

УДК 519.72

О РАЗБИЕНИЯХ q -ИЧНЫХ КОДОВ ХЕММИНГА НА НЕПЕРЕСЕКАЮЩИЕСЯ КОМПОНЕНТЫ

А. М. Романов

Найдены необходимые и достаточные условия непересекаемости компонент q -ичного кода Хемминга. Предложены разбиения q -ичных кодов Хемминга на непересекающиеся компоненты, позволяющие получать нелинейные совершенные q -ичные коды сдвигами компонент. Получена новая нижняя оценка для числа различных совершенных q -ичных кодов.

Введение

Пусть F_q^n — векторное пространство размерности n над полем Галуа $GF(q)$. Произвольное подмножество векторов $C \subseteq F_q^n$ называется q -ичным кодом длины n . Векторы, принадлежащие коду, называются *кодowymi словами*. *Расстоянием Хемминга* $d(\mathbf{x}, \mathbf{y})$ между векторами $\mathbf{x} \in F_q^n$ и $\mathbf{y} \in F_q^n$ называется число координат, в которых векторы \mathbf{x} и \mathbf{y} различаются. Минимально возможное расстояние d между двумя различными кодowymi словами называется *минимальным расстоянием* кода. Код C с минимальным расстоянием $d = 2e + 1$ называется *совершенным*, если для любого вектора $\mathbf{x} \in F_q^n$ существует единственное кодowoе слово $\mathbf{c} \in C$ такое, что $d(\mathbf{x}, \mathbf{c}) \leq e$. Совершенный код с минимальным расстоянием $d = 2e + 1$ является совершенной упаковкой шаров радиусом e в пространстве F_q^n ; при этом центрами шаров являются кодowoе слова. В работе рассматриваются совершенные q -ичные коды с минимальным расстоянием 3. Известно, что такие коды существуют при $n = (q^m - 1)/(q - 1)$, где q — простое число или степень простого числа, $m = 2, 3, \dots$, и каждый код содержит q^{n-m} кодowych слов. Коды $C_1, C_2 \subseteq F_q^n$ называются *изоморфными*, если существует перестановка π такая, что $C_2 = \{\pi(\mathbf{c}) \mid \mathbf{c} \in C_1\}$. Коды C_1 и C_2 называются *эквивалентными*, если существует вектор $\mathbf{x} \in F_q^n$ и перестановка π такие, что $C_2 = \{\pi(\mathbf{c}) + \mathbf{x} \mid \mathbf{c} \in C_1\}$. Рассматриваются и другие более общие определения эквивалентности (см., например [3, 13]). Код называется

линейным, если его слова образуют линейное подпространство в F_q^n . Линейные совершенные коды с минимальным расстоянием 3 называются кодами Хемминга. Известны также нелинейные совершенные q -ичные коды с параметрами кодов Хемминга. Впервые такие коды при $q = 2$ были предложены в работе [2], а при $q \geq 3$ в работах [10, 14]. Имеются и другие способы построения нелинейных совершенных q -ичных кодов при $q \geq 3$ см. [3, 11–13].

Кроме кодов Хемминга и нелинейных совершенных кодов с параметрами кодов Хемминга в F_q^n существуют еще два нетривиальных совершенных кода, которые называют кодами Голея. Двоичный код Голея имеет длину $n = 23$, минимальное расстояние $d = 7$ и содержит 2^{12} кодовых слов. Троиичный код Голея имеет длину $n = 11$, минимальное расстояние $d = 5$ и содержит 3^6 кодовых слов. Известно [15, 16], что других нетривиальных совершенных кодов в F_q^n не существует.

В коде Хемминга рассматриваются подпространства R_i , где i — номер координаты, $i = 1, 2, \dots, n$. Всевозможные смежные классы, образованные подпространством R_i , представляют собой совокупность i -компонент кода Хемминга. Разбиение кода Хемминга на компоненты назовем *регулярным*, если в нем компоненты с одинаковыми координатами встречаются равное число раз. Регулярное разбиение имеет параметры $[k, l]$, если в нем участвуют k различных координат и каждая координата представлена l компонентами. В работе [6] описаны все возможные разбиения на компоненты двоичных кодов Хемминга длины $n = 15$, а именно это разбиения с параметрами $[1, 16]$, $[2, 8]$, $[4, 4]$, $[8, 2]$ и единственная тупиковая упаковка с параметрами $[5, 2]$. Предложенные в настоящей работе разбиения являются обобщением конструкций из [7, 8]. Новые коды получаются из разбиений q -ичных кодов Хемминга сдвигами компонент (см. [8, 9, 13]). Неопределяемые в статье понятия можно найти в [5].

