ДИСКРЕТНЫЙ АНАЛИЗ И ИССЛЕДОВАНИЕ ОПЕРАЦИЙ
Май—июнь 2009. Том 16, № 3. С. 63–73

УДК 519.2+621.391

О ПОСТРОЕНИИ РАЗБИЕНИЙ F_q^N НА СОВЕРШЕННЫЕ q-ЗНАЧНЫЕ КОДЫ

Ф. И. Соловьева, А. В. Лось

Аннотация. Для любого числа $N = (q^m - 1)/(q - 1)$, где $q > 2$ — степень простого числа, предложены две конструкции построения различных разбиений множества F_q^N всех q-значных векторов длины N на совершенные q-значные коды длины N. Кроме того, приведены нижние оценки числа таких разбиений.

Ключевые слова: совершенный q-значный код, разбиение пространства на коды, нижняя оценка числа различных разбиений на коды.

Введение

Через F_q^N обозначим N-мерное метрическое пространство над полем Галуа $GF(q)$ по отношению к метрике Хэмминга, где $q = p^r$, p — простое число. В настоящей статье предложены два метода построения разбиений пространства F_q^N на различные совершенные q-значные коды длины N с кодовым расстоянием 3, здесь $N = (q^m - 1)/(q - 1)$. В первом методе построения разбиений используется некоторая модификация хорошо известной конструкции Шонхайма [10]. Этот метод является обобщением аналогичного результата для совершенных двоичных кодов (см. [11], а также [1], где установлено, что для любого допустимого $N > 15$ число различных разбиений множества всех двоичных векторов F_2^N на совершенные коды длины N не меньше $2^{2^{(N-1)/2}}$). Недавно стало известно [3], что эта оценка верна для любого допустимого $N \geqslant 7$. Во второй конструкции используются свитчинги простых компонент [6] смежных классов q-значного кода Хэмминга в пространстве F_q^N, где $q > 2$.

Проблема перечисления всех разбиений пространства F_q^N на совершенные q-значные коды тесно связана с классической проблемой перечисления всех совершенных q-значных кодов. В настоящей статье рассматриваются различные разбиения, поскольку, зная оценку снизу числа

различных разбиений, легко оценить снизу число неэквивалентных таких разбиений с учётом порядка группы автоморфизмов F_q^N. Конструкции разбиений могут также быть полезны для построения новых классов q-значных кодов, в частности, совершенных. В [8, гл. 11] описано несколько конструкций совершенных q-значных кодов, в основе которых лежат разбиения пространства F_q^N на совершенные коды. Следует отметить, что для $q > 2$ известно не так много работ, посвящённых построению разбиений пространства F_q^N на совершенные коды, двоичный же случай исследован гораздо глубже.

Напомним некоторые необходимые определения. Произвольное подмножество C пространства F_q^N называется *совершенным q-значным кодом длины N с кодовым расстоянием* 3 (далее кратко *совершенным кодом*), если для любого вектора $x \in F_q^N$ существует единственное кодовое слово y из кода C такое, что расстояние Хэмминга $d(x, y)$ между ними удовлетворяет неравенству $d(x, y) \leqslant 1$. Хорошо известно, что такие коды существуют только для $N = (q^m - 1)/(q - 1)$, $m \geqslant 2$, см. [4, 5, 12]. Код называется *линейным*, если он образует линейное подпространство в пространстве F_q^N. Совершенный линейный код $\mathcal{H}_q^N$ называется *кодом Хэмминга*. Далее будем обозначать его через $\mathcal{H}$. Два кода $C, C' \subset F_q^N$ называются *изоморфными*, если существует такая перестановка σ на N координатных позициях, что $C' = \sigma(C)$. Код Хэмминга единственен с точностью до изоморфизма. Всюду далее $N = qn + 1$, $n = (q^{m-1} - 1)/(q - 1)$ и $m \geqslant 2$.

1. Нижняя оценка числа различных разбиений, полученных с использованием конструкции Шонхайма

В этом разделе описана конструкция класса нетривиальных разбиений пространства F_q^N на совершенные q-значные, $q > 2$, коды длины N с использованием некоторой модификации конструкции Шонхайма [10]. Данная конструкция является обобщением метода построения разбиений пространства всех двоичных векторов на совершенные двоичные коды из [11], где была использована широко известная конструкция Васильева [2].

