Problems of Information Transmission, Vol. 41, No. 2, 2005, pp. 113–124. Translated from Problemy Peredachi Informatsii, No. 2, 2005, pp. 50–62.

CODING THEORY

Representation of $\mathbb{Z}_4$-Linear Preparata Codes Using Vector Fields[1]

N. N. Tokareva

Novosibirsk State University
toknn@ngs.ru

Received December 8, 2004; in final form, March 14, 2005

Abstract—A binary code is called $\mathbb{Z}_4$-linear if its quaternary Gray map preimage is linear. We show that the set of all quaternary linear Preparata codes of length $n = 2^m$, m odd, $m \geq 3$, is nothing more than the set of codes of the form $\mathcal{H}_{\lambda,\psi} + \mathcal{M}$ with

$$\mathcal{H}_{\lambda,\psi} = \{y + T_\lambda(y) + S_\psi(y) \mid y \in H^n\}, \quad \mathcal{M} = 2H^n,$$

where $T_\lambda(\cdot)$ and $S_\psi(\cdot)$ are vector fields of a special form defined over the binary extended linear Hamming code H^n of length n. An upper bound on the number of nonequivalent quaternary linear Preparata codes of length n is obtained, namely, $2^{n \log_2 n}$. A representation for binary Preparata codes contained in perfect Vasil'ev codes is suggested.

1. INTRODUCTION

All Preparata codes presently known are contained in perfect codes belonging to the class of Vasil'ev codes [1]. Indeed, the original Preparata code [2] and the series of codes [3,4] partition the linear Hamming code (which belongs to the class of Vasil'ev codes) into cosets. Any $\mathbb{Z}_4$-linear extended Preparata code [5,6] is also a subcode of a special $\mathbb{Z}_4$-linear Vasil'ev code (see Proposition 8). The structure of perfect Vasil'ev codes, as well as that of their minimal i-components, is well known. Using the relation between i-components of Preparata codes and perfect codes [7], one can get the general representation for Preparata codes contained in Vasil'ev codes (see Theorem 1).

$\mathbb{Z}_4$-linear Preparata codes are considered separately. To study them, it is convenient to pass to quaternary Gray map preimages of these codes. We show that the set of quaternary linear Preparata codes of length $n = 2^m$, m odd, $m \geq 3$, is nothing more than the set of codes of the form $\mathcal{H}_{\lambda,\psi} + \mathcal{M}$ with

$$\mathcal{H}_{\lambda,\psi} = \{y + T_\lambda(y) + S_\psi(y) \mid y \in H^n\}, \quad \mathcal{M} = 2H^n,$$

where $T_\lambda(\cdot)$ and $S_\psi(\cdot)$ are vector fields of a special form defined over the binary extended linear Hamming code H^n of length n (see Theorems 2 and 3). Using vector fields is convenient for the description of various combinatorial objects (see [8]). In particular, representation in terms of vector fields was proposed for some Preparata codes (see [9]). In [10], a relation between diameter perfect ternary codes and Preparata codes is established; the construction suggested in [10], using vector fields, resembles the construction of the present paper.

Sections 2 and 3 contain necessary definitions and facts for binary and quaternary codes. In Section 4, Preparata codes contained in Vasil'ev codes are studied. Section 5 is devoted to representation of quaternary linear Preparata codes using vector fields. Section 6 contains an example of such a representation for one known Preparata code.

[1] Supported in part by the Ministry of Education of the Russian Federation program "Development of the Scientific Potential of the Higher School," project no. 512.

2. BINARY AND QUATERNARY CODES

Consider the field $\mathbb{Z}_2$ of integers modulo 2 and the ring $\mathbb{Z}_4$ of integers modulo 4. The set $\mathbb{Z}_2^n$ consists of all *binary* vectors of length n, i.e.,

$$\mathbb{Z}_2^n = \{(x_1, \ldots, x_n) \mid x_i \in \mathbb{Z}_2,\ i = 1, \ldots, n\};$$

it is an n-dimensional vector space over $\mathbb{Z}_2$. Let $\oplus$ denote addition of binary vectors. The set $\mathbb{Z}_4^n$ consists of all *quaternary* vectors of length n, i.e.,

$$\mathbb{Z}_4^n = \{(x_1, \ldots, x_n) \mid x_i \in \mathbb{Z}_4,\ i = 1, \ldots, n\},$$

and is a module with addition operation $+$ over the ring $\mathbb{Z}_4$.

The *Hamming weight*, $w_H(\cdot)$, of a binary vector is the number of its nonzero coordinates. The *Hamming distance*, $d_H(\cdot\,,\cdot)$, between two binary vectors is the number of positions where they differ. The *Lee weight*, $w_L(\cdot)$, of a quaternary vector is the sum of weights of its coordinates, defined as $w_L(0) = 0$, $w_L(1) = w_L(3) = 1$, and $w_L(2) = 2$. The *Lee distance*, $d_L(\cdot\,,\cdot)$, between quaternary vectors x and y is defined as $d_L(x, y) = w_L(x - y)$.

The sets $\mathbb{Z}_2^n$ and $\mathbb{Z}_4^n$ are metric spaces with respect to the Hamming and Lee metric respectively. Elements of these sets will be referred to as vectors, or vertices. Note that any binary vector can be considered as a quaternary one. Concatenation of binary or quaternary vectors x and y is denoted by (x, y).

A *binary code of length* n is any subset of the metric space $\langle \mathbb{Z}_2^n, d_H \rangle$. A *quaternary code of length* n is any subset of the metric space $\langle \mathbb{Z}_4^n, d_L \rangle$. In what follows, we use notations from [5]. For binary codes we use capital letters C, P, H, R, M, etc.; for quaternary codes, calligraphic letters $\mathcal{C}$, $\mathcal{P}$, $\mathcal{H}$, $\mathcal{R}$, $\mathcal{M}$, etc.

Code parameters (n, M, d) of a binary, or quaternary, code are its *length*, n; *cardinality*, M; and minimum *distance*, d, between distinct codewords (in the corresponding metric). A code that contains the zero vector $\mathbf{0}$ is called *reduced*.

