# RECONSTRUCTION OF CAPS FOR CENTERED FUNCTION

A. Yu. Vasil'eva

We consider the space $E^n = \{0;1\}^n$ with the Hamming metric $\rho$, where $\rho(\mathbf{x},\mathbf{y}) = \sum_{i=0}^{n} |x_i - y_i|$. Denote by $wt(\mathbf{x}) = \rho(\mathbf{x},\mathbf{0})$ the Hamming weight of $\mathbf{x}$. A partial ordering of $E^n$ is defined as usual: $\mathbf{x} \preceq \mathbf{y}$ if $x_i \le y_i$ for any $i = 0, 1, \ldots, n$.

We study centered functions as a generalization of perfect binary codes with distance 3. A function $f : E^n \longrightarrow \mathbf{R}$ is said to be *centered* [2] if a sum of its values on every ball of radius 1 is equal to 0. It is known [1, 2], that the values of a 0-centered function at the vertices of weight $(n+1)/2$ uniquely determine all values of this function. Moreover [3, 4], given all values of such a function at the vertices of weight $i$, $0 \le i \le (n-1)/2$, all values of this function at the vertices of weight less than $i$ and more than $n-i$ are uniquely determined.

If $wt(\mathbf{x}) = i \le h$, then put $U^h(\mathbf{x}) = \{\mathbf{y} \in E^n \mid \mathbf{x} \preceq \mathbf{y},\ wt(\mathbf{y}) = h\}$ and call the set $U^h(\mathbf{x})$ an $(i,h)$-cap with respect to $\mathbf{x}$. We also say that a sum $\sum_{\mathbf{y}\in U^h(\mathbf{x})} f(\mathbf{y})$ is an *$(i,h)$-cap of the function $f$ with respect to the vertex* $\mathbf{x}$. Our main result is the following:

**Theorem.** Let $f : E^n \longrightarrow \mathbf{R}$ be a 0-centered function and $0 \le i \le k, h \le n$. Then all $(i,h)$-caps of the function $f$ are uniquely determined by all $(i,k)$-caps of this function.

The corresponding reconstruction formula is obtained.

**Corollary 1.** Let $f : E^n \longrightarrow \mathbf{R}$ be a 0-centered function and $0 \le i \le h \le n$. Given all values of $f$ at the vertices of weight $i$, all $(i,h)$-caps of $f$ are uniquely determined.

**Corollary 2.** Let $f : E^n \longrightarrow \mathbf{R}$ be a 0-centered function and $0 \le i \le h \le n$. Given all $(i,h)$-caps of $f$ at the vertices of weight $i$, all values of $f$ at the vertices of weight $i$ and less than $i$ are uniquely determined.

The author is grateful to S.V. Avgustinovich for statement of the problem and constant attention to this work.

## REFERENCES

1. S. V. Avgustinovich, (1995) *On a property of perfect binary codes*, Discrete Analysis and Operation Research V.2. No. 1. 1995. P. 4-6. (in Russian).

2. S. V. Avgustinovich, A. Yu. Vasil'eva, (2003) *Reconstruction of centered function by its values at two middle levels of hypercube*, Discrete Analysis and Operation Research V. 10. No. 2. 2003. P. 3-16. (in Russian).

3. S. V. Avgustinovich, A. Yu. Vasil'eva, (2002) *Testing sets for 1-perfect codes*, Proc. of Int. Conf. "General theory of information transfer and combinatorics", Germany, Bielefeld, November 4-9, 2002, submitted.

4. A. Yu. Vasil'eva, 92003) *Partial reconstruction of perfect binary codes*, Proc. of Int. Workshop on Coding and Cryptography, March 24-28 2003, Versailles, France. P. 445-452.