Рассмотрим произвольное разбиение пространства F_q^n на совершенные коды C_i^n длины n:

$$F_q^n = \bigcup_{i=1}^{(q-1)n+1} C_i^n, \text{ где } n = (q^{m-1} - 1)/(q - 1), \ q > 2. \tag{1}$$

Элементы множества $F_q = \{0, 1, \ldots, q-1\}$ взаимно однозначно сопоставим элементам поля $GF(q)$. Из каждого кода данного разбиения построим для всех $j \in F_q$ с помощью модифицированной конструкции Шонхайма следующие q кодов длины $N = qn+1$:

$$C_k = \left\{ \left(x_1, x_2, \ldots, x_{q-1}, \sum_{t=1}^{q-1} \mid x_t \mid + \lambda_i(c) + j, \sum_{t=1}^{q-1} \alpha_t x_t + c \right) \mid x_t \in F_q^n, \right. \\ \left. c \in C_i^n \right\},$$

где $\alpha_t \in F_q^* = F_q \setminus \{0\}$ и $\alpha_t \neq \alpha_s$ при $t \neq s$, $k = i + j((q-1)n+1)$, $|x_t| = x_{t1} + x_{t2} + \cdots + x_{tn}$ для $x_t = (x_{t1}, x_{t2}, \ldots, x_{tn})$, λ_i — произвольная функция, действующая из кода C_i^n длины n во множество элементов поля $GF(q)$.

Теорема 1. *Для любого $N = qn+1$, $q = p^r$, существует не менее $p^{p^{rn+\log_p r}}$ различных разбиений пространства F_q^N на совершенные q-значные коды длины N.*

Доказательство. При $q = 2$, $n > 15$ доказательство см. в [11], а также в [1], при $q = 2$, $n = 7$ и 15 — в [3]. Пусть $q > 2$. Доказательство того, что построенные множества являются совершенными q-значными кодами, аналогично доказательству из [10]. Покажем, что любые два построенных кода не пересекаются.

Предположим противное, пусть существуют два кода C_1 и C_2 из построенного выше разбиения пространства F_q^N, содержащие совпадающие кодовые слова

$$c_1 = \left(x_1, x_2, \ldots, x_{q-1},\ \sum_{t=1}^{q-1} |x_t| + \lambda_i(c) + j,\ \sum_{t=1}^{q-1} \alpha_t x_t + c \right),$$

$$c_2 = \left(x'_1, x'_2, \ldots, x'_{q-1},\ \sum_{t=1}^{q-1} |x'_t| + \lambda'_i(c') + j'\ \sum_{t=1}^{q-1} \alpha_t x'_t + c' \right),$$

где $c_1 \in C_1$, $c_2 \in C_2$. Из равенств $x_t = x'_t$, $t = 1, \ldots, q-1$, по последним n координатам векторов c_1 и c_2 следует, что $c = c'$. Отсюда получаем, что оба кода C_1 и C_2 были построены из одного и того же кода, принадлежащего разбиению (1) пространства F_q^n и, следовательно, с помощью одной функции λ_i, т. е. $\lambda_i = \lambda'_i$. С учётом того, что значения координат с номером $(q-1)n+1$ кодовых слов c_1 и c_2 совпадают, получаем, что

$j = j'$. Но тогда при совпадениях исходных кодов длины n, функций λ_i и λ_i' и элементов j и j' поля $GF(q)$ получим одинаковые коды длины N, т. е. $C_1 = C_2$. Значит, все коды построенного разбиения попарно не пересекаются.

Число таких разбиений не меньше числа различных функций λ_i для каждого $i = 1, 2, \ldots, (q-1)n+1$. Следовательно, мощность класса различных разбиений пространства F_q^N на совершенные q-значные коды длины $N = qn + 1 = (q^m - 1)/(q - 1)$ не меньше чем

$$(q^{|C_i^n|})^{(q-1)n+1} = (q^{q^{n-(m-1)}})^{q^{m-1}} = q^{q^n} = p^{p^{rn+\log_p r}}.$$

Теорема 1 доказана.

Следует отметить, что доказательство теоремы 1 при $q > 2$ отличается от доказательства для случая $q = 2$ в силу того, что недвоичные совершенные коды не обладают свойством антиподальности. Напомним, что в двоичном случае любой совершенный код помимо кодового слова x содержит антиподальное слово $\mathbf{1}^N - x$, где $\mathbf{1}^N$ — единичный вектор длины N. Этот факт является существенным при исследовании свойств совершенных двоичных кодов и, в частности, учитывается при получении нижней оценки числа различных разбиений пространства F_2^N на совершенные двоичные коды.