Standard maps β and γ from $\mathbb{Z}_4$ to $\mathbb{Z}_2$ are defined as

$\mathbb{Z}_4$	β	γ
0	0	0
1	0	1
2	1	1
3	1	0

and are coordinatewise extended to maps $\mathbb{Z}_4^n \to \mathbb{Z}_2^n$. The *Gray map* $\varphi\colon \mathbb{Z}_4^n \to \mathbb{Z}_2^{2n}$ is defined by

$$\varphi(x) = (\beta(x), \gamma(x)), \quad \text{for any } x \in \mathbb{Z}_4^n.$$

It is known [5] that φ is an isometry of the metric spaces $\langle \mathbb{Z}_4^n, d_L \rangle$ and $\langle \mathbb{Z}_2^{2n}, d_H \rangle$.

We denote the set of coordinates $\{1, 2, \ldots, n\}$ by I. For binary vectors x and y of length n, the vector $x * y$ is $(x_1 y_1, \ldots, x_n y_n)$. A vector x *precedes* a vector y (notation: $x \prec y$) if $x \neq y$ and $x_i \leq y_i$ for all $i \in I$, where $\leq$ is the standard order on $\mathbb{Z}_2$. By $|x|$ we denote the sum $x_1 \oplus \ldots \oplus x_n$. For quaternary vectors x and y, we define $x \prec y$ if $\varphi(x) \prec \varphi(y)$.

Consider the group S_n of permutations of order n and the group J_n of inversions on n coordinates (by an *inversion* of a quaternary vector, we mean the replacement of elements of the ring $\mathbb{Z}_4$ in some coordinates by the inverse elements; i.e., 0 is replaced by 0, 1 by 3, 2 by 2, and 3 by 1). Note that the groups J_n and $\mathbb{Z}_2^n$ are isomorphic. Two binary codes, C and C', of length n are *equivalent*

if there exist a vector $x \in \mathbb{Z}_2^n$ and a permutation $\pi \in S_n$ such that $C = \pi(C') \oplus x$. Two quaternary codes, $\mathcal{C}$ and $\mathcal{C}'$, of length n are *equivalent* if there exist a vector $x \in \mathbb{Z}_4^n$, a permutation $\pi \in S_n$, and an inversion $\tau \in J_n$ such that $C = \pi(\tau(C')) + x$. A binary (quaternary) code of length n is *linear* if it is a subgroup of the additive group of the field $\mathbb{Z}_2^n$ (the ring $\mathbb{Z}_4^n$). A binary code is called $\mathbb{Z}_4$-*linear* if there exists an equivalent code C such that its preimage $\varphi^{-1}(C)$ is linear.

3. AUXILIARY DEFINITIONS AND STATEMENTS

3.1. Notion of an $\{i, j\}$-Component

Let us give some definitions for extended binary codes (in [11, 12], analogous definitions were introduced for codes with odd distances).

By e_i we denote a vector of length n with one in the ith coordinate and zeros in the others. A subset M of a binary code C is called an $\{i, j\}$-*component* of the code for two different coordinates i and j if the codes C and $C' = (C \setminus M) \cup (M \oplus e_i \oplus e_j)$ have the same code parameters. Let two vectors of a binary code be at the minimum code distance from each other, and let they differ in coordinates i and j. Such code vectors are called $\{i, j\}$-*close*. Any set of codewords which is closed with respect to inclusion of $\{i, j\}$-close vertices is an $\{i, j\}$-component. Consider a graph on the set of code vertices where $\{i, j\}$-close vertices are joined by edges. Each of its connected components uniquely corresponds to a minimal (i.e., indivisible into smaller ones) $\{i, j\}$-component of the code; it is called the *characteristic graph* of this $\{i, j\}$-component. The characteristic graph G^R of a component R is a metric space with the natural metric: the distance $d_G(\cdot\,, \cdot)$ between vertices is the length of the shortest path joining them.

3.2. Perfect Codes and Preparata Codes

A subset of a metric space is called a *perfect code with distance* 3 (briefly, a *perfect* code) if the distance between any two of its elements is at least 3 and balls of radius 1 centered at code vertices are disjoint and cover the whole space. It is well known that binary perfect codes exist only for lengths $n = 2^m - 1$, $m \geq 2$, and are of cardinality $M = 2^n/(n + 1)$. Among them, only one code up to equivalence is linear, namely, the *Hamming code*. A binary code of maximal cardinality with distance 5 and of length $n = 2^{m+1} - 1$, m odd, $m \geq 3$, is called a *Preparata code*; its cardinality, M, equals $2^{n+1}/(n + 1)^2$. For an extended binary perfect code C, we call its Gray map preimage $\varphi^{-1}(C)$ a *quaternary perfect* code (omitting the term "extended"). We call the preimage $\varphi^{-1}(P)$ of an extended binary Preparata code P a *quaternary Preparata code*. It follows from the definitions that a quaternary perfect code has the parameters ($n = 2^m$, $M = 4^n/4n$, $d = 4$) for any integer $m \geq 1$, and a quaternary Preparata code has the parameters ($n = 2^m$, $M = 4^n/4n^2$, $d = 6$) for an odd integer $m \geq 3$. We have the following result.

Proposition 1 (see [13]). *Each Preparata code is contained in some perfect code, which is unique.*

For a Preparata code P, we denote the corresponding perfect code by $C(P)$ and in what follows call it the *base* code. We need the following fact.

Proposition 2 (see [14]). *For any binary Preparata code P of length n, each vertex of the code $C(P) \setminus P$ is at distance 3 from precisely $n/3$ vertices of P.*

Note that the set of vectors of weight 4 of an extended binary perfect code C of length n forms a *Steiner quadruple system* of order n (see [14]). We denote this set by $SQS(C)$.

Proposition 3 (see [15, Glagolev's lemma]). *A basis of an extended Hamming code H^n of length n can be chosen among vectors of $SQS(H^n)$.*

4. PREPARATA CODES CONTAINED IN VASIL'EV CODES

In this section we study general properties of Preparata codes with a base perfect Vasil'ev code. Only binary codes will be considered.