Vasil'eva Anastasia Yurievna,
Sobolev Institute of Mathematics,
pr. Akademika Koptyuga, 4, Novosibirsk, 630090, Russia,
phone: (8-383-2) 33-38-96, fax: (8-383-2) 33-25-98, e-mail: vasilan@math.nsc.ru

# CODING THEORY OVER POSET METRICS

Hyun Kwang Kim

Let $\mathbb{F}_q$ be the finite field with $q$ elements and $\mathbb{F}_q^n$ be the vector space of $n$-tuples of $\mathbb{F}_q$. Coding theory may be viewed as the study of $\mathbb{F}_q^n$ when $\mathbb{F}_q^n$ is endowed with the Hamming metric. Let $P$ be a poset on $[n] = \{1, 2, \cdots, n\}$. Brualdi *et al.*([2]) defined a new non Hamming metric on $\mathbb{F}_q^n$ which is associated to $P$. This metric is called the $P$-metric or simply the poset metric. In this talk we survey recent results on codes over poset metrics. We first review basic facts on poset metrics. Next we discuss some results on the classification of perfect codes over crown poset metrics([1],[9]), the classification of posets admitting a given code to be a perfect code([5]), the automorphism groups of certain poset metric spaces([3],[10]), generalizations of MacWilliams identity on poset codes([4],[6],[7]), and association schemes arising from poset metrics([8]).

This research was supported by Com$^2$MaC-KOSEF and BK-21 research fund.

## REFERENCES

1. J. Ahn, H. K. Kim, J. S. Kim and M. Kim, (2003) *Classification of perfect codes with crown poset structure*, Discrete Math. **268**, P/ 21–30.
2. R. A. Brualdi, J. Graves and K. M. Lawrence, (1995) *Codes with a poset metric*, Discrete Math. **147**, P. 57–72.
3. S. H. Cho and D. S. Kim, *Automorphism group of the crown-weighted space*, submitted.
4. S. T. Dougherty and M. M. Skriganov, (2002) *MacWilliams duality and the Rosenbloom-Tsfasman metric*, Mosc. Math. J. **2**, P. 82–97.
5. J. Y. Hyun and H. K. Kim, *The poset structures admitting the extended binary Hamming code to be a perfect code*, submitted.
6. D. S. Kim, *MacWilliams-type identities for fragment and sphere enumerators*, submitted.
7. H. K. Kim and D. Y. Oh, *A classification of posets admitting MacWilliams identity*, submitted.
8. H. K. Kim and D. Y. Oh, *Association schemes for poset metrics and MacWilliams duality*, preprint.
9. H. K. Kim and D. Y. Oh, *On the nonexistence of triple-error-correcting perfect binary linear codes with crown poset structure*, submitted.
10. K. Lee, (2003) *Automorphism group of the Rosenbloom-Tsfasman space*, Eur. J. Combin. **24**, P. 607-612.

Hyun Kwang Kim,
Pohang University of Science and Technology,
Department of Mathematics, San 31 Hyoja Dong, Pohang, 790-784, Korea,
phone: 82-54-279-2049, fax: 82-54-279-2799, e-mail: hkkim@postech.ac.kr

# ON THE NUMBER OF 1-PERFECT BINARY CODES. A LOWER BOUND

D. S. Krotov and S. V. Avgustinovich

Let $F^n$ ($F^n_{ev}$, $F^n_{od}$) be the set of binary $n$-words (with even or odd number of ones, respectively) with the Hamming distance $d$ and mod 2 coordinate-wise addition. If $S \subseteq F^n$, then $\mathrm{Aut}(S)$ is the group of isometries $g$ of $F^n$ such that $g(S) = S$, and the *neighborhood* of $S$ is the set $\Omega(S) \stackrel{df}{=} \bigcup_{\bar{x}\in S} \Omega(\bar{x})$, where $\Omega(\bar{x}) \stackrel{df}{=} \{\bar{y} \in F^n \,|\, d(\bar{y}, \bar{x}) = 1\}$. For a collection $\mathbf{S} = \{S_1, ..., S_l\}$ of subsets of $F^n$, by $\mathrm{Aut}(\mathbf{S})$ denote the group of isometries $g$ of $F^n$ such that for each $S \in \mathbf{S}$ the set $g(S)$ is also in $\mathbf{S}$.

