ДИСКРЕТНЫЙ АНАЛИЗ И ИССЛЕДОВАНИЕ ОПЕРАЦИЙ
Март—апрель 2012. Том 19, № 2. С. 84–91

УДК 519.176

О ДОПУСТИМЫХ СЕМЕЙСТВАХ КОМПОНЕНТ КОДОВ ХЭММИНГА [*)]

А. М. Романов

Аннотация. Описаны свойства i-компонент кодов Хэмминга и предложены конструкции их допустимых семейств. Показано, что каждый q-ичный код длины m с расстоянием 5 (при $q = 3$ с расстоянием 3) может быть вложен в некоторый q-ичный 1-совершенный код длины $n = (q^m - 1)/(q - 1)$. Показано также, что каждый двоичный код длины $m + k$ с расстоянием $3k + 3$ может быть вложен в некоторый двоичный 1-совершенный код длины $n = 2^m - 1$.

Ключевые слова: код Хэмминга, 1-совершенный код, q-ичный код, двоичный код, i-компонента.

Введение

Пусть $\mathbb{F}_q^n$ — векторное пространство размерности n над полем Галуа $\mathbb{F}_q$. Обозначим через $d(\vec{x}, \vec{y})$ расстояние Хэмминга между векторами $\vec{x}$ и $\vec{y}$. Произвольное подмножество C векторов из пространства $\mathbb{F}_q^n$ называется *q-ичным 1-совершенным кодом* длины n, если для каждого вектора $\vec{x} \in \mathbb{F}_q^n$ существует единственный вектор $\vec{c}$ из множества C такой, что $d(\vec{x}, \vec{c}) \leqslant 1$. Известно, что q-ичные 1-совершенные коды существуют только при $n = (q^m - 1)/(q - 1)$, где $m \geqslant 2$ — натуральное число. Будем предполагать, что нулевой вектор $\vec{0}$ принадлежит коду. Код называется *линейным*, если он образует линейное подпространство в пространстве $\mathbb{F}_q^n$. Линейные 1-совершенные коды называются *кодами Хэмминга*. Через $\mathbb{H}$ будем обозначать q-ичный код Хэмминга длины n. *Весом* вектора $\vec{x} \in \mathbb{F}_q^n$ называется число $d(\vec{x}, \vec{0})$. Вектор веса 3, принадлежащий коду $\mathbb{H}$, называется *тройкой*. Рассмотрим подпространство R_i, порождённое множеством всех троек кода $\mathbb{H}$ с единичной i-й координатой. Всевозможные смежные классы $R_i + \vec{u}$ представляют собой совокупность всех *i-компонент* кода Хэмминга $\mathbb{H}$, где $i \in \{1, 2 \ldots n\}$, $\vec{u} \in \mathbb{H}$.

[*)] Исследование выполнено при финансовой поддержке Российского фонда фундаментальных исследований (проект 11–01–00997).

Семейство компонент $R_{i_1}+\vec{u}_1, R_{i_2}+\vec{u}_2, \ldots, R_{i_t}+\vec{u}_t$ кода Хэмминга $\mathbb{H}$ называется *допустимым*, если $(R_{i_r}+\vec{u}_r)\cap(R_{i_s}+\vec{u}_s) = \varnothing$ при $r, s \in \{1, 2, \ldots, t\}$, $r \neq s$ [5].

Пусть $n_1 \leqslant n_2$, $C_1 \subseteq \mathbb{F}_q^{n_1}$ и $C_2 \subseteq \mathbb{F}_q^{n_2}$. Все кодовые векторы из кода C_1 удлиним с помощью нулевого вектора длины $n_2 - n_1$ до длины n_2. Говорят, что код C_1 *вкладывается* в C_2, если все удлинённые векторы из C_1 принадлежат C_2. В C_2 рассмотрим все кодовые векторы, в которых последние $n_2 - n_1$ координат равны нулю. Удалим последние $n_2 - n_1$ координат во всех таких векторах. Если полученное множество укороченных кодовых векторов совпадает с C_1, то говорят, что код C_1 *вкладывается в код C_2 в строгом смысле*. В нашей работе речь идёт о вложении в строгом смысле, за исключением случая двоичных кодов.

А. В. Августинович и Д. С. Кротов [2] показали, что любой двоичный код длины m с минимальным расстоянием 3 вкладывается (в строгом смысле) в некоторый двоичный 1-совершенный код длины $2^m - 1$.