Let us give a construction of widely known extended perfect Vasil'ev codes [1] using their representation proposed in [16]. Let $n = 2^m$, $m \geq 2$; let i be a fixed coordinate from I. The set E_0^n consists of all even-weight binary vectors of length n. Let us be given an arbitrary extended reduced perfect code C^n of length n and a function $\lambda\colon C^n \to \{0,1\}$ with $\lambda(\mathbf{0}) = 0$. Consider the sets

$$R = \{(x,x) \mid x \in E_0^n\},$$
$$C_\lambda = \{(\lambda(y)e_i, \lambda(y)e_i \oplus y) \mid y \in C^n\}.$$

If we take for C^n the extended linear Hamming code H^n, we denote the set C_λ by H_λ. The set

$$V_C^\lambda = C_\lambda \oplus R$$

is an extended perfect *Vasil'ev code* of length $2n$ (see [16]). By R^y denote the coset of R corresponding to a vector y from C^n, i.e.,

$$R^y = R \oplus v^y, \quad \text{where} \quad v^y = (\lambda(y)e_i, \lambda(y)e_i \oplus y).$$

It is easily seen that the set $R^{\mathbf{0}}$ coincides with R. From the definition of the code V_C^λ it immediately follows that each set R^y is its minimal $\{i, n+i\}$-component.

Proposition 4. *For any vector y from C^n, the metric spaces $\langle G^{R^y}, d_G\rangle$ and $\langle \mathbb{Z}_2^{n-1}, d_H\rangle$ are isometric.*

Proof. It suffices to show that the spaces $\langle G^R, d_G\rangle$ and $\langle \mathbb{Z}_2^{n-1}, d_H\rangle$ are isometric. Define a map $f\colon R \to \mathbb{Z}_2^{n-1}$ as follows: for $x \in E_0^n$ let $f((x,x)) = \widehat{x}$, where $\widehat{x}$ is the projection of x with respect to the ith coordinate. It is easily checked that f is a one-to-one map. Let us show that it preserves distance 1. Let $d_G((x^1,x^1),(x^2,x^2)) = 1$ for vectors $x^1, x^2 \in E_0^n$; then (x^1,x^1) and (x^2,x^2) are $\{i, n+i\}$-close vectors, i.e., differ in positions i and $n+i$, and the distance $d_H((x^1,x^1),(x^2,x^2))$ equals 4. Hence we get $d_H(x^1,x^2) = 2$, and therefore $d_H(\widehat{x}^1,\widehat{x}^2) = 1$. Isometries $f_y\colon R^y \to \mathbb{Z}_2^{n-1}$ are defined similarly: $f_y((x,x) \oplus v^y) = \widehat{x}$. $\triangle$

In [7], the following fact was proved, which we formulate in terms of extended codes.

Proposition 5. *Let P be an extended Preparata code. Then, for any $\{i,j\}$-component R of its base extended perfect code $C(P)$, the set $P \cap R$ is a perfect code with distance 3 in the metric space $\langle G^R, d_G\rangle$.*

We have the following theorem.

Theorem 1. *Any binary extended Preparata code P contained in the extended perfect Vasil'ev code*

$$V_C^\lambda = \{(x \oplus \lambda(y)e_i, x \oplus y \oplus \lambda(y)e_i) \mid x \in E_0^n,\ y \in C^n\}$$

is uniquely represented in the form

$$P = \{(x \oplus \lambda(y)e_i, x \oplus y \oplus \lambda(y)e_i) \mid x \in C_y^n,\ y \in C^n\},$$

where for each $y \in C^n$ there is a specially chosen extended perfect code C_y^n of length $n = 2^m$, m odd, $m \geq 3$.

Proof. Let P be contained in V_C^λ. For any vector $y \in C^n$, denote by M^y the set $P \cap R^y$. Since the code V_C^λ is divided into disjoint $\{i, n+i\}$-components R^y, we have

$$P = P \cap V_C^\lambda = P \cap \left(\bigcup_{y \in C^n} R^y\right) = \bigcup_{y \in C^n} (P \cap R^y) = \bigcup_{y \in C^n} M^y.$$

By Proposition 5, the set M^y is a perfect code in the space $\langle G^{R^y}, d_G\rangle$. Let $f_y\colon R^y \to \mathbb{Z}_2^{n-1}$ be the isometry defined in Proposition 4. Then $f_y(M^y)$ is a perfect code in the space $\langle \mathbb{Z}_2^{n-1}, d_H\rangle$. Denote by C_y^n the extended perfect code of length n such that puncturing of its ith coordinate yields the code $f_y(M^y)$. Then we obviously have

$$M^y = v^y \oplus \{(x,x) \mid x \in C_y^n\};$$

substituting here the vector

$$v^y = (\lambda(y)e_i, \lambda(y)e_i \oplus y),$$

we get the desired representation of P. $\triangle$

All Preparata codes presently known are contained in perfect Vasil'ev code and can therefore be represented via the construction of Theorem 1. For instance, for $\lambda(\cdot) \equiv 0$ and $C^n = H^n$, the Vasil'ev code V_H^λ is a linear extended Hamming code. It contains a series of Preparata codes [3, 4]. In Section 5 we show that an arbitrary $\mathbb{Z}_4$-linear extended Preparata code is contained in a unique (up to equivalence) Vasil'ev code with a special function λ. For this code, the codes C^n and C_y^n in terms of Theorem 1 are cosets of an extended linear Hamming code H^n. The choice of cosets is controlled by a function ψ. Below, as a particular case of Theorem 1, we give a representation for $\mathbb{Z}_4$-linear extended Preparata codes and establish a one-to-one correspondence between all such codes and special *shift functions* φ, defined on blocks $SQS(H^n)$. We show that constructing a shift function is equivalent to constructing a $\mathbb{Z}_4$-linear extended Preparata code.

5. LINEAR QUATERNARY PREPARATA CODES

5.1. Base Perfect Code

Consider an arbitrary linear quaternary Preparata code $\mathcal{P}$ of length $n = 2^m$, m odd, $m \geq 3$, and its base quaternary perfect code $\mathcal{C}(\mathcal{P})$. Recall that the *rank* of a set of binary vectors is the dimension of the linear subspace spanned by these vectors. By the rank of a set of quaternary vectors, we call the rank of its Gray map image.