An *extended* 1*-perfect code* is a set $C \subseteq F^n_{ev}$ such that the neighborhoods of the words of $C$ are pairwise disjoint and $\Omega(C) = F^n_{od}$. It follows that $|C| = |F^n_{od}|/n = 2^{n-\log_2 n - 1}$ and $n$ is a power of 2. We assume $n = 2^m \geq 16$. A unique (up to equivalence) linear extended 1-perfect code $H$ (the Hamming code) can be represented by the following inductive formulas

$$A^1 \stackrel{df}{=} V^1, \quad A^t \stackrel{df}{=} \bigcup_{\bar{r}\in V^t} (\bar{r} + A^{t-1}), \quad H \stackrel{df}{=} A^{m-1}, \tag{1}$$
$$\text{where} \quad V^t \stackrel{df}{=} \{(\bar{v}, \bar{v}, 0, ..., 0) \in F^n \,|\, \bar{v} \in F^{2^{m-t}}_{ev}\}.$$

If in (1) for some $\bar{r}$ we replace $A^{t-1}$ by the set with the same neighborhood, then $\Omega(A^t)$ and, consequently, $\Omega(H)$ do not change. Let $\mathcal{A}^t \stackrel{df}{=} \mathrm{Aut}(\Omega(A^t))$. Then the set $C$ represented by the following formulas is an extended 1-perfect code.

$$A^1_{\bar{r}_1,...,\bar{r}_{m-1}} \stackrel{df}{=} V^1, \quad A^t_{\bar{r}_{t+1},...,\bar{r}_{m-1}} \stackrel{df}{=} \bigcup_{\bar{r}_t \in V^t} \left(\bar{r}_t + g_{\bar{r}_t,...,\bar{r}_{m-1}}(A^{t-1}_{\bar{r}_t,...,\bar{r}_{m-1}})\right), \quad C \stackrel{df}{=} g(A^{m-1}), \tag{2}$$

where $g_{\bar{r}_t,...,\bar{r}_{m-1}} \in \mathcal{A}^{t-1}$; in particular, $g \in \mathcal{A}^{m-1}$. Let $\mathcal{B}^t \stackrel{df}{=} \mathrm{Aut}\big(\{\Omega(r + A^{t-1})\}_{\bar{r}\in V^t}\big)$, $t = 2, ..., m-1$, and $\mathcal{B}^1 \stackrel{df}{=} \mathrm{Aut}(A^1)$. For each $t = 1, ..., m-1$ we fix a set $\mathcal{D}^t$ of representatives of cosets from $\mathcal{A}^t/\mathcal{B}^t$. It can be shown by induction that the restrictions

$$g_{\bar{r}_t,...,\bar{r}_{m-1}} \in \mathcal{D}^{t-1} \tag{3}$$

do not reduce the set of codes that can be represented by (2). Almost all ($n \to \infty$) codes represented by (2,3) have a unique representation (2,3), and their number is not less than

$$K(n) \stackrel{df}{=} |\mathcal{D}^{m-1}| \prod_{t=1}^{m-2} \left(|\mathcal{D}^t|^{|V_{t+1}|} - |\mathcal{D}^t| \cdot |V_{t+1}|\right)^{|V_{t+2}|\cdot...\cdot|V_{m-1}|} = \tag{4}$$

$$= \frac{n!}{6\cdot\left(\frac{n}{4}!\right)^4} \prod_{\substack{t=1\\k=2^t}}^{m-2} \left(\left(2\left(\tfrac{1}{2}\binom{k}{k/2}\right)^{\frac{n}{k}}\right)^{2^{\frac{n}{2k}-1}} - 2\left(\tfrac{1}{2}\binom{k}{k/2}\right)^{\frac{n}{k}} \cdot 2^{\frac{n}{2k}-1}\right)^{2^{\frac{n}{2k}-\log_2\frac{n}{2k}-1}} \simeq \frac{n!}{6\cdot\left(\frac{n}{4}!\right)^4} \prod_{\substack{t=1\\k=2^t}}^{m-2} \left(2\left(\tfrac{1}{2}\binom{k}{k/2}\right)^{\frac{n}{k}}\right)^{2^{\frac{n}{k}-\log_2\frac{n}{k}-1}}.$$

There is a one-to-one correspondence (deleting the last symbol) between extended 1-perfect codes and 1-*perfect codes*. So, for the number $B(n-1)$ of 1-perfect binary codes of length $n-1$ we get the lower bound $B(n-1) \geq K(n)$. All previous lower bounds are restricted by two multipliers ($t = 1, 2$) of (4).