В нашей работе описаны свойства i-компонент кодов Хэмминга и предложены конструкции допустимых семейств компонент кодов Хэмминга. Показано, что каждый q-ичный код длины m с расстоянием 5 (при $q = 3$ с расстоянием 3) может быть вложен в некоторый q-ичный 1-совершенный код длины $n = (q^m - 1)/(q - 1)$. Показано также, что каждый двоичный код длины $m + k$ с расстоянием $3k + 3$ может быть вложен в некоторый двоичный 1-совершенный код длины $n = 2^m - 1$.

Приводятся три примера допустимых семейств компонент кодов Хэмминга. В примере 1 по произвольному q-ичному коду $(\Lambda\cup\{\vec{0}\}) \subset \mathbb{F}_q^m$ с кодовым расстоянием 5 строится допустимое семейство компонент q-ичного кода Хэмминга длины $n = (q^m - 1)/(q - 1)$. Оно построено так, что, сдвигая компоненты из этого семейства, получаем q-ичный 1-совершенный код $\mathbb{T}$ длины n, в который вкладываются q-ичный код $\Lambda \cup \{\vec{0}\}$ длины m. В примере 2 по произвольному троичному коду длины m с расстоянием 3 точно аналогично примеру 1 строится допустимое семейство компонент троичного кода Хэмминга длины $n = (3^m - 1)/2$. В примере 3 по произвольному двоичному коду длины $m + k$ с расстоянием $3k + 3$ строится допустимое семейство компонент двоичного кода Хэмминга длины $n = 2^m - 1$. Допустимые семейства компонент из примеров 2 и 3 обладают такими же свойствами, что и допустимое семейство компонент из примера 1, и позволяют сдвигом компонент строить 1-совершенные коды, в которые вкладываются коды меньшей длины.

В разд. 1 приведены теоремы, описывающие свойства i-компонент кода $\mathbb{H}$. В разд. 2 описаны конструкции допустимых семейств компонент

кода $\mathbb{H}$. В разд. 3 приведены примеры 2 и 3, а в разд. 4 доказывается теорема о вложимости.

Проверочная матрица H кода $\mathbb{H}$ длины $n = (q^m - 1)/(q - 1)$ состоит из n попарно линейно независимых вектор-столбцов $\vec{h}_i$. Транспонированный вектор-столбец $\vec{h}_i$ принадлежит $\mathbb{F}_q^m$, $i \in \{1, \ldots, n\}$. Будем считать, что столбцы проверочной матрицы H упорядочены произвольным, но фиксированным образом. Совокупность векторов $\mathbb{F}_q^m \setminus \{\vec{0}\}$ порождает конечную $(m-1)$-мерную проективную геометрию $PG_{m-1}(q)$ над полем Галуа $\mathbb{F}_q$. В этой геометрии точкам соответствуют столбцы проверочной матрицы H и три точки i, j, k лежат на одной прямой, если соответствующие им столбцы $\vec{h}_i, \vec{h}_j, \vec{h}_k$ линейно зависимы. Прямую, проходящую через точки x и y, обозначим через l_{xy}. Через P_{xyz} обозначим плоскость, порождённую тремя неколлинеарными точками x, y, z. *Носителем* вектора $\vec{x} = (x_1, x_2, \ldots, x_n) \in \mathbb{F}_q^n$ называется множество $\{i : x_i \neq 0\}$. Тройка принадлежит прямой, если её носитель принадлежит прямой. Тройки пересекаются в точке i, если их носители пересекаются в точке i.

1. Свойства i-компонент

Приведём теоремы, описывающие свойства i-компонент кода $\mathbb{H}$.

Пусть $\mathbb{H}_l$ — подкод кода $\mathbb{H}$, определяемый прямой l. Рассмотрим пучок прямых $l_1, l_2, \ldots, l_{(n-1)/q}$ с центром в точке i. Известно [1], что

$$R_i = \mathbb{H}_{l_1} + \mathbb{H}_{l_2} + \cdots + \mathbb{H}_{l_{(n-1)/q}}. \tag{1}$$

Теорема 1. *Пусть $\vec{u} = (u_1, u_2, \ldots, u_n) \in R_i$ и некоторая компонента u_x вектора $\vec{u}$ отлична от нуля, $x \neq i$. Тогда на прямой l_{ix} существует точка y, отличная от i, x и такая, что компонента u_y вектора $\vec{u}$ отлична от нуля.*

