes // Designs, Codes and Cryptogr. 1995. V. 6, N 3. P. 247–257.

- 22. Phelps K. T., LeVan M. J.** Non-sistematic perfect codes // SIAM J. Discrete Math. 1999. V. 12, N 1. P. 27–34.
- 23. Phelps K. T., LeVan M. J.** Switching equivalence classes of perfect codes // Designs, Codes and Cryptogr. 1999. V. 16, N 2. P. 179–184.

Адрес авторов:

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

Статья поступила  
26 сентября 2001 г.