2. Нижняя оценка числа различных разбиений, построенных с помощью простых компонент и латинских квадратов

Всюду далее положим $q = p^r$, где r — произвольное целое число, большее 1. Обозначим через R_i подпространство, порождённое всеми тройками (кодовыми словами веса 3) кода Хэмминга $\mathcal{H}_q^N$, $N = nq+1$, с единицей в i-й координате. Известно [9], что множество R_i является i-компонентой и $|R_i| = q^{n(q-1)}$. Через P_i обозначим множество, состоящее из всевозможных линейных комбинаций троек, порождающих компоненту R_i, над простым полем $GF(p)$, т. е. с коэффициентами из простого поля $GF(p)$. Все слова множества P_i имеют в i-й позиции элементы простого поля $GF(p)$, в остальных координатных позициях могут встречаться элементы поля $GF(q)$. Такое множество называется *простой i-компонентой*, для его мощности справедливо равенство $|P_i| = p^{nr(q-2)+n}$. В случае $r = 1$, т. е. $q = p$, множества R_i и P_i совпадают. Простые компоненты введены в [9] для исследования свойств специального вида линейных подкодов (p-ядер) q-значных кодов Хэмминга. В [6] с помощью метода свитчинга простых компонент получена нижняя оценка числа различ-

ных совершенных q-значных кодов для $q > 2$, которая на настоящий момент является лучшей.

Рассмотрим тривиальное разбиение пространства F_q^N на классы смежности по произвольному коду Хэмминга $\mathcal{H}$ длины $N = nq+1$, где $q = p^r$, p — простое, т. е.

$$F_q^N = \mathcal{H} \cup \bigcup_{i=1}^{N} \bigcup_{\alpha \in F_q^*} (\mathcal{H} + \alpha e_i). \tag{2}$$

Основная идея построения различных разбиений заключается в следующем: выбираем произвольную координатную позицию $i \in \{1, 2, \ldots, N\}$, разбиваем код Хэмминга и его смежные классы по i-му направлению из этого разбиения на q/p подклассов смежности по простой i-компоненте (каждый такой подкласс содержит p простых компонент). Далее, используя q/p произвольных латинских квадратов порядка p, делаем свитчинги простых компонент в каждом из этих подклассов. Аналогичные свитчинги делаем для каждой простой компоненты кода Хэмминга независимо, однако латинские квадраты выбираем так, чтобы изменения не касались компонент исходного линейного кода Хэмминга. Подобные преобразования осуществляем по всем N направлениям независимо. Учитывая это, несложно подсчитать число получающихся различных разбиений.

Теперь рассмотрим эту конструкцию в деталях. Обозначим через U объединение

$$U = \bigcup_{\alpha \in F_p} (P_i + \alpha e_i),$$

где P_i — простая i-компонента кода Хэмминга $\mathcal{H}$, F_p — множество элементов простого поля $GF(p)$, $i \in \{1, 2, \ldots, N\}$. Упорядочим строки кодовой матрицы подкода P_i так, чтобы элементы простого поля F_p в i-м столбце расположились в порядке неубывания. Обозначим через $A_{0,\beta}$, $\beta \in F_p$, подкод кода P_i, i-я координата кодовых слов которого равна элементу β, т. е. $A_{0,\beta} = \{v \in P_i \mid v_i = \beta\}$. Тогда код $P_i + \alpha e_i$ будет состоять из подкодов $A_{\alpha,\beta} = A_{0,\beta} + \alpha e_i$ для всех $\beta \in F_p$. Таким образом, множество U состоит из векторов подкодов $A_{\alpha,\beta}$ для всех $\alpha, \beta \in F_p$:

$$U = \bigcup_{\alpha=0}^{p-1} \bigcup_{\beta=0}^{p-1} A_{\alpha,\beta}. \tag{3}$$

Составим $(p \times p)$-матрицу S такую, что в строке с номером α и столбце с номером β будет находиться элемент $s_{\alpha,\beta} \in GF(p)$, равный элементу, стоящему в i-й координатной позиции всех векторов множества $A_{\alpha,\beta}$.