Доказательство. Базис подпространства R_i образуют все линейно независимые тройки кода $\mathbb{H}$ с единичной i-й координатой. Рассмотрим разложение вектора $\vec{u}$ по базису. В этом разложении присутствует тройка, носитель которой содержит точки i, x и ещё некоторую точку, лежащую на прямой l_{ix}. Из (1) следует, что базисные тройки, принадлежащие прямой l_{ix}, образуют подпространство $\mathbb{H}_{l_{ix}}$. Базисный тройки, принадлежащие другим прямым из пучка прямых с центром в точке i, пересекаются с базисными тройками, лежащими на прямой l_{ix}, только в одной точке i. Теорема 1 доказана.

Теорема 2. *Пусть $i \neq j$, $\vec{u} = (u_1, u_2, \ldots, u_n) \in R_i + R_j$, некоторая компонента u_x вектора $\vec{u}$ отлична от нуля и точка x не лежит на прямой l_{ij}. Тогда на плоскости P_{ijx} существует точка y, отличная от точек i, j, x и такая, что компонента u_y вектора $\vec{u}$ отлична от нуля.*

Доказательство. Эта теорема доказывается аналогично предыдущей. Базисные тройки пространства $R_i + R_j$, лежащие на плоскости P_{ijx}, образуют подпространство. Прямые из пучка прямых с центром в точке i либо лежат на плоскости P_{ijx}, либо пересекаются с ней только в одной точке i. Аналогичным свойством обладают и прямые из пучка прямых с центром в точке j. Теорема 2 доказана.

2. Пример 1

Опишем конструкции допустимых семейств компонент кода $\mathbb{H}$.

Пример 1. Выберем m линейно независимых столбцов в проверочной матрице H кода Хэмминга $\mathbb{H}$ длины $n = (q^m - 1)/(q - 1)$. Будем считать, что выбранными являются столбцы $\vec{h}_1, \vec{h}_2, \ldots, \vec{h}_m$. Пусть код $(\Lambda \cup \{\vec{0}\}) \subset \mathbb{F}_q^m$ содержит t ненулевых векторов $\vec{\lambda}_1, \vec{\lambda}_2, \ldots, \vec{\lambda}_t$, вес каждого из которых больше или равен трём. Пусть также расстояние между любыми двумя различными векторами из множества $\Lambda = \{\vec{\lambda}_1, \vec{\lambda}_2, \ldots, \vec{\lambda}_t\}$ больше или равно пяти. Каждому вектору $\vec{\lambda}_s = (\lambda_{s1}, \lambda_{s2}, \ldots, \lambda_{sm})$ длины m сопоставим вектор $\vec{u}_s$ длины n, где $s \in \{1, \ldots, t\}$. Пусть

$$\mu_s \vec{h}_{i_s} = \lambda_{s1}\vec{h}_1 + \lambda_{s2}\vec{h}_2 + \cdots + \lambda_{sm}\vec{h}_m,$$

где $\mu_s \in \mathbb{F}_q$, $i_s \in \{1, 2, \ldots, n\}$. Тогда положим

$$\vec{u}_s = (\lambda_{s1}, \lambda_{s2}, \ldots, \lambda_{sm}, 0, \ldots, 0, -\mu_s, 0, \ldots, 0).$$

Носитель вектора $\vec{u}_s$ принадлежит множеству $\{1, 2, \ldots, m\} \cup \{i_s\}$. Поскольку код Хэмминга $\mathbb{H}$ образует нулевое пространство проверочной матрицы H, то $\vec{u}_s \in \mathbb{H}$.

Таким образом, по векторам длины m из множества Λ построено семейство компонент $R_{i_1} + \vec{u}_1, R_{i_2} + \vec{u}_2, \ldots, R_{i_t} + \vec{u}_t$ q-ичного кода Хэмминга $\mathbb{H}$ длины $n = (q^m - 1)/(q - 1)$.

Эцион и Варди [3] использовали множество линейно независимых столбцов проверочной матрицы кода Хэмминга для построения двоичных 1-совершенных кодов полного ранга.

Покажем, что это семейство компонент допустимо.