**Hypothesis.** The lower bound $B(n-1) \geq K(n)$ is asymptotically tight.

Krotov Denis Stanislavovich, Avgustinovich Sergey Vladimirovich,
Sobolev Institute of Mathematics, Koptyuga, 4, Novosibirsk, 630090, Russia,
e-mail: avgust@math.nsc.ru, krotov@math.nsc.ru

# О ТРАНЗИТИВНЫХ СОВЕРШЕННЫХ КОДАХ ДЛИНЫ 15

С. А. Малюгин

Число нелинейных совершенных двоичных кодов длины $n = 2^k - 1$ ($k \geq 4$) оценивается снизу величиной $2^{2^{\frac{n}{2}+o(n)}}$. До настоящего времени задача перечисления и классификации не решена даже для кодов минимальной длины $n = 15$. В последнее время интерес к этой задаче возрос в связи с возможностью применения компьютеров [1–3]. В [4] дана классификация всех кодов длины 15, которые строятся из кода Хемминга сдвигами непересекающихся компонент. Так как кодов очень много, то имеет смысл перечислять только неэквивалентные друг другу коды. Например, число всех неэквивалентных кодов Васильева равно 19 [1], для кодов, построенных в [2] и [3], эти числа равны соответственно 963 и 777. Число неэквивалентных кодов, построенных в [4] равно 370. Кроме этого можно рассматривать только специальные подклассы кодов, которые в каком то смысле близки к линейным кодам. Сейчас появляется интерес к транзитивным кодам [5]. Код $C$ называется транзитивным, если группа автоморфизмов $\mathrm{Aut}(C)$ действует транзитивно на элементах кода $C$. Среди кодов, построенных в [4], найдены все транзитивные. Оказалось, что существует всего 5 неэквивалентных транзитивных кодов Васильева (включая один линейный код ранга 11 и 4 кода ранга 12), 9 кодов ранга 13 и 2 кода ранга 14. Их разбиения на группы из расширенно эквивалентных кодов соответственно имеют вид 2+1+1+1, 3+2+2+1+1 и 1+1. Не существует транзитивных кодов ранга 15. Размерности ядер трех кодов Васильева равны 9 и у одного кода размерность ядра равна 7. У всех кодов ранга 13 размерности ядер равны 8. Размерности ядер двух кодов ранга 14 равны соответственно 8 и 5. Найдены также группы автоморфизмов всех перечисленных кодов.

Работа поддержана грантом РФФИ (проект 02-01-00939) и программой поддержки ведущих научных школ (проект НШ–313.2003.1).

## ЛИТЕРАТУРА

1. Hergert F. *The equivalence classes of the Vasil'ev codes of length 15* // Combinatorial theory (Schloss Rauischholzhausen, 1982), P. 176–186, Lectures Notes in Math.,969, Springer, Berlin—New York, 1982.
2. Phelps K. T. *An enumeration of 1-perfect binary codes* // Australasian Journal of Combinatorics. 2000. V. 21. P. 287–298.
3. Зиновьев В. А., Зиновьев Д. В. *Двоичные совершенные коды длины 15, построенные обобщенной каскадной конструкцией* // Проблемы передачи информации. 2004. Т. 40, вып. 1. С. 27–39.
4. Малюгин С. А. *О перечислении совершенных двоичных кодов длины 15* // Дискрет. анализ и исслед. операций. Сер. 2. 1999. Т. 6, № 2. С. 48–73.
5. Solov'eva F. I. *On transitive codes* // См. настоящий сборник. с. 99

Малюгин Сергей Артемьевич,
Институт математики им. С. Л. Соболева СО РАН,
пр. Академика Коптюга 4, Новосибирск, 630090, Россия,
тел. (8-383-2) 33-38-69, факс (8-383-2) 32-25-98, e-mail: mal@math.nsc.ru

# ON PERFECT COLORINGS OF THE INFINITE RECTANGULAR GRID

S. A. Puzynina

Let $M = (m_{ij})_{i,j=1}^{n}$ be an arbitrary nonnegative integer matrix and $A = \{a_1, ..., a_n\}$ be a set of colors. A coloring of vertices of a graph $G$ into colors from $A$ is called *perfect* with matrix $M$ if the number of vertices of a color $a_j$ incident to a vertex of a color $a_i$ does not depend on the vertex and equals to $m_{ij}$.