Очевидно, что в рассматриваемом случае такой элемент равен $\alpha+\beta$. Отметим, что в полученной матрице S в любом столбце находятся все различные элементы поля F_p, то же самое верно и для любой строки, т. е. матрица S является латинским квадратом. Кроме того, по матрице S и простой компоненте P_i можно однозначно восстановить множество U. Действительно, произвольная строка с номером α задаёт перестановку (в данном случае циклическую)

$$\pi_\alpha=\begin{pmatrix} 0 & 1 & \dots & p-1 \\ s_{\alpha,0} & s_{\alpha,1} & \dots & s_{\alpha,p-1}\end{pmatrix}=\begin{pmatrix} 0 & 1 & \dots & p-1 \\ 0+\alpha & 1+\alpha & \dots & p-1+\alpha\end{pmatrix},$$

осуществляя по которой свитчинг простой компоненты P_i, получим простую компоненту кода $\mathcal{H}+\alpha e_i$ (в данном случае — компоненту $P_i+\alpha e_i$). Обозначим через

$$U(S)=\bigcup_{\alpha=0}^{p-1}\pi_\alpha(P_i)=\bigcup_{\alpha=0}^{p-1}\bigcup_{\beta=0}^{p-1}A_{\pi_\alpha(\beta),\beta} \tag{4}$$

объединение простых компонент, полученных в результате свитчингов, заданных латинским квадратом S, а точнее свитчингов с помощью подстановок, соответствующих строкам латинского квадрата S. Нетрудно видеть, что вместо S может быть взят любой латинский квадрат L порядка p.

Как ранее упоминалось, множество U можно представить в виде объединения (3). Поскольку в строках латинского квадрата L находятся все различные элементы поля F_p, то из того факта, что множества U и $U(L)$ состоят из одинаковых подмножеств (см., например, (3) и (4)), получаем равенство $U=U(L)$. Таким образом, справедливо

Утверждение 1. *Если множество $U(L)$ построено из множества U свитчингами простых компонент по перестановкам, заданным строками произвольного латинского квадрата L, то эти множества совпадают, т. е. $U=U(L)$.*

Нетрудно видеть, что код $((\mathcal{H}+\alpha e_i)\setminus(P_i+\alpha e_i))\cup\pi_\alpha(P_i)$, полученный свитчингом простой компоненты $P_i+\alpha e_i$ по перестановке π_α, соответствующей некоторой строке латинского квадрата L, отличается от исходного кода $\mathcal{H}+\alpha e_i$, $\alpha\in F_p$.

Пусть $V_i=\bigcup\limits_{\gamma\in F_q}(P_i+\gamma e_i)$. Рассмотрим разбиение множества V_i на классы смежности множества U. Всего таких классов смежности $q/p=$

p^{r-1}. Таким образом,

$$V_i = \bigcup_{t=0}^{p^{r-1}-1} (U + \gamma_t e_i), \tag{5}$$

где $\gamma_t e_i$ — некоторые представители классов смежности, $\gamma_t \in F_q$. В каждом таком классе смежности $U^t = U + \gamma_t e_i$, за исключением множества U, сделаем свитчинги всех простых компонент с помощью перестановок π_α, заданных строками своего латинского квадрата L_t порядка p, где $t \in \{1, 2, \ldots, p^{r-1} - 1\}$, $\alpha = 0, 1, \ldots, p-1$. Полученные множества обозначим через

$$\widetilde{U}^t(L_t) = \bigcup_{\alpha \in F_p} (\pi_\alpha(P_i) + \gamma_t e_i), \tag{6}$$

$t \in \{1, 2, \ldots, p^{r-1} - 1\}$. Подчеркнём, что для всех таких t строим множества (6), а для $t = 0$ положим, что первая строка латинского квадрата L_0 фиксирована и имеет вид $(0\ 1\ \ldots\ (p-1))$, тогда

$$\widetilde{U}^0(L_0) = P_i \cup \bigcup_{\alpha \in F_p^*} (\pi_\alpha(P_i)).$$

Таким образом, простая компонента кода Хэмминга, как и сам код Хэмминга, в процессе всех преобразований останутся без изменений. В силу того, что множество V_i представимо в виде объединения (5), согласно утверждению 1 получаем

Утверждение 2. *Для произвольных латинских квадратов L_t порядка p, $t \in \{1, 2, \ldots, p^{r-1} - 1\}$, и произвольного латинского квадрата L_0 с фиксированной первой строкой вида $(0\ 1\ \ldots\ (p-1))$ справедливо равенство*

$$V_i = \bigcup_{t=0}^{p^{r-1}-1} \widetilde{U}^t(L_t).$$

Из построения множества V_i следует, что оно состоит из q простых компонент, принадлежащих каждая своему коду из объединения $W_i = \bigcup_{\gamma \in F_q} (\mathcal{H} + \gamma e_i)$. Рассмотрим разбиение этого множества W_i на классы смежности множества V_i, обозначим их через $V_i^k = V_i + v^k$, где v^k является некоторым представителем класса смежности. Ясно, что число таких классов смежности будет равно числу K простых компонент в коде Хэмминга, т. е. $W_i = \bigcup_{k=0}^{K-1} V_i^k$, где $K = p^{n(2r-1)-r(m-1)}$ (см., например, [6]).