Утверждение 1. *Пусть $s \in \{1, 2, \ldots, t\}$. Тогда $\vec{u}_s \notin R_{i_s}$.*

Доказательство. Из конструкции следует, что носитель вектора $\vec{u}_s = (u_1, u_2, \ldots, u_n)$ принадлежит множеству $\{1, 2, \ldots, m\} \cup \{i_s\}$, а столбец $\vec{h}_{i_s}$ является линейной комбинацией трёх или более столбцов из множества $\{\vec{h}_1, \vec{h}_2, \ldots, \vec{h}_m\}$. Поскольку столбцы $\vec{h}_1, \vec{h}_2, \ldots, \vec{h}_m$ линейно независимы, при $x \in \{1, 2, \ldots, m\}$ любая линейная комбинация столбцов $\vec{h}_x$ и $\vec{h}_{i_s}$ не принадлежит множеству $\{\vec{h}_1, \vec{h}_2, \ldots, \vec{h}_m\} \setminus \{\vec{h}_x\}$. Поэтому из теоремы 1 следует, что $\vec{u}_s \notin R_{i_s}$. Утверждение 1 доказано.

Теорема 3. *Семейство компонент* $R_{i_1} + \vec{u}_1, R_{i_2} + \vec{u}_2, \ldots, R_{i_t} + \vec{u}_t$ q*-ичного кода Хэмминга* $\mathbb{H}$ *длины* n *допустимо.*

Доказательство. Пусть $r, s \in \{1, 2, \ldots, t\}$, $r \neq s$. Покажем, что

$$(R_{i_r} + \vec{u}_r) \cap (R_{i_s} + \vec{u}_s) = \varnothing. \tag{2}$$

Для этого достаточно убедиться, что $\vec{u}_r - \vec{u}_s \notin R_{i_r} + R_{i_s}$. Рассмотрим несколько случаев.

Случай 1. Пусть $i_r = i_s$. Тогда векторы $\vec{u}_r$ и $\vec{u}_s$ линейно зависимы. Из конструкции векторов $\vec{u}_r$ и $\vec{u}_s$ следует, что вес вектора $\vec{u}_r - \vec{u}_s$ больше или равен шести. Следовательно, рассуждая так же, как при доказательстве утверждения 1, получим, что $\vec{u}_r - \vec{u}_s \notin R_{i_r}$.

Случай 2. Пусть $i_r \neq i_s$. Покажем, что $\vec{u}_r - \vec{u}_s \notin R_{i_r} + R_{i_s}$. В силу теоремы 2 достаточно убедиться, что носитель вектора $\vec{u}_r - \vec{u}_s$ содержит некоторую точку x, не лежащую на прямой $l_{i_r i_s}$ и такую, что никакая другая точка из этого носителя (отличная от точек x, i_r, i_s) не принадлежит плоскости $P_{x i_r i_s}$.

Случай 2.1. Пусть столбцы $\vec{h}_{i_r}$ и $\vec{h}_{i_s}$ таковы, что в результате любой линейной их комбинации получается столбец, представимый линейной комбинацией трёх или более столбцов из множества $\{\vec{h}_1, \vec{h}_2, \ldots, \vec{h}_m\}$.

Носитель вектора $\vec{u}_r - \vec{u}_s$ принадлежит множеству $\{1, 2, \ldots, m\} \cup \{i_r\} \cup \{i_s\}$. Следовательно, $x \in \{1, 2, \ldots, m\}$. Так как $\vec{h}_1, \vec{h}_2, \ldots, \vec{h}_m$ линейно независимы, очевидно, что ни один столбец из $\{\vec{h}_1, \vec{h}_2, \ldots, \vec{h}_m\} \setminus \{\vec{h}_x\}$ линейно не выражается через $\vec{h}_x, \vec{h}_{i_r}, \vec{h}_{i_s}$. Поэтому $\vec{u}_r - \vec{u}_s \notin R_{i_r} + R_{i_s}$.

Случай 2.2. Пусть столбцы $\vec{h}_{i_r}$ и $\vec{h}_{i_s}$ таковы, что в результате некоторой линейной их комбинации получается столбец $\vec{h}$, представимый линейной комбинацией двух столбцов $\vec{h}_{y'}, \vec{h}_{y''}$ из множества $\{\vec{h}_1, \vec{h}_2, \ldots, \vec{h}_m\}$.

Случай 2.2.1. Если хотя бы одна из точек y', y'' не принадлежит носителю вектора $\vec{u}_r - \vec{u}_s$, то $\vec{u}_r - \vec{u}_s \notin R_{i_r} + R_{i_s}$.