Proposition 6 (see [17]). *The following statements hold true*:

(i) *The rank of any Preparata code equals the rank of the ambient perfect code*;

(ii) *The rank of any quaternary linear Preparata code of length $n = 2^m$ equals $2^{m+1} - m - 1$ for $m > 3$, and equals 11 for $m = 3$*;

(iii) *For an arbitrary quaternary linear Preparata code $\mathcal{P}$, its base quaternary code $\mathcal{C}(\mathcal{P})$ is also linear.*

Proposition 7 (see [18, 19]). *The number of pairwise nonequivalent quaternary linear perfect codes of length $n = 2^m$, $m \geq 3$, is $\lfloor m/2 \rfloor + 1$. All these codes are of different ranks.*

Let an extended binary linear Hamming code H^n and a coordinate $i \in I$ be fixed. To present the construction of a quaternary Vasi'ev code, it is convenient to assign to a function $\lambda\colon H^n \to \{0,1\}$ a quaternary vector field over H^n,

$$T_\lambda\colon H^n \to \{\mathbf{0}, 2e_i\},$$

according to the rule

$$T_\lambda(y) = 2\lambda(y)e_i \quad \text{for } y \in H^n.$$

The quaternary sets

$$\mathcal{R} = 2E_0^n, \qquad \mathcal{H}_\lambda = \{y + T_\lambda(y) \mid y \in H^n\}$$

are the Gray map preimages of the binary sets R and H_λ.

The following result is due to D.S. Krotov.

Proposition 8 (see [20]). *Any quaternary linear Preparata code is contained in a quaternary perfect code equivalent to the code $\mathcal{V}_{\mathcal{H}}^{\lambda} = \mathcal{H}_{\lambda} + \mathcal{R}$ with λ of the form*

$$\lambda(y) = \begin{cases} 0 & \text{if } w_H(y) \equiv 0 \pmod 4, \\ 1 & \text{if } w_H(y) \equiv 2 \pmod 4, \end{cases} \qquad \text{for } y \in H^n.$$

Proof. It follows from Proposition 6 that the code $\mathcal{C}(\mathcal{P})$ is linear and is of rank $2^{m+1} - m - 1$ for $m > 3$, or 11 for $m = 3$. By Proposition 7, such a code is unique up to equivalence. Let us show that this code is $\mathcal{V}_{\mathcal{H}}^{\lambda}$ with the above function λ. The definition of the map φ obviously implies the equality

$$\varphi(x + 2y) = \varphi(x) \oplus \varphi(2y) \quad \text{for any } x, y \in \mathbb{Z}_4^n. \tag{1}$$

Then we have

$$\mathcal{V}_{\mathcal{H}}^{\lambda} = \varphi^{-1}(H_{\lambda}) + \varphi^{-1}(R) = \varphi^{-1}(H_{\lambda} \oplus R) = \varphi^{-1}(V_H^{\lambda});$$

i.e., $\mathcal{V}_{\mathcal{H}}^{\lambda}$ is the Gray map preimage of the extended binary perfect Vasil'ev code. It is easily checked that its rank equals $2^{m+1} - m - 1$ for $m > 3$, and equals 11 for $m = 3$ (for details, see [21,22]). Let us show that the sum $v^1 + v^2$ of any two vectors v^1 and v^2 of the perfect code $\mathcal{V}_{\mathcal{H}}^{\lambda}$ also belongs to the code. Let

$$v^k = y^k + T_{\lambda}(y^k) + 2x^k, \quad \text{where} \quad x^k \in E_0^n, \quad y^k \in H^n, \quad k = 1, 2.$$

Let us use the equalities

$$y^1 + y^2 = (y^1 \oplus y^2) + 2y^1 * y^2, \tag{2}$$

$$\lambda(y^1 \oplus y^2) = \lambda(y^1) \oplus \lambda(y^2) \oplus |y^1 * y^2|; \tag{3}$$

the first equality here is obvious, and the second is easily obtained from the identities

$$w_H(y^1 \oplus y^2) = w_H(y^1) + w_H(y^2) - 2w_H(y^1 * y^2),$$
$$w_H(y) \equiv 2\lambda(y) \pmod 4, \quad \text{for any } y \text{ in } H^n.$$

Then we have

$$\begin{aligned} v^1 + v^2 &= (y^1 \oplus y^2) + T_{\lambda}(y^1) + T_{\lambda}(y^2) + 2(y^1 * y^2 \oplus x^1 \oplus x^2) \\ &= (y^1 \oplus y^2) + T_{\lambda}(y^1 \oplus y^2) + 2(y^1 * y^2 \oplus x^1 \oplus x^2 \oplus |y^1 * y^2| e_i), \end{aligned}$$

whence follows the equality $v^1 + v^2 = y + T_{\lambda}(y) + 2x$ for some $x \in E_0^n$ and $y \in H^n$. Therefore, the vector $v^1 + v^2$ belongs to $\mathcal{V}_{\mathcal{H}}^{\lambda}$. Thus, the linearity, code parameters, and the corresponding rank of $\mathcal{V}_{\mathcal{H}}^{\lambda}$ are shown. $\triangle$

Throughout what follows, $\lambda(\cdot)$ is the function defined in Proposition 8. Without loss of generality we may assume that the code $\mathcal{P}$ is contained direct in the quaternary Vasil'ev code $\mathcal{V}_{\mathcal{H}}^{\lambda}$.

5.2. Representation of Quaternary Linear Preparata Codes

The Gray map preimage of a quaternary linear Preparata code has a representation given in Theorem 1. The code C^n is H^n. For codes C_y^n, choose cosets of H^n with the help of a function $\psi\colon H^n \to I$. It is convenient to associate with ψ a quaternary vector field over H^n,

$$S_{\psi}\colon H^n \to \{2e_i + 2e_1, \ldots, 2e_i + 2e_n\},$$

according to the rule

$$S_{\psi}(y) = 2e_i + 2e_{\psi(y)} \quad \text{for } y \in H^n.$$

Note that the vector $S_{\psi}(y)$ is contained in $\mathcal{R}$. Consider the quaternary sets

$$\mathcal{M} = 2H^n, \qquad \mathcal{H}_{\lambda,\psi} = \{y + T_{\lambda}(y) + S_{\psi}(y) \mid y \in H^n\}.$$