A coloring of a graph $G$ can be considered as a function

$$\varphi : V(G) \to A.$$

We consider perfect colorings of the graph $G(Z^2)$ that is an infinite rectangular grid. This graph is regular of degree 4. Each vertex of graph $G(Z^2)$ corresponds to a pair of integers, two vertices are adjacent if their pairs differ in one coordinate by unit, and the other coordinate is the same.

We say that a matrix $M$ is *possible*, if a perfect coloring of $G(Z^2)$ with matrix $M$ exists.

A perfect coloring $\varphi$ of $G(Z^2)$ is $(p, q)$-*periodic* if $\varphi(x + p, y + q) = \varphi(x, y)$ for any integers $x$, $y$. A perfect coloring that is $(p, p)$- and $(q, -q)$-periodic is called *periodic*. The existence of a periodic perfect coloring for any possible matrix is proved [1].

The main result is the following

**Theorem 1** *Every possible matrix of perfect colorings into three colors is equivalent to one of the following* 21 *matrices:*

*1.* $\begin{pmatrix} 0 & 0 & 4 \\ 0 & 0 & 4 \\ 1 & 3 & 0 \end{pmatrix}$ *2.* $\begin{pmatrix} 0 & 0 & 4 \\ 0 & 0 & 4 \\ 2 & 2 & 0 \end{pmatrix}$ *3.* $\begin{pmatrix} 0 & 2 & 2 \\ 2 & 0 & 2 \\ 2 & 2 & 0 \end{pmatrix}$ *4.* $\begin{pmatrix} 0 & 0 & 4 \\ 0 & 0 & 4 \\ 1 & 1 & 2 \end{pmatrix}$ *5.* $\begin{pmatrix} 0 & 1 & 3 \\ 1 & 0 & 3 \\ 1 & 1 & 2 \end{pmatrix}$ *6.* $\begin{pmatrix} 0 & 2 & 2 \\ 2 & 0 & 2 \\ 1 & 1 & 2 \end{pmatrix}$

*7.* $\begin{pmatrix} 0 & 2 & 2 \\ 4 & 0 & 0 \\ 2 & 0 & 2 \end{pmatrix}$ *8.* $\begin{pmatrix} 0 & 3 & 1 \\ 3 & 0 & 1 \\ 1 & 1 & 2 \end{pmatrix}$ *9.* $\begin{pmatrix} 0 & 2 & 2 \\ 1 & 1 & 2 \\ 1 & 2 & 1 \end{pmatrix}$ *10.* $\begin{pmatrix} 0 & 2 & 2 \\ 2 & 1 & 1 \\ 2 & 1 & 1 \end{pmatrix}$ *11.* $\begin{pmatrix} 0 & 4 & 0 \\ 1 & 1 & 2 \\ 0 & 2 & 2 \end{pmatrix}$ *12.* $\begin{pmatrix} 0 & 2 & 2 \\ 1 & 2 & 1 \\ 1 & 1 & 2 \end{pmatrix}$

*13.* $\begin{pmatrix} 0 & 2 & 2 \\ 2 & 2 & 0 \\ 2 & 0 & 2 \end{pmatrix}$ *14.* $\begin{pmatrix} 1 & 0 & 3 \\ 0 & 1 & 3 \\ 1 & 2 & 1 \end{pmatrix}$ *15.* $\begin{pmatrix} 1 & 0 & 3 \\ 0 & 1 & 3 \\ 1 & 1 & 2 \end{pmatrix}$ *16.* $\begin{pmatrix} 1 & 1 & 2 \\ 1 & 1 & 2 \\ 1 & 1 & 2 \end{pmatrix}$ *17.* $\begin{pmatrix} 1 & 2 & 1 \\ 2 & 1 & 1 \\ 1 & 1 & 2 \end{pmatrix}$ *18.* $\begin{pmatrix} 2 & 0 & 2 \\ 0 & 2 & 2 \\ 1 & 1 & 2 \end{pmatrix}$