1. Обозначения и основные определения

Пусть H_m — q -ичный код Хемминга длины $n = (q^m - 1)/(q - 1)$, где q — простое число или степень простого числа, $m = 2, 3, \dots$. Сумму векторов $\mathbf{u}, \mathbf{v} \in F_q^n$ обозначим через $\mathbf{u} + \mathbf{v}$. Базисный вектор, в котором i -я координата равна единице, обозначим через \mathbf{e}_i , $i = 1, \dots, n$. Символом $\mathbf{0}$ обозначим нулевой вектор. Проверочная матрица кода H_m состоит из n попарно линейно независимых столбцов $h_i \in F_q^m$, $i = 1, \dots, n$. Совокупность векторов $F_q^m \setminus \{\mathbf{0}\}$ порождает конечную $(m - 1)$ -мерную проективную геометрию $PG_{m-1}(q)$ над полем $GF(q)$. В этой геометрии точкам соответствуют столбцы проверочной матрицы кода H_m и три

точки i, j, k лежат на одной прямой, если соответствующие им столбцы h_i, h_j, h_k являются линейно зависимыми.

Пусть $\mathbf{u} = (u_1, u_2, \dots, u_n) \in F_q^n$. Тогда носителем вектора \mathbf{u} называется множество $S(\mathbf{u}) = \{i \mid u_i \neq 0\}$. Число элементов в $S(\mathbf{u})$ называется весом вектора \mathbf{u} .

В коде H_m рассмотрим вектор \mathbf{x} такой, что его носитель $S(\mathbf{x})$ является $(m-2)$ -мерной гиперплоскостью в $PG_{m-1}(q)$. Обозначим через $H_{\mathbf{x}}$ множество всех векторов $\mathbf{u} \in H_m$ таких, что $S(\mathbf{u}) \subseteq S(\mathbf{x})$. Очевидно, что $H_{\mathbf{x}}$ образует в H_m подкод Хемминга предыдущей размерности.

В q -ичном коде Хемминга H_m рассмотрим подпространство R_i , порожденное всеми векторами веса 3 с ненулевой i -й координатой. Всевозможные смежные классы $R_i + \mathbf{u}$ ($\mathbf{u} \in H_m$) представляют собой совокупность всех i -компонент кода Хемминга H_m , $i = 1, \dots, n$.

Пусть l_1, l_2, \dots, l_t — прямые, проходящие через точку i . Тогда

$$R_i = H_{l_1} + H_{l_2} + \dots + H_{l_t},$$

где H_{l_p} — подкод кода H_m , определяемый прямой l_p , $p = 1, 2, \dots, t = (n-1)/q$. Так как размерность подпространства H_{l_p} равна $q-1$, то размерность R_i равна $(q-1)((n-1)/q) = q^{m-1} - 1$.

Если в коде H_m компоненты $R_{i_1} + \mathbf{u}_1, \dots, R_{i_s} + \mathbf{u}_s$ попарно не пересекаются и $\lambda_p \in GF(q)$, $p = 1, \dots, s$, то множество

$$C = \left(H_m \setminus \bigcup_{p=1}^s R_{i_p} + \mathbf{u}_p \right) \cup \left(\bigcup_{p=1}^s R_{i_p} + \mathbf{u}_p + \lambda_p \mathbf{e}_{i_p} \right)$$

является совершенным q -ичным кодом (см., например [13]).

2. Условия непересекаемости компонент кода Хемминга

В этом разделе будет показано, что при $i \notin S(\mathbf{x})$ в пересечении $(R_i + \mathbf{u}) \cap H_{\mathbf{x}}$ содержится только один вектор. Поскольку число i -компонент равно мощности множества $H_{\mathbf{x}}$, то каждый вектор из $H_{\mathbf{x}}$ является представителем некоторой i -компоненты. Ниже будет сформулирован критерий непересекаемости компонент q -ичного кода Хемминга в терминах $H_{\mathbf{x}}$ -представителей.