Множество, полученное свитчингами всех простых i-компонент кодов объединения W_i, обозначим через $\widetilde{W_i}$, т. е. $\widetilde{W_i} = \bigcup\limits_{k=0}^{K-1} \bigcup\limits_{t=0}^{p^{r-1}-1} \widetilde{U}^t(L_t)$.

Заметим, что такие преобразования кодов разбиения (2) можно делать по всем направлениям $i \in \{1, 2, \ldots, N\}$ одновременно и независимо, поскольку линейный код Хэмминга $\mathcal{H}$, содержащийся в каждом объединении W_i, $i \in \{1, 2, \ldots, N\}$, не изменяется в процессе описанных преобразований, т. е. объединения $\widetilde{W_i}$ также содержат код $\mathcal{H}$. Учитывая этот факт, удалим из объединений $\widetilde{W_i}$ для всех i из множества $\{1, 2, \ldots, N-1\}$ общий линейный код Хэмминга и обозначим их через $\widetilde{W_i'} = \widetilde{W_i} \setminus \mathcal{H}$. При конструировании множества $\widetilde{W_N'}$ из объединения W_N осуществляем свитчинги всех простых компонент вместе с компонентами линейного кода Хэмминга, за исключением одной линейной простой компоненты. Отметим, что в качестве последней координатной позиции может быть выбрана произвольная.

Теорема 2. *Объединение $\bigcup\limits_{i=1}^{N} \widetilde{W_i'}$ представимо в виде разбиения пространства F_q^N на совершенные q-значные коды.*

Доказательство. Объединение $\bigcup\limits_{i=1}^{N} \widetilde{W_i'}$ состоит из множеств вида (6). Такие множества получены объединением преобразованных с помощью некоторых свитчингов простых компонент кодов исходного разбиения пространства F_q^N. В силу того, что в результате свитчингов из классов смежности кодов Хэмминга получаются совершенные коды той же длины, а также в силу утверждения 2 получаем требуемое. Теорема 2 доказана.

Обозначим число различных латинских квадратов порядка p через $L(p)$. Известно, что $L(p) \geqslant \prod\limits_{s=1}^{p} s!$ (см., например, [7]). Из конструкции разбиений и предыдущей теоремы нетрудно доказать следующее утверждение.

Теорема 3. *Число различных разбиений пространства F_q^N, $q > 2$, на совершенные q-значные коды не меньше чем*

$$((L(p))^{p^{r-1}})^{KN} \cdot (p!)^{K(1-N)-1}, \tag{7}$$

где $K = p^{n(2r-1)-r(m-1)}$, $q = p^r$.

Доказательство. Рассмотрим множество $U(L)$, где L — некоторый латинский квадрат порядка p, см. (4). Число различных таких множеств

равно числу различных латинских квадратов $L(p)$. Множество V_i состоит из $q/p = p^{r-1}$ сдвигов множества U, для свитчингов каждого из них выбирается произвольный латинский квадрат. Однако среди этих p^{r-1} латинских квадратов один всегда с фиксированной строкой, т. е. общее число различных конфигураций нужно разделить на $p!$. Таким образом, учитывая приведённые выше рассуждения и тот факт, что подобные преобразования можно независимо осуществлять для всех K простых компонент кода и по всем координатным позициям, за исключением последней, N-й координаты, получаем следующий вклад преобразований по всем координатам кроме N-й в оценку снизу числа различных разбиений: $((L(p))^{p^{r-1}}/p!)^{K(N-1)}$.

Для последней N-й координаты рассуждения аналогичны с той только разницей, что все кроме одного латинские квадраты, взятые для осуществления свитчингов, не имеют фиксированных строк. Таким образом, вклад преобразований по последней координате в общее число получаемых разбиений составит по крайней мере $((L(p))^{p^{r-1}})^K/p!$. В итоге получаем

$$\left(\frac{(L(p))^{p^{r-1}}}{p!}\right)^{K(N-1)} \cdot \frac{\left((L(p))^{p^{r-1}}\right)^K}{p!} = ((L(p))^{p^{r-1}})^{KN} \cdot (p!)^{K(1-N)-1}.$$

Теорема 3 доказана.