Случай 2.2.2. Пусть обе точки y', y'' принадлежат носителю вектора $\vec{u}_r - \vec{u}_s$. Тогда выберем в носителе вектора $\vec{u}_r - \vec{u}_s$ точку x, отличную от y', y'', i_r, i_s. Такой выбор возможен в силу конструкции векторов $\vec{u}_r, \vec{u}_s$. Носитель вектора $\vec{u}_r - \vec{u}_s$ принадлежит множеству $\{1, 2, \ldots, m\} \cup \{i_r\} \cup \{i_s\}$. Следовательно, точки x, y', y'' принадлежат множеству $\{1, 2, \ldots, m\}$ и не являются коллинеарными. Рассмотрим любую другую линейную комбинацию столбцов $\vec{h}_{i_r}, \vec{h}_{i_s}$, в результате которой получается столбец, линейно независимый от столбца h. Поскольку расстояние между векторами $\vec{\lambda}_r$ и $\vec{\lambda}_s$ больше или равно пяти и столбцы $\vec{h}_1, \vec{h}_2, \ldots, \vec{h}_m$ линейно независимы, расстояние между столбцами $\vec{h}_r$ и $\vec{h}_s$ также больше или равно пяти. Следовательно, в результате рассматриваемой линейной комбинации получится столбец, который является линейной комбинацией трёх или более столбцов из множества $\{\vec{h}_1, \vec{h}_2, \ldots, \vec{h}_m\}$. Таким образом, $\vec{u}_r - \vec{u}_s \notin R_{i_r} + R_{i_s}$.

Случай 2.3. Пусть столбцы $\vec{h}_{i_r}$ и $\vec{h}_{i_s}$ таковы, что в результате некоторой линейной их комбинации получается столбец из множества $\{\vec{h}_1, \vec{h}_2, \ldots, \vec{h}_m\}$. Тогда такими же рассуждениями, как и в предыдущем случае, получим, что $\vec{u}_r - \vec{u}_s \notin R_{i_r} + R_{i_s}$. Теорема 3 доказана.

3. Примеры 2 и 3

Семейства компонент в примерах 2 и 3 строятся точно так же, как и в примере 1.

Пример 2. Пусть код $(\Lambda \cup \{\vec{0}\}) \subset \mathbb{F}_3^m$ содержит t ненулевых векторов $\vec{\lambda}_1, \vec{\lambda}_2, \ldots, \vec{\lambda}_t$, вес каждого из которых больше или равен трём. Пусть также расстояние между любыми двумя различными векторами из $\Lambda = \{\vec{\lambda}_1, \vec{\lambda}_2, \ldots, \vec{\lambda}_t\}$ больше или равно трём. Тогда множеству Λ соответствует допустимое семейство компонент троичного кода Хэмминга длины $n = (3^m - 1)/2$.

Пример 3. В проверочной матрице H двоичного кода Хэмминга $\mathbb{H}$ длины $n = 2^m - 1$ выберем m линейно независимых столбцов. Будем считать, что выбранными являются столбцы $\vec{h}_1, \vec{h}_2, \ldots, \vec{h}_m$. В H выберем также k столбцов, которые являются линейной комбинацией двух столбцов из множества $\{\vec{h}_1, \vec{h}_2, \ldots, \vec{h}_m\}$. Будем считать, что этими столбцами являются $\vec{h}_{m+1}, \vec{h}_{m+2}, \ldots, \vec{h}_{m+k}$. Пусть код $(\Lambda \cup \{\vec{0}\}) \subset \mathbb{F}_2^{m+k}$ содержит t ненулевых векторов $\vec{\lambda}_1, \vec{\lambda}_2, \ldots, \vec{\lambda}_t$, вес каждого из которых больше или равен $3k + 3$. Пусть также расстояние между любыми двумя различными векторами из $\Lambda = \{\vec{\lambda}_1, \vec{\lambda}_2, \ldots, \vec{\lambda}_t\}$ больше или равно $3k + 3$. Каждому вектору $\vec{\lambda}_s = (\lambda_{s1}, \lambda_{s2}, \ldots, \lambda_{sm+k})$ длины $m + k$ так же, как в примере 1,

сопоставим вектор $\vec{u}_s$ длины $n = 2^m - 1$, где $s \in \{1, \dots, t\}$. Тогда множеству Λ соответствует допустимое семейство компонент двоичного кода Хэмминга длины $n = 2^m - 1$.