Theorem 2. *An arbitrary quaternary linear Preparata code has a unique representation in the form $\mathcal{P} = \mathcal{H}_{\lambda,\psi} + \mathcal{M}$ for some extended linear Hamming code H^n and a function $\psi\colon H^n \to I$.*

Proof. It follows from Proposition 8 that each code $\mathcal{P}$ is contained in the code

$$\mathcal{V}^{\lambda}_{\mathcal{H}} = \bigcup_{y\in H^n} (y + T_\lambda(y) + \mathcal{R}),$$

and therefore

$$\mathcal{P} = \bigcup_{y\in H^n} (\mathcal{P} \cap (y + T_\lambda(y) + \mathcal{R})).$$

Let us show that for any y in H^n we can uniquely define $S_\psi(y)$ as the least-weight vector such that $y+T_\lambda(y)+S_\psi(y)$ belongs to $\mathcal{P}$. To this end, define ψ as follows. If the vector $y+T_\lambda(y)$ is contained in $\mathcal{P}$, put $\psi(y) = i$; then $S_\psi(y) = \mathbf{0}$. Let $y + T_\lambda(y)$ be contained in $\mathcal{C}(\mathcal{P}) \setminus \mathcal{P}$. It follows from Proposition 2 that there exists a unique binary vector v of length $2n$, of weight 4, with nonzero coordinates i and $n + i$ such that the vector $\varphi(y + T_\lambda(y)) \oplus v$ belongs to $\varphi(\mathcal{P})$. The preimage $\varphi^{-1}(v)$ contains 2 in the ith coordinate. Since the Gray map is isometric, its weight is 4. From the definition of $\mathcal{V}^{\lambda}_{\mathcal{H}}$ it follows that the vector $\varphi^{-1}(v)$ is of the form $2e_i + 2e_j$ for some coordinate j distinct from i. Put $\psi(y) = j$; then $S_\psi(y) = \varphi^{-1}(v)$. Using (1), we get

$$\varphi(y + T_\lambda(y)) \oplus \varphi(S_\psi(y)) = \varphi(y + T_\lambda(y) + S_\psi(y)),$$

and therefore the vector $y + T_\lambda(y) + S_\psi(y)$ is contained in $\mathcal{P}$ for any y in H^n.

Since the vectors $y+T_\lambda(y)+S_\psi(y)$ and $S_\psi(y)$ belong to linear codes $\mathcal{P}$ and $\mathcal{R}$ respectively, for y in H^n we have

$$\begin{aligned}\mathcal{P} \cap (y + T_\lambda(y) + \mathcal{R}) &= (y + T_\lambda(y) + S_\psi(y) + \mathcal{P}) \cap (y + T_\lambda(y) + S_\psi(y) + S_\psi(y) + \mathcal{R})\\ &= y + T_\lambda(y) + S_\psi(y) + (\mathcal{P} \cap (S_\psi(y) + \mathcal{R}))\\ &= y + T_\lambda(y) + S_\psi(y) + (\mathcal{P} \cap \mathcal{R}).\end{aligned}$$

Then

$$\mathcal{P} = \bigcup_{y\in H^n} (y + T_\lambda(y) + S_\psi(y) + (\mathcal{P} \cap \mathcal{R})).$$

It remains to show that the sets $\mathcal{P} \cap \mathcal{R}$ and $\mathcal{M}$ coincide. Indeed, from Theorem 1 it follows that they are of the same cardinality, and the obvious inclusions $\mathcal{M} \subset \mathcal{R}$ and $\mathcal{M} = 2\mathcal{P} \subset \mathcal{P}$ imply the inclusion $\mathcal{M} \subseteq \mathcal{P} \cap \mathcal{R}$. $\triangle$

Proposition 9. *A quaternary code $\mathcal{H}_{\lambda,\psi} + \mathcal{M}$ is linear if and only if for any y^1 and y^2 in H^n the function ψ satisfies the condition*

$$S_\psi(y^1) + S_\psi(y^2) + S_\psi(y^1 \oplus y^2) + 2\, y^1 * y^2 + 2\, |y^1 * y^2|\, e_i \in \mathcal{M}. \tag{4}$$

Proof. Consider two arbitrary code vectors

$$v^k = y^k + T_\lambda(y^k) + S_\psi(y^k) + 2x^k, \quad \text{where} \quad x^k, y^k \in H^n, \quad k = 1, 2.$$

Let us determine a condition for their sum $v^1 + v^2$ to belong to the code. Using (2) and (3), we get

$$\begin{aligned}v^1 + v^2 &= (y^1 \oplus y^2) + T_\lambda(y^1) + T_\lambda(y^2) + S_\psi(y^1) + S_\psi(y^2) + (2\, y^1 * y^2 + 2x^1 + 2x^2)\\ &= (y^1 \oplus y^2) + T_\lambda(y^1 \oplus y^2) + S_\psi(y^1 \oplus y^2) + (S_\psi(y^1) + S_\psi(y^2) + S_\psi(y^1 \oplus y^2)\\ &\quad + 2\, y^1 * y^2 + 2\, |y^1 * y^2|\, e_i + 2x^1 + 2x^2).\end{aligned}$$

Hence, $v^1 + v^2$ is a code vector if and only if the vector $S_\psi(y^1) + S_\psi(y^2) + S_\psi(y^1 \oplus y^2) + 2\, y^1 * y^2 + 2\, |y^1 * y^2|\, e_i$ belongs to $\mathcal{M}$. $\triangle$

Note that not every quaternary linear code $\mathcal{H}_{\lambda,\psi}+\mathcal{M}$ is a Preparata code.

Proposition 10. *A quaternary linear code $\mathcal{H}_{\lambda,\psi}+\mathcal{M}$ is a Preparata code if and only if, for any $y^1, y^2 \in SQS(H^n)$ such that $y^1 \oplus y^2 \in SQS(H^n)$, the function ψ satisfies the following conditions:*

$$\begin{aligned} &1.\ \ S_\psi(y^1) \neq \mathbf{0};\\ &2.\ \ S_\psi(y^1) \not\prec 2y^1;\\ &3.\ \ S_\psi(y^1 \oplus y^2) \neq 2y^1 * y^2. \end{aligned} \tag{5}$$

Proof. Let us verify that these conditions are necessary and sufficient for the code distance of $\mathcal{H}_{\lambda,\psi}+\mathcal{M}$ to be 6.