*19.* $\begin{pmatrix} 2 & 1 & 1 \\ 1 & 2 & 1 \\ 1 & 1 & 2 \end{pmatrix}$ *20.* $\begin{pmatrix} 2 & 1 & 1 \\ 2 & 2 & 0 \\ 1 & 0 & 3 \end{pmatrix}$ *21.* $\begin{pmatrix} 2 & 1 & 1 \\ 1 & 3 & 0 \\ 1 & 0 & 3 \end{pmatrix}$

We also found that 5 of these matrices correspond to uncountably many perfect colorings, others correspond to finite set of colorings. Earlier a similar problem was solved for two colors [2].

## REFERENCES

1. Puzynina S. A. *Periodicity of perfect colorings of the infinite rectangular grid.* // Discrete analysis and operations research, 2004, 1:11, P. 79–92.[Russian]

2. Axenovich M. *On multiple coverings of the infinite rectangular grid with balls of constant radius.* // Discrete Math. 2003. V. 268. P. 31–49.

Puzynina Svetlana Aleksandrovna, Sobolev Institute of Mathematics,
pr. Akademika Koptyuga, 4, Novosibirsk, 630090, Russia,
e-mail: sveta_nsu@www.ngs.ru

# О РАЗБИЕНИЯХ $q$-ИЧНЫХ КОДОВ ХЕММИНГА НА НЕПЕРЕСЕКАЮЩИЕСЯ КОМПОНЕНТЫ

А. М. Романов

Найдены новые разбиения $q$-ичных кодов Хемминга на непересекающиеся компоненты, которые позволяют сдвигами компонент получать новые нелинейные совершенные $q$-ичные коды.

В $n$-мерном векторном пространстве $F_q^n$ над полем Галуа $GF(q)$ рассматривается $q$-ичный код Хемминга $H_k$ длины $n$, где $n = \frac{q^k-1}{q-1}$, $k \geq 2$, $q$ — простое число или степень простого числа. Пусть $R_i$ — подпространство, порожденное всеми векторами веса 3 кода $H_k$ с ненулевой $i$-й координатой. Всевозможные смежные классы $R_i + \mathbf{u}$ $(\mathbf{u} \in H_k)$ представляют собой совокупность всех *$i$-компонент* $q$-ичного кода Хемминга $H_k$.

Пусть $\lambda \in GF(q)$, $\lambda \neq 0$, $\mathbf{u} \in H_k$, $\mathbf{e}_i$ — базисный вектор, в котором $i$-я координата равна 1. Тогда при $k \geq 4$ множество $H'_k = (H_k \setminus (R_i + \mathbf{u})) \cup (R_i + \mathbf{u} + \lambda\mathbf{e}_i)$ является нелинейным совершенным $q$-ичным кодом длины $n$. Говорят, что код $H'_k$ получен из кода $H_k$ сдвигом компоненты $R_i + \mathbf{u}$.

**Теорема.** *Для любого $k \geq 3$ и любого $p$ такого, что $0 \leq p \leq k-3$, существует разбиение $q$-ичного кода Хемминга $H_k$ на $i_s$-компоненты $(1 \leq s \leq q^p)$, в котором при каждом $s$ число $i_s$-компонент равно $q^{\frac{n-1}{q}-k-p+1}$.*

Предложенные разбиения являются обобщением конструкций из [1, 2].

## ЛИТЕРАТУРА

1. 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.
2. 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.

Романов Александр Михайлович,
Институт математики им. С. Л. Соболева СО РАН,
пр. Академика Коптюга, 4, Новосибирск, 630090, Россия,
тел. (8-383-2) 33-38-69, e-mail: rom@math.nsc.ru