Лемма 1. Пусть $i \notin S(\mathbf{x})$ и $\mathbf{u} \in H_m$. Тогда в пересечении $(R_i + \mathbf{u}) \cap H_{\mathbf{x}}$ содержится только один вектор.

Доказательство. Поскольку $i \notin S(\mathbf{x})$, то любая прямая, проходящая

через точку i , пересекается с гиперплоскостью $S(\mathbf{x})$ только в одной точке. Следовательно, $H_{l_p} \cap H_{\mathbf{x}} = \{\mathbf{0}\}$ при любом $p = 1, 2, \dots, t = (n-1)/q$. Минимальный вес подкода H_{l_p} равен 3. Таким образом, $R_i \cap H_{\mathbf{x}} = \{\mathbf{0}\}$ и $|(R_i + \mathbf{u}) \cap H_{\mathbf{x}}| \leq 1$. Размерность кода H_m равна $n - m$, а размерность подпространства R_i ($i = 1, \dots, n$) равна $q^{m-1} - 1$. Следовательно, число смежных классов, образованных подпространством R_i , равно $q^{\frac{n-1}{q}-m+1}$. С другой стороны, размерность подкода $H_{\mathbf{x}}$ равна $((n-1)/q) - m + 1$. Таким образом $|(R_i + \mathbf{u}) \cap H_{\mathbf{x}}| = 1$. Лемма 1 доказана.

Лемма 2. Пусть $i \notin S(\mathbf{x})$ и $k \in S(\mathbf{x})$. Тогда

$$R_i + (R_k \cap H_{\mathbf{x}}) = R_i + R_k.$$

Доказательство. Очевидно, что

$$R_i + (R_k \cap H_{\mathbf{x}}) \subseteq R_i + R_k.$$

В силу леммы 1 справедливо равенство

$$|R_i + (R_k \cap H_{\mathbf{x}})| = |R_i| \cdot |R_k \cap H_{\mathbf{x}}|.$$

Множество $R_k \cap H_{\mathbf{x}}$ является компонентой кода Хемминга предыдущей размерности. Следовательно,

$$|R_i| \cdot |R_k \cap H_{\mathbf{x}}| = q^{q^{m-1} + q^{m-2} - 2}.$$

С другой стороны, в силу предложения 3.3 из [13] имеем

$$|R_i \cap R_k| = q^{(q-1)q^{m-2}}.$$

Следовательно,

$$|R_i + R_k| = q^{q^{m-1} + q^{m-2} - 2}.$$

Таким образом,

$$|R_i + (R_k \cap H_{\mathbf{x}})| = |R_i + R_k|.$$

Лемма 2 доказана.

Лемма 3. Если точка k лежит на прямой, соединяющей точки i и j , то

$$R_k \subset R_i + R_j.$$

Доказательство. Пусть l — прямая, соединяющая точки i и j . Прямая l принадлежит $(n - q - 1)/q^2$ плоскостям. Рассмотрим одну из них.

Пусть прямые l_i, l_j, l_k проходят соответственно через точки i, j, k , отличны от прямой l и лежат в рассматриваемой плоскости. Допустим, что $\{i, a, b\} \subseteq l_i, \{j, a, c\} \subseteq l_j, \{b, c\} \subseteq l_k$. Тогда линейной комбинацией векторов с носителями $\{i, j, k\}, \{i, a, b\}, \{j, a, c\}$ может быть получен вектор с носителем $\{k, b, c\} \subseteq l_k$. Остается только показать, что для каждого $k \in l$ ($k \neq i, k \neq j$) и для каждой прямой, проходящей через точку k , линейной комбинацией векторов с носителями, принадлежащими прямым l, l_i, l_j , может быть получено $q - 1$ линейно независимых векторов веса 3 с ненулевой k -й координатой. На прямых l_i и l_j можно выбрать по $q - 1$ троек $\{i, a, b_1\}, \dots, \{i, a, b_{q-1}\}, \{j, a, c_1\}, \dots, \{j, a, c_{q-1}\}$. Линейной комбинацией векторов с носителями $\{i, a, b_1\}, \dots, \{i, a, b_{q-1}\}, \{j, a, c_1\}, \dots, \{j, a, c_{q-1}\}$ и векторов веса 3 с носителями, содержащими точки i, j , можно получить $(q - 1)^2$ векторов с носителями, содержащими пары $\{b_s, c_t\}, s = 1, \dots, q - 1, t = 1, \dots, q - 1$. Так как через любую точку в плоскости проходит $q + 1$ прямая, то выбирая различные пары прямых, проходящих через точки i, j и отличные от прямой l , получим $q^2(q - 1)^2$ пар точек. Так как в проективной геометрии из существования троек $\{i, a, b\}, \{j, a, c\}$ следует существование троек $\{i, c, d\}, \{j, b, d\}$, то из $q^2(q - 1)^2$ пар точек только $q^2(q - 1)^2/2$ пар являются различными.