The necessity is checked directly. The weight of any code vector

$$v = y + T_\lambda(y) + S_\psi(y) + 2x, \quad \text{where} \quad x \in H^n, \quad y \in SQS(H^n),$$

is at least 6. Note that by the definition of the vector field T_λ we have $T_\lambda(y) = \mathbf{0}$. Then, if $S_\psi(y) = \mathbf{0}$ or $S_\psi(y) \prec 2y$, for $x = \mathbf{0}$ we have $w_L(v) = 4$, a contradiction. If $S_\psi(y) = 2y^1 * y^2$ for some $y^1, y^2 \in SQS(H^n)$ such that $y = y^1 \oplus y^2$, then for $x = y^1$ we also get $w_L(v) = 4$.

Let us check the sufficiency of conditions 1–3. Since the code $\mathcal{H}_{\lambda,\psi}+\mathcal{M}$ is linear, it suffices to show that the minimum nonzero weight of its code vectors is 6. An arbitrary code vector

$$v = y + T_\lambda(y) + S_\psi(y) + 2x, \quad \text{where} \quad x, y \in H^n,$$

has an even weight. We have

$$w_L(v) \geq w_L(y).$$

Therefore, we may in the sequel restrict ourselves to the cases $w_L(y) = 0$ and $w_L(y) = 4$; in each of these cases, we have $T_\lambda(y) = \mathbf{0}$. One easily verifies the inequality

$$w_L(v) \geq w_L(x).$$

Indeed, if $w_L(y) = 0$, or if $w_L(y) = 4$ and $x = y$, the inequality is obvious. If $w_L(y) = 4$ and $x \neq y$, we have

$$w_L(v) \geq w_L(y + 2x) - 4 = w_L(y) + 2w_L(x) - 2w_L(x * y) - 4 = w_L(x) + w_L(x \oplus y) - 4 \geq w_L(x).$$

Therefore, we shall only consider vectors x with $w_L(x) \leq 4$. Thus, we have to verify the code distance in the following cases.

Case 1. If $w_L(x) = 0$ and $w_L(y) = 0$, then v is the zero vector.

Case 2. For $w_L(x) = 4$ and $w_L(y) = 0$, we have $w_L(v) = 8$.

Case 3. For $w_L(x) = 0$ and $w_L(y) = 4$, conditions 1 and 2 imply $w_L(v) \geq 6$.

Case 4. Let $w_L(x) = 4$ and $w_L(y) = 4$. If $x = y$, then, similarly to Case 3, we have $w_L(v) \geq 6$. For $x \neq y$ let us use the inequality $w_L(v) \geq 4$. Assume that $w_L(v) = 4$. Then the weight-4 vectors x and $x \oplus y$ satisfy $S_\psi(y) = 2(x * (x \oplus y))$, and therefore condition 3 is violated. Thus, since the weight $w_L(x \oplus y)$ is even, we have $w_L(v) \geq 6$. $\triangle$

Propositions 9 and 10 imply the following result.

Corollary 1. *A quaternary code $\mathcal{H}_{\lambda,\psi}+\mathcal{M}$ is a linear Preparata code if and only if ψ satisfies conditions* (4) *and* (5).

Proposition 11. *Let a basis of a linear code H^n be fixed. Then an arbitrary collection of values of ψ on the basis uniquely determines ψ so that it satisfies condition* (4).

Proof. Let D be the set consisting of all vectors of H^n where values of ψ are already defined. Initially, D contains basis vectors only. Let us extend D to H^n with the help of condition (4). Using the fact that the vector $e_{\psi(y^1)} \oplus e_{\psi(y^2)} \oplus e_{\psi(y^1 \oplus y^2)} \oplus y^1 * y^2 \oplus (|y^1 * y^2| \oplus 1)e_i$ belongs to H^n for any vectors $y^1, y^2 \in D$, we uniquely define $\psi(y^1 \oplus y^2)$. Indeed, the vector $e_{\psi(y^1)} \oplus e_{\psi(y^2)} \oplus y^1 * y^2$ upon puncturing the ith coordinate in H^n will be at distance at most 1 from some codeword. If the distance is 1, let $\psi(y^1 \oplus y^2)$ indicate the direction towards this codeword. If the distance is 0, put $\psi(y^1 \oplus y^2) = i$. Add the vector $y^1 \oplus y^2$ to the set D. Proceeding in this way, we uniquely extend ψ to the whole code H^n. $\triangle$

5.3. Quaternary Linear Preparata Codes and Translation Functions

For a fixed coordinate $i \in I$ and a binary extended Hamming code H^n, let a function $\psi\colon H^n \to I$ satisfy conditions (4) and (5). From Propositions 3 and 11 it follows that ψ is uniquely reconstructed from its values on the set of weight-4 vectors of H^n. Therefore, it is reasonable to consider the restriction φ of ψ onto $SQS(H^n)$, which we call a *shift function*. Let us substitute the expressions for $T_\lambda(\cdot)$ and $S_\psi(\cdot)$ into (4) and (5). Then we have an equivalent definition for φ which follows.

A function $\varphi\colon SQS(H^n) \to I \setminus \{i\}$ is a *shift function* if, for any y^1, y^2 in $SQS(H^n)$ such that $y^1 \oplus y^2$ belongs to $SQS(H^n)$, the following conditions are satisfied:

1. $e_i \oplus e_{\varphi(y^1)} \not\prec y^1$;
2. $e_i \oplus e_{\varphi(y^1 \oplus y^2)} \neq y^1 * y^2$;
3. $e_i \oplus e_{\varphi(y^1)} \oplus e_{\varphi(y^2)} \oplus e_{\varphi(y^1 \oplus y^2)} \oplus y^1 * y^2 \in H^n$.

Theorem 3. *For any coordinate i there exists a one-to-one correspondence between the set of all different quaternary linear Preparata codes of length n and the set of all pairs (H^n, φ), where H^n is a binary extended linear Hamming code of length n, and $\varphi\colon SQS(H^n) \to I \setminus \{i\}$ is a shift function.*

Proof. According to Theorem 2 and Corollary 1, the set of all quaternary linear Preparata codes of length n is covered by codes of the form $\mathcal{H}_{\lambda,\psi} + \mathcal{M}$, where H^n is an extended Hamming code and ψ satisfies conditions (4) and (5). For a fixed H^n, there is a one-to-one correspondence between the set of such functions ψ and the set of shift functions φ. Then to an arbitrary linear quaternary Preparata code we uniquely assign a pair (H^n, φ).