# ON TRANSITIVE CODES

F. I. Solov'eva

Transitive objects play an important role in coding theory, combinatorics, graph theory and group theory. Applying some well-known constructions (Vasil'ev's, Plotkin's and Mollard's) to known binary transitive codes of some lengths, see [1–3], it is possible to get infinite classes of transitive binary codes of greater lengths. Let $E^n$ be the set of all binary vectors of length $n$. It is well known that every isometry of $E^n$ is defined by a permutation $\pi$ on the $n$ coordinate positions and by adding a vector $v \in E^n$, i.e., for the automorphism group of $E^n$ it is true that $\mathrm{Aut}(E^n) = S_n \leftthreetimes E^n = \{(\pi, v) \mid \pi \in S_n, v \in E^n\}$, where $\leftthreetimes$ denotes a semidirect product. The *automorphism group* $\mathrm{Aut}(C)$ of any code $C$ of length $n$ consists of all the isometries of $E^n$ that transform the code into itself, i.e., $\mathrm{Aut}(C) = \{(\pi, v) \mid \pi(C) + v = C\}$. The set $\mathrm{Sym}(C) = \{\pi \in S_n \mid \pi(C) = C\}$ is called the *group of symmetries* of the code $C$. A code $C$ is said to be *transitive* if for every codeword $v \in C$ there exists a permutation $\pi_v \in S_n$ such that $(\pi_v, v) \in \mathrm{Aut}(C)$ and $\pi_v$ may not belong to the set $\mathrm{Sym}(C)$.

**Theorem 1.** *Let $C_1$ and $C_2$ be arbitrary binary transitive codes of length $n$ with code distance $d_1$ and $d_2$ respectively, such that for every automorphism $(\pi_y, y) \in \mathrm{Aut}(C_2)$ it holds $\pi_y \in \mathrm{Sym}(C_1)$. Then the Plotkin code $C^{2n} = \{(x, x+y) : x \in C_1, y \in C_2\}$ is a binary transitive code of length $2n$, size $|C_1| \times |C_2|$ and code distance $d = \min\{2d_1, d_2\}$.*

Let $C^r$ and $C^m$ be two perfect binary codes of length $r$ and $m$ respectively, where $r = 2^k - 1$, $m = 2^p - 1$. Let $x = (x_{11}, x_{12}, \ldots, x_{1m}, x_{21}, \ldots, x_{2m}, \ldots, x_{r1}, \ldots, x_{rm}) \in E^{rm}$. The generalized parity functions $p_1(x)$ and $p_2(x)$ are defined by $p_1(x) = (\sigma_1, \sigma_2, \ldots, \sigma_r) \in E^r$, $p_2(x) = (\sigma'_1, \sigma'_2, \ldots, \sigma'_m) \in E^m$, where $\sigma_i = \sum_{j=1}^{m} x_{ij}$ and $\sigma'_j = \sum_{i=1}^{r} x_{ij}$.

**Theorem 2.** *Let $C^r$ and $C^m$ be arbitrary perfect binary transitive codes of length $r$ and $m$ respectively. Then the Mollard code $C^n = \{(x, y + p_1(x), z + p_2(x)) : x \in E^{rm}, y \in C^r, z \in C^m\}$ is a perfect binary transitive code of length $n = rm + r + m$.*

It is easy to see that an extended code obtained by adding an overall parity check to a transitive code is transitive. Using Theorem 2, we get transitive Vasil'ev codes in the case $r = 1$. The dimension of the subspace spanned by a code $C$ is called the *rank* of the code $C$. The *kernel* of a code $C$ is the set of all codewords $x \in C$ such that $x + C = C$. Ranks and kernels of all these transitive codes can be easily found from ranks and kernels of starting transitive codes and used to obtain new transitive codes.

## REFERENCES

1. Borges J., Phelps K. T., Rifa J. K. *The rank and kernel of extended* 1*-perfect $Z_4$-linear and additive non-$Z_4$-linear codes* // IEEE Trans. on Inform. Theory. 2003. V 49. N 8. P. 2028-2034.

2. Krotov D. S. *$Z_4$-linear perfect codes* // Discrete Analysis and Operation Research. Ser. 1. 2000. V.7. N 4. P. 78–90 (in Russian).