С другой стороны, плоскость содержит $q^2 + q + 1$ прямую. Следовательно, число прямых, которые не проходят через точки i или j , равно $q(q - 1)$. На каждой прямой можно выбрать $q(q - 1)/2$ различных пар точек, которые не пересекаются с прямой l . Следовательно, число различных пар, которые содержатся в $q(q - 1)$ прямых, равно $q^2(q - 1)^2/2$. Лемма 3 доказана.

Теорема 1. Для любых $i, j \notin S(\mathbf{x})$ и $\mathbf{u}, \mathbf{v} \in H_{\mathbf{x}}$ компоненты $R_i + \mathbf{u}$ и $R_j + \mathbf{v}$ не пересекаются тогда и только тогда, когда $\mathbf{u} - \mathbf{v} \notin R_k \cap H_{\mathbf{x}}$, где k является точкой пересечения прямой, проходящей через точки i и j , с плоскостью $S(\mathbf{x})$.

Доказательство. Так как $\mathbf{u}, \mathbf{v} \in H_{\mathbf{x}}$, то компоненты $R_i + \mathbf{u}$ и $R_j + \mathbf{v}$ не пересекаются, тогда и только тогда, когда $\mathbf{u} - \mathbf{v} \notin (R_i + R_j) \cap H_{\mathbf{x}}$. Остается показать, что

$$(R_i + R_j) \cap H_{\mathbf{x}} = R_k \cap H_{\mathbf{x}}.$$

В силу леммы 3 имеем

$$R_i + R_j = R_i + R_k.$$

Следовательно,

$$(R_i + R_j) \cap H_{\mathbf{x}} = (R_i + R_k) \cap H_{\mathbf{x}}.$$

В силу леммы 2

$$(R_i + R_k) \cap H_{\mathbf{x}} = (R_i + (R_k \cap H_{\mathbf{x}})) \cap H_{\mathbf{x}},$$

а в силу леммы 1

$$(R_i + (R_k \cap H_{\mathbf{x}})) \cap H_{\mathbf{x}} = R_k \cap H_{\mathbf{x}}.$$

Теорема 1 доказана.

3. Разбиения кодов Хемминга на непересекающиеся компоненты

В этом разделе будут построены некоторые разбиения q -ичного кода Хемминга H_m длины $n = (q^m - 1)/(q - 1)$ ($m \geq 3$) на непересекающиеся компоненты.

Лемма 4. Пусть $k_1, \dots, k_s \in S(\mathbf{x})$ и $\mathbf{u}_1, \dots, \mathbf{u}_s \in H_{\mathbf{x}}$. Если множества $(R_{k_1} \cap H_{\mathbf{x}}) + \mathbf{u}_1, \dots, (R_{k_s} \cap H_{\mathbf{x}}) + \mathbf{u}_s$ попарно не пересекаются, то при фиксированном $i \notin S(\mathbf{x})$ множества $R_i + R_{k_1} + \mathbf{u}_1, \dots, R_i + R_{k_s} + \mathbf{u}_s$ попарно не пересекаются.

Доказательство. В силу леммы 1 множества

$$R_i + (R_{k_1} \cap H_{\mathbf{x}}) + \mathbf{u}_1, \dots, R_i + (R_{k_s} \cap H_{\mathbf{x}}) + \mathbf{u}_s$$

попарно не пересекаются. В силу леммы 2 при $p = 1, \dots, s$

$$R_i + (R_{k_p} \cap H_{\mathbf{x}}) + \mathbf{u}_p = R_i + R_{k_p} + \mathbf{u}_p.$$

Следовательно, множества $R_i + R_{k_1} + \mathbf{u}_1, \dots, R_i + R_{k_s} + \mathbf{u}_s$ тоже попарно не пересекаются. Лемма 4 доказана.