It remains to show that different pairs (H_1^n, φ_1) and (H_2^n, φ_2) correspond to different Preparata codes $\mathcal{P}_1$ and $\mathcal{P}_2$. If we have $H_1^n = H_2^n$ and $\varphi_1 \neq \varphi_2$, then the codes $\mathcal{P}_1$ and $\mathcal{P}_2$ are obviously different. If $H_1^n \neq H_2^n$, then, due to the equalities $2\mathcal{P}_1 = 2H_1^n$ and $2\mathcal{P}_2 = 2H_2^n$, the codes $\mathcal{P}_1$ and $\mathcal{P}_2$ are also different. $\triangle$

Corollary 2. *For the number of nonequivalent quaternary linear Preparata codes of length n we have an upper bound $2^{n \log_2 n}$.*

Proof. By Proposition 11, the number of different shift functions for a fixed extended Hamming code and fixed coordinate i is at most $(n - 1 - \log_2 n)^{n-1}$. $\triangle$

6. EXAMPLE OF DESCRIPTION OF ONE QUATERNARY LINEAR PREPARATA CODE USING A TRANSLATION FUNCTION

Let us present a construction of a known quaternary linear Preparata code [5] and determine the pair (H^n, φ) corresponding to it according to Theorem 3.

With the help of the standard map $\bar{}\colon \mathbb{Z}_4 \to \mathbb{Z}_2$ given by the rule $\overline{0} = \overline{2} = 0$ and $\overline{1} = \overline{3} = 1$ (see [23]), define the ring homomorphism

$$\bar{}\colon \mathbb{Z}_4[X] \to \mathbb{Z}_2[X]$$

which takes a polynomial $a_0+a_1X+\ldots+a_nX^n$ to $\overline{a}_0+\overline{a}_1X+\ldots+\overline{a}_nX^n$. For any natural number m there exists a reduced polynomial $h(X)\in\mathbb{Z}_4[X]$ of degree m such that $h(X)$ divides $X^{2^m-1}-1$ in $\mathbb{Z}_4[X]$ and $\overline{h}(X)$ is a primitive polynomial of degree m in $\mathbb{Z}_2[X]$. Let $(h(X))$ denote the ideal generated by $h(X)$. Then the quotient ring $\mathbb{Z}_4[X]/(h(X))$ is the Galois ring $GR(4^m)$ and coincides with the ring $\mathbb{Z}_4[\xi]$, where $\xi=X+(h(X))$. Note that ξ is a root of $h(X)$. Consider the homomorphism

$$^-\colon \mathbb{Z}_4[X]/(h(X))\to\mathbb{Z}_2[X]/(\overline{h}(X)).$$

Then the element $\overline{\xi}$ equals $X+(\overline{h}(X))$ and is a root of the primitive polynomial $\overline{h}(X)$. The ring $\mathbb{Z}_2[\overline{\xi}]$ is the Galois field $GF(2^m)$. Thus, the map

$$^-\colon \mathbb{Z}_4[\xi]\to\mathbb{Z}_2[\overline{\xi}]$$

defines a homomorphism, which takes $a_0+a_1\xi+\ldots+a_n\xi^{m-1}$ to $\overline{a}_0+\overline{a}_1\overline{\xi}+\ldots+\overline{a}_n\overline{\xi}^{m-1}$ (see [23, Chapter 6]).

An arbitrary element of $GR(4^m)$ is uniquely represented in the form

$$a+2b\quad\text{for } a,b\in\mathcal{T},\quad\text{where } \mathcal{T}=\{0,1,\xi,\xi^2,\ldots,\xi^{2^m-2}\}.$$

The quaternary linear Preparata code $\mathcal{P}(m)$ of length $n=2^m$, m odd, $m\ge 3$, is defined by the parity-check matrix

$$\begin{pmatrix}1&1&1&1&\ldots&1\\0&1&\xi&\xi^2&\ldots&\xi^{n-2}\end{pmatrix}.$$

The base quaternary Vasil'ev code $\mathcal{V}^{\lambda}_{\mathcal{H}}$ has the parity-check matrix

$$\begin{pmatrix}1&1&1&1&\ldots&1\\0&2&2\xi&2\xi^2&\ldots&2\xi^{n-2}\end{pmatrix}.$$

By Theorem 2, to $\mathcal{P}(m)$ corresponds a binary extended linear Hamming code H^n, which is uniquely determined by the equality $2\mathcal{P}=2H^n$. It has the parity-check matrix

$$\begin{pmatrix}1&1&1&1&\ldots&1\\0&1&\overline{\xi}&\overline{\xi}^2&\ldots&\overline{\xi}^{n-2}\end{pmatrix}.$$

Let the coordinates be enumerated as follows:

$$I=\{\infty,0,1,2,\ldots,n-2\}.$$

Let us assume that $\xi^{\infty}=0$. Then we easily establish a correspondence between the sets I and $\mathcal{T}$, assigning to i the element ξ^i. Let us select the coordinate ∞ and define a shift function $\varphi\colon SQS(H^n)\to I\setminus\{\infty\}$. For any vector y in $SQS(H^n)$ with nonzero coordinates j,k,ℓ,m, we have

$$\overline{\xi}^j+\overline{\xi}^k+\overline{\xi}^{\ell}+\overline{\xi}^m=0.$$

Hence,

$$\xi^j+\xi^k+\xi^{\ell}+\xi^m=2\xi^r$$

for some r in I. Note that $\xi^r\ne 0$; i.e., $r\ne\infty$ since otherwise the code $\mathcal{P}(m)$ would contain the vector y of weight 4. Then the equality $\xi^j+\xi^k+\xi^{\ell}+\xi^m+2\xi^r=0$ implies that the quaternary vector

$$y+2e_{\infty}+2e_r$$

belongs to the code $\mathcal{P}(m)$. Set $\varphi(y)=r$. Thus, $y+T_{\lambda}(y)+S_{\psi}(y)$ is a code vector. The pair (H^n,φ) corresponding to the code $\mathcal{P}(m)$ is well defined.