3. Malyugin S. A. *On transitive perfect codes of length 15*, see present volume. P. 96

Solov'eva Faina Ivanovna, Sobolev Institute of Mathematics RAS,
pr. Akademika Koptyuga, 4, Novosibirsk, 630090, Russia;
phone: 8-3832-333788, fax: 8-3832-332598, e-mail: sol@math.nsc.ru

# THE NECESSARY AND SUFFICIENT CONDITION FOR A BINARY CODE TO BE A $Z_4$-LINEAR PREPARATA CODE

N. N. Tokareva

Codes with a group structure are the most important codes in the coding theory. The family of $Z_4$-linear codes have such property among extended binary Preparata codes (i.e., codes of length $4^m$, cardinality $2^{4^m-4m}$ with code distance 6). The first $Z_4$-linear Preparata code for every admissible length was discovered in [2], the reach class of such codes was constructed in [1]. It is an open problem to classify all such codes.

Let us consider the metric spaces $Z_2^{2N}$ and $Z_4^N$ with the *Hamming* and the *Lee* metrics respectively. The *Gray map* $\phi : Z_4 \to Z_2^2$ is defined as follows: $\phi(0) = 00$, $\phi(1) = 01$, $\phi(2) = 11$, $\phi(3) = 10$ and can be extended to the map $Z_4^N \to Z_2^{2N}$ in the natural way. It is well-known that the Gray map is an isometry of the metric space $Z_4^N$ onto $Z_2^{2N}$, see [2]. A binary code $C \subseteq Z_2^{2N}$ is called $Z_4$-*linear* if the code $\phi^{-1}(C)$ is a subgroup of the additive group of the ring $Z_4^N$.

Let $n = 2^{2m-1} - 1$, $m = 2, 3, \ldots$ For vectors from $Z_2^n$ we use the following notations: $e_0$ is the all-zero vector, $e_i$ is the vector with one only in the $i$th coordinate, $x * y$ is the vector $(x_1y_1, \ldots, x_ny_n)$ for any $x, y$ from $Z_2^n$. Let $H$ be a binary Hamming code of length $n$, i.e., a code of cardinality $2^{n-\log_2(n+1)}$ with code distance 3 that is a linear subspace of the space $Z_2^n$. Suppose $\lambda$ is a Boolean function such that $\lambda(y) = 0$ if and only if $wt(y) = 0, 3 (\mod 4)$, where $wt(y)$ is the Hamming weight of the vector $y \in Z_2^n$. Let $\varphi$ be a function from $H$ to the set $\{0, 1, \ldots, n\}$. With arbitrary vectors $x, y$ from $H$ we associate the following vectors of length $2(n + 1)$:

$\mathbf{x} = (x,\ |x|,\ x,\ |x|)$,

$\mathbf{y}_\varphi = (e_{\varphi(y)},\ \lambda(y) + |e_{\varphi(y)}|,\ y + e_{\varphi(y)},\ |y| + \lambda(y) + |e_{\varphi(y)}|)$.

**Theorem.** *A code $P$ of length $2(n + 1) = 4^m$ is a $Z_4$-linear extended Preparata code if and only if it can be represented in the form $P = \{\mathbf{x} + \mathbf{y}_\varphi \,|\, x, y \in H\}$ for some function $\varphi$ satisfying the following conditions*:

1. *it is true that $\varphi(e_0) = 0$;*
2. *for all $u$ and $v$ from $H$ the vector $u * v + e_{\varphi(u)} + e_{\varphi(v)} + e_{\varphi(u+v)}$ belongs to $H$;*
3. *for any $u = e_i + e_j + e_k \in H$ it should be $\varphi(u) \notin \{0, i, j, k\}$;*
4. *for any $u = e_i + e_j + e_k$ and $v = e_i + e_m + e_l$ from $H$ it is true that $\varphi(u + v) \notin \{0, i\}$.*

## REFERENCES

1. Calderbank A. R., Cameron P. J., Kantor W. M., Seidel J. J. *$Z_4$-Kerdock Codes, Orthogonal Spreads, and Extremal Euclidean Line-sets* // Proc. London Math. Soc. 1997. V. 75, P. 436–480.

2. Hammons A. R., Kumar P. V., Calderbank A. R., Sloane N. J. A., Solé P. *The $Z_4$-linearity of Kerdock, Preparata, Goethals, and Related Codes* // IEEE Trans. on Information Theory 1994. V. 40, P. 301–319.

Tokareva Natalia Nikolaevna,
Novosibirsk State University, ul. Pirogova 2, Novosibirsk, 630090, Russia;
e-mail: tokareva@ccfit.nsu.ru