Теорема 2. Для любых $m \geq 3$ и p , $0 \leq p \leq m - 3$, существует регулярное разбиение q -ичного кода Хемминга H_m на компоненты с параметрами $[q^p, q^{\frac{p-1}{q}-m-p+1}]$.

Доказательство. Воспользуемся индукцией по m . При $m = 3$ код H_3 разбивается на смежные классы по подпространству R_i . Пусть теперь имеется разбиение кода H_{m-1} на i_s -компоненты, где $1 \leq s \leq q^p$. В коде H_m рассмотрим подкод $H_{\mathbf{x}}$, который соответствует коду H_{m-1} . В силу леммы 4 из разбиения кода $H_{\mathbf{x}}$ на компоненты следует разбиение кода H_m на множества $R_i + R_{i_s}$, где $i \notin S(\mathbf{x})$. Так как в проективной геометрии $PG_{m-1}(q)$ прямая содержит $q + 1$ точку, то в силу леммы 3 для каждого $r = 1, \dots, q$ существует разбиение множества $R_i + R_{i_s}$ на компоненты $R_{t_r} + \mathbf{u}$, где точка t_r лежит на прямой, соединяющей точки i и i_s ,

и $t_r \notin S(\mathbf{x})$. Совокупность подмножеств $R_i + R_{i_s}$ разобьем на q частей. Подмножества $R_i + R_{i_s}$ из r -й части разобьем на компоненты $R_{t_r} + \mathbf{u}$. Теорема 2 доказана.

Из лемм 3 и 4 следует, что из любого разбиения кода H_{m-1} можно построить некоторое разбиения для кода H_m .

Пусть $F_q(n)$ — число различных совершенных q -ичных кодов длины n . Тогда с учетом леммы 3 нижняя оценка, полученная в [4], приобретает вид

$$F_q(n) > q^{q^{(q^{m-2}-1)\frac{q}{q-1}-(m-2)}} (q^2 + q)^{q^{\frac{q^{m-2}-1}{q-1}-(m-2)}}.$$

Эта оценка является обобщением оценки из [1].

ЛИТЕРАТУРА

1. **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.
2. **Васильев Ю. Л.** О негрупповых плотно упакованных кодах // Проблемы кибернетики. Вып. 8. М.: Физматгиз, 1962. С. 75–78.
3. **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.
4. **Лось А. В.** Построение совершенных q -значных кодов последовательными сдвигами $\tilde{\alpha}$ -компонент // Проблемы передачи информации. 2004. Т. 40, вып. 1. С. 40–47.
5. **Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А.** Теория кодов, исправляющих ошибки. М.: Связь, 1979.
6. **Малюгин С. А.** О перечислении совершенных двоичных кодов длины 15 // Дискрет. анализ и исслед. операций. Сер. 2. 1999. Т. 6, № 2. С. 48–73.
7. **Малюгин С. А., Романов А. М.** О разбиениях кодов Хемминга на непересекающиеся компоненты // Дискрет. анализ и исслед. операций. Сер. 1. 2002. Т. 9, № 1. С. 42–48.
8. **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.
9. **Etzion T., Vardy A.** Perfect binary codes: Constructions, properties and enumeration // IEEE Trans. on Inform. Theory. 1994. V. 40, N 3. P. 754–763.

10. **Linström B.** On group and nongroup perfect codes in q symbols // Math. Scand. 1969. V. 25. P. 149–158.
11. **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.
12. **Phelps K. T.** A product construction for perfect codes over arbitrary alphabets // IEEE Trans. on Inform. Theory. 1984. V. 30, N 5. P. 769–771.
13. **Phelps K. T., Villanueva M.** Ranks of q -ary 1-perfect codes // Designs, Codes and Cryptogr. 2002. V. 27, N 1/2. P. 139–144.
14. **Schönheim J.** On linear and nonlinear single-error-correcting q -nary perfect codes // Inform. and Control. 1968. V. 12, N 1. P. 23–26.
15. **Tietäväinen A.** On the nonexistence of perfect codes over finite fields // SIAM J. Applied Mathematics. 1973. V. 24, N 1. P. 88–96.
16. **Zinoviev V. A., Leontiev V. K.** The nonexistence of perfect codes over Galois field // Probl. Control and Inform. Theory 1973. V. 2, N 2. P. 16–24.

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

Статья поступила
8 апреля 2004 г.