Следствие 1. *Число различных разбиений пространства F_q^N, $q > 2$, на совершенные q-значные коды с одним фиксированным кодом Хэмминга не меньше $((L(p))^{p^{r-1}}/p!)^{KN}$, где $K = p^{n(2r-1)-r(m-1)}$, $q = p^r$.*

Нетрудно видеть, что оценка (7) существенно лучше оценки, даваемой теоремой 1.

Для сравнения полученной нижней оценки числа различных разбиений пространства F_q^N на совершенные q-значные коды с нижней оценкой числа различных таких кодов [6] приведём их выражения при $p \to \infty$, $q = p^r$, $r > 1$. Используя неравенство $p! < p^p$ и оценку снизу числа различных латинских квадратов [7]

$$L(p) > p^{p^2}(2\pi p)^p e^{1/6-2p^2} > p^{p^2+p} \cdot p^{-2p^2 \log_p e} > p^{p^2(1-\log_p e)} = p^{p^2(1-o(1))},$$

с учётом значения N из оценки следствия 1 получаем, что число различных разбиений при $p \to \infty$ не меньше числа

$$(p^{p^{r+1}(1-o(1))})^{p^{n(2r-1)}} = p^{p^{n(2r-1)+r+1} \cdot (1-\varepsilon_p)}.$$

В то же время, согласно [6] число различных совершенных q-значных кодов при $p \to \infty$ не меньше $(p!)^{p^{n(2r-1)-r(m-1)}} > p^{p^{n(2r-1)-r(m-1)+1} \cdot (1-\delta_p)}$, где ε_p и δ_p стремятся к 0 при $p \to \infty$.

ЛИТЕРАТУРА

1. **Августинович С. В., Соловьева Ф. И., Хеден У.** О разбиениях n-куба на неэквивалентные совершенные коды // Проблемы передачи информации. — 2007. — Т. 43, № 4. — С. 45–50.
2. **Васильев Ю. Л.** О негрупповых плотно упакованных кодах // Проблемы кибернетики. — 1962. — Вып. 8. — С. 337–339.
3. **Гуськов Г. К.** О числе различных разбиений куба E^{15} на совершенные двоичные коды // Материалы 47-й международной научной студенческой конференции «Студент и научно-технический прогресс»: Математика. — Новосибирск: Новосибирский гос. ун-т, 2009. — С. 160.
4. **Зиновьев В. А., Леонтьев В. К.** О совершенных кодах // Препринт/ ИППИ АН СССР. — 1972. — Вып. 1. — С. 26–35.
5. **Зиновьев В. А., Леонтьев В. К.** Несуществование совершенных кодов над полями Галуа // Проблемы управления и теории информации. — 1973. — Вып. 2. — С. 123–132.
6. **Лось А. В.** Построение совершенных q-ичных кодов свитчингами простых компонент // Проблемы передачи информации. — 2006. — Т. 42, № 1. — С. 34–42.
7. **Тимашёв А. Н.** О перманентах случайных дважды стохастических матриц и асимптотических оценках чисел латинских прямоугольников и латинских квадратов // Дискрет. математика. — 2002. — Т. 14. Вып. 4. — С. 65–86.
8. **Cohen G., Honkala I., Lobstein A., Litsyn S.** Covering codes. — Amsterdam, Lausanne, New York, Oxford, Shannon, Tokyo: Elsevier, 1998. — 542 p.
9. **Phelps K. T., Villanueva M.** Ranks of q-ary 1-perfect codes // Des. Codes Cryptogr. — 2002. — V. 27. — P. 139–144.
10. **Schönheim J.** On linear and nonlinear single-error-correcting q-ary 1-perfect codes // Inform. Control. — 1986. — Vol. 12. — P. 23–26.
11. **Solov′eva F. I.** On perfect codes and related topics // Com²Mac Lecture Note. Series 13. — Pohang, 2004. — 80 p.

12. **Tietäväinen A.** On the nonexistence of perfect codes over finite fields // SIAM J. Appl. Math. — 1973. — Vol. 24. — P. 88–96.

Соловьева Фаина Ивановна,
e-mail: sol@math.nsc.ru

Лось Антон Васильевич,
e-mail: sozercatel@gmail.com

Статья поступила
28 октября 2008 г.
Переработанный вариант —
1 апреля 2009 г.