The author is deeply grateful to F.I. Solov'eva for fruitful discussions and valuable advice.

REFERENCES

1. Vasil'ev, Yu.L., On Nongroup Closely Packed Codes, *Probl. Kibern.*, 1962, vol. 8, pp. 337–339.
2. Preparata, F.P., A Class of Optimum Nonlinear Double-Error-Correcting Codes, *Inf. Control*, 1968, vol. 13, no. 4, pp. 378–400.
3. Dumer, I.I., Some New Uniformly Packed Codes, in *Proc. Moscow Inst. Physics and Technology*, Moscow, 1976, pp. 72–78.
4. Baker, R.D., van Lint, J.H., and Wilson R.M., On the Preparata and Goethals Codes, *IEEE Trans. Inform. Theory*, 1983, vol. 29, no. 3, pp. 342–345.
5. Hammons, A.R., Jr., Kumar, P.V., Calderbank, A.R., Sloane, N.J.A., and Solé, P., The $\mathbb{Z}_4$-Linearity of Kerdock, Preparata, Goethals, and Related Codes, *IEEE Trans. Inform. Theory*, 1994, vol. 40, no. 2, pp. 301–319.
6. Calderbank, A.R., Cameron, P.J., Kantor, W.M., and Seidel, J.J., $\mathbb{Z}_4$-Kerdock Codes, Orthogonal Spreads, and Extremal Euclidean Line-Sets, *Proc. London Math. Soc.*, 1997, vol. 75, pp. 436–480.
7. Tokareva, N.N., On Components of Preparata Codes, *Probl. Peredachi Inf.*, 2004, vol. 40, no. 2, pp. 63–69 [*Probl. Inf. Trans.* (Engl. Transl.), 2004, vol. 40, no. 2, pp. 159–164].
8. Vasil'ev, Yu.L., Vector Fields on the Vertex Set of the n-Dimensional Unit Cube, in *Diskretnyi analiz* (Discrete Analysis), Novosibirsk: Inst. Mat. Sib. Otd. Akad. Nauk SSSR, 1967, issue 11, pp. 21–59.
9. Krotov, D.S., Vector Fields, Preparata Codes, and Partitions of a Boolean Cube in Cylinders, in *Proc. XII Int. Conf. on Problems of Theoretical Cybernetics, Nizhnii Novgorod, 1999*, Moscow: Dept. Math. Mech. of Moscow State Univ., 1999, p. 122.
10. Krotov, D.S., On Diameter Perfect Constant-Weight Ternary Codes, *Discrete Math.*, submitted.
11. Solov'eva, F.I., On Factorization of Code-Generating DNFs, *Metody diskretnogo analiza v issledovanii funktsional'nykh sistem* (Methods of Discrete Analysis in Studying Functional Systems), Novosibirsk: Inst. Mat. Sib. Otd. Akad. Nauk SSSR, 1988, vol. 47, pp. 66–88.
12. Avgustinovich, S.V. and Solov'eva, F.I., Construction of Perfect Binary Codes by Sequential Shifts of $\widetilde{\alpha}$-Components, *Probl. Peredachi Inf.*, 1997, vol. 33, no. 3, pp. 15–21 [*Probl. Inf. Trans.* (Engl. Transl.), 1997, vol. 33, no. 3, pp. 202–207].
13. Zaitsev, G.V., Zinoviev, V.A., and Semakov, N.V., Interrelation of Preparata and Hamming Codes and Extension of Hamming Codes to New Double-Error-Correcting Codes, *Proc. 2nd Int. Symp. on Information Theory, Tsahkadsor, Armenia, USSR, 1971*, Petrov, P.N. and Csaki, F., Eds., Budapest: Akad. Kiado, 1973, pp. 257–263.
14. Semakov, N.V., Zinoviev, V.A., and Zaitsev, G.V., Uniformly Packed Codes, *Probl. Peredachi Inf.*, 1971, vol. 7, no. 1, pp. 38–50 [*Probl. Inf. Trans.* (Engl. Transl.), 1971, vol. 7, no. 1, pp. 30–39].
15. Kurlyandchik, Ya.M., On the Logarithmic Asymptotics of the Lenghth of a Maximal Cycle of Span $r > 2$, *Metody diskretnogo analiza* (Methods of Discrete Analysis), Novosibirsk: Inst. Mat. Sib. Otd. Akad. Nauk SSSR, 1971, vol. 19, pp. 48–55.
16. Avgustinovich, S.V., Solov'eva, F.I., and Heden, O., On Group of Symmetries of Vasil'ev Codes, in *Proc. 9th Int. Workshop on Algebraic and Combinatorial Coding Theory, Kranevo, Bulgaria, 2004*, pp. 27–33.
17. Borges, J., Phelps, K.T., Rifà, J., and Zinoviev, V.A., On Z_4-Linear Preparata-like and Kerdock-like Codes, *IEEE Trans. Inf. Theory*, 2003, vol. 49, no. 11, pp. 2834–2843.
18. Krotov, D.S., $\mathbb{Z}_4$-Linear Perfect Codes, *Diskr. Analiz Issled. Operatsii, Ser. 1*, 2000, vol. 7, no. 4, pp. 78–90.
19. Krotov, D.S., $\mathbb{Z}_4$-Linear Hadamard and Extended Perfect Codes, in *Proc. Int. Workshop on Coding and Cryptography, 2001, Paris, France*, pp. 329–334.
20. Krotov, D.S., private communication, 2003.

21. Avgustinovich, S.V., Heden, O., and Solov'eva, F.I., The Classification of Some Perfect Codes, *Research Rep. of the Royal Inst. of Technology, Dep. Math.*, Stockholm, Sweden, 2001, no. TRITA-MATH-2001-09.

22. Avgustinovich, S.V., Heden, O., and Solov'eva, F.I., The Classification of Some Perfect Codes, *Des. Codes Cryptogr.*, 2004, vol. 31, no. 3, pp. 313–318.

23. Wan, Z.-X., *Quaternary Codes*, Singapore: World Scientific, 1997.