Доказательство того факта, что приведённые в примерах 2 и 3 семейства компонент являются допустимыми, аналогично доказательству теоремы 3. В случае троичных кодов следует учитывать особенности поля Галуа $\mathbb{F}_3$. Пусть $\vec{x}$, $\vec{y} \in \mathbb{F}_3^m$. Тогда очевидно, что если $d(\vec{x}, \vec{y}) = m$ и векторы $\vec{x}$,, $\vec{y}$ не содержат нулевых компонент, то они линейно зависимы.

4. Вложение в совершенный код

Далее докажем теорему о вложимости.

Через $\vec{e}_i$ обозначим вектор длины n, в котором i-я компонента равна 1, а другие компоненты равны 0. Пусть

$$\mathbb{T} = \left(\mathbb{H} \setminus \bigcup_{s=1}^{t} (R_{i_s} + \vec{u}_s)\right) \cup \left(\bigcup_{s=1}^{t} (R_{i_s} + \vec{u}_s + \mu_s \cdot \vec{e}_{i_s})\right). \qquad (3)$$

В силу теоремы 3 семейство компонент $R_{i_1} + \vec{u}_1, R_{i_2} + \vec{u}_2, \dots, R_{i_t} + \vec{u}_t$ q-ичного кода Хэмминга $\mathbb{H}$ допустимо (аналогичные теоремы о допустимости семейства компонент справедливы и для кодов из примеров 2 и 3). Следовательно, множество $\mathbb{T}$ является q-ичным 1-совершенным кодом длины n [3, 4]. В силу утверждения 1 код $\mathbb{T}$ содержит нулевой вектор.

Теорема 4. *Каждый q-ичный код длины m с кодовым расстоянием 5 (при $q = 3$ с кодовым расстоянием 3) вкладывается в некоторый q-ичный 1-совершенный код длины $n = (q^m - 1)/(q - 1)$. Каждый двоичный код длины $m + k$ с кодовым расстоянием $3k + 3$ вкладывается в некоторый двоичный 1-совершенный код длины $n = 2^m - 1$, $k \geqslant 0$.*

Доказательство. Из конструкции допустимого семейства компонент q-ичного кода $\mathbb{H}$ в примере 1 и формулы (3) следует, что каждый q-ичный код $\Lambda \cup \{\vec{0}\}$ длины m с кодовым расстоянием 5 может быть вложен (в строгом смысле) в q-ичный 1-совершенный код $\mathbb{T}$ длины $n = (q^m - 1)/(q - 1)$.

Из конструкции допустимого семейства компонент троичного кода $\mathbb{H}$ в примере 2 и формулы (3) следует, что каждый троичный код $\Lambda \cup \{\vec{0}\}$ длины m с кодовым расстоянием 3 может быть вложен (в строгом смысле) в некоторый троичный 1-совершенный код $\mathbb{T}$ длины $n = (3^m - 1)/2$.

Из конструкции допустимого семейства компонент двоичного кода $\mathbb{H}$ в примере 3 и формулы (3) следует, что каждый двоичный код $\Lambda \cup \{\vec{0}\}$

длины $m+k$ с кодовым расстоянием $3k+3$ может быть вложен в некоторый двоичный 1-совершенный код $\mathbb{T}$ длины $n = 2^m - 1$, $k \geqslant 0$. В случае двоичных кодов из примера 3 вложение не является строгим. Теорема 4 доказана.

ЛИТЕРАТУРА

1. **Романов А. М.** О разбиениях q-ичных кодов Хэмминга на непересекающиеся компоненты // Дискрет. анализ и исслед. операций. Сер. 1. — 2004. — Т. 11, № 3. — С. 80–87.
2. **Avgustinovich S. V., Krotov D. S.** Embedding in a perfect code // J. Comb. Des. — 2009. — Vol. 17, N 5. — P. 419—423.
3. **Etzion T., Vardy A.** Perfect binary codes: Constructions, properties and enumeration // IEEE Trans. Inf. Theory. — 1994. — Vol. 40, N 3. — P. 754–763.
4. **Phelps K. T., Villanueva M.** Ranks of q-ary 1-perfect codes // Des. Codes Cryptography. — 2002. — Vol. 27, N 1–2. — P. 139–144.
5. **Romanov A. M.** Survey of methods for construction of nonlinear perfect binary codes // J. Appl. Industr. Math. — 2008. — Vol. 2, N 2. — P. 252–269.

Романов Александр Михайлович,
e-mail: rom@math.nsc.ru

Статья поступила
13 мая 2011 г.

Переработанный вариант —
21 ноября 2011 г.