Problems of Information Transmission, Vol. 40, No. 1, 2004, pp. 5–12. Translated from Problemy Peredachi Informatsii, No. 1, 2004, pp. 6–14.

CODING THEORY

On Multifold MDS and Perfect Codes That Are Not Splittable into Onefold Codes

D. S. Krotov and V. N. Potapov[1]

Sobolev Institute of Mathematics, Siberian Branch of the RAS, Novosibirsk
krotov@math.nsc.ru vpotapov@math.nsc.ru

Received December 20, 2002; in final form, May 13, 2003

Abstract—The union of ℓ disjoint MDS (or perfect) codes with distance 2 (respectively, 3) is always an ℓ-fold MDS (perfect) code. The converse is shown to be incorrect. Moreover, if k is a multiple of 4 and $n+1 \geq 16$ is a power of two, then a $k/2$-fold k-ary MDS code of length $m \geq 3$ and an $(n+1)/8$-fold perfect code of length n exist from which no MDS (perfect) code can be isolated.

1. INTRODUCTION

Let $F_k^n = \{0, 1, \ldots, k-1\}^n$ be the set of words of length n over the alphabet $F_k = \{0, 1, \ldots, k-1\}$. Let $E^n \stackrel{\text{def}}{=} F_2^n$ be a *Boolean cube*. The *Hamming distance* $d(\bar{x}, \bar{y})$ between two words, $\bar{x}$ and $\bar{y}$, in F_k^n is the number of positions in which they differ. A *sphere* $\{\bar{y} \in F_k^n : d(\bar{x}, \bar{y}) \leq r\}$ of radius r centered at a word $\bar{x} \in F_k^n$ will be denoted by $\mathcal{B}_r(\bar{x})$. An *edge* $\{(x_1, x_2, \ldots, x_{i-1}, y, x_{i+1}, \ldots, x_n) : y \in F_k\} \subseteq F_k^n$ of direction i passing through a word $\bar{x} = (x_1, x_2, \ldots, x_n)$ in F_k^n will be denoted by $\mathcal{E}_i(\bar{x})$. By $\overline{E}^n$ and $\underline{E}^n$, we denote the sets of all words from E^n in which the number of ones is, respectively, even or odd.

A set $C \subseteq F_k^n$ (or $C \subseteq E^n$) is called an $(n, M, d)_k$-*code* (respectively, an (n, M, d)-*code*), or a k-*ary* (*binary*) *code of length* n, *cardinality* M, *and with distance* d if $|C| = M$ and $d(\bar{x}, \bar{y}) \geq d$ for any distinct $\bar{x}$ and $\bar{y}$ in C.

A subset C of F_k^n is called a *perfect* k-*ary* r-*error-correcting code* if $|\mathcal{B}_r(\bar{x}) \cap C| = 1$ for any $\bar{x}$ in F_k^n. In the present paper, perfect binary one-error-correcting codes are considered, which we for brevity call perfect codes. Such codes have parameters $\left(n, \frac{2^n}{n+1}, 3\right)$ and exists if and only if $n+1$ is a power of two.

If we append to each word of an $\left(n', \frac{2^{n'}}{n'+1}, 3\right)$ code one more symbol, the *parity-check bit*, which is equal to the sum modulo 2 of all the preceding symbols, we obtain an $\left(n, \frac{2^n}{2n}, 4\right)$ code (with $n = n' + 1$), called an *extended perfect code*. A subset C of $\overline{E}^n$ is an $\left(n, \frac{2^n}{2n}, 4\right)$ code if and only if $|\mathcal{B}_1(\bar{x}) \cap C| = 1$ for each $\bar{x}$ in $\underline{E}^n$.

For any n and k, there exists an $(n, k^{n-1}, 2)_k$ code, which is called an *MDS code with distance* 2 (in the sequel, simply an MDS code). A subset C of F_k^n is an $(n, k^{n-1}, 2)_k$ code if and only if $|\mathcal{E}_i(\bar{x}) \cap C| = 1$ for each $\bar{x}$ in F_k^n and any $i = 1, \ldots, n$.

Remark 1. Generally, by an MDS code, a code with parameters of the type $(n, k^{n-d+1}, d)_k$ is called. Though MDS codes with distance 2 (as well as those with distance 1 or n) are called

[1] Supported in part by the Russian Foundation for Basic Research, project no. 02-01-00939.

0032-9460/04/4001-0005 © 2004 MAIK "Nauka/Interperiodica"

trivial [1], the problem of describing them and estimating their number remains open. Recently, asymptotics of quaternary MDS codes with distance 2 was announced [2].

A code is called *reduced* if it contains the word $(0, 0, \ldots, 0)$.

Definition 1. A subset C of E^n is an *ℓ-fold perfect code* if $|\mathcal{B}_1(\bar{x}) \cap C| = \ell$ for each $\bar{x}$ in E^n. A subset C of $\overline{E}^n$ is an *ℓ-fold extended perfect code* if $|\mathcal{B}_1(\bar{x}) \cap C| = \ell$ for each $\bar{x}$ in $\underline{E}^n$. A subset C in F_k^n is an *ℓ-fold MDS code* if $|\mathcal{E}_i(\bar{x}) \cap C| = \ell$ for each $\bar{x}$ in F_k^n and any $i = 1, \ldots, n$.

Remark 2. Twofold quaternary codes were considered in [3], where a criterion for such codes (more precisely, their characteristic functions) to be decomposable into a sum (modulo 2) of twofold MDS codes of a smaller length was presented. This criterion implied a test for decomposability of ordinary (onefold) MDS codes.

Definition 2. An ℓ-fold perfect code (extended perfect code, MDS code) is *unsplittable* if it cannot be represented as a union of ℓ disjoint perfect codes (extended perfect codes, MDS codes).

An ℓ-fold perfect code (extended perfect code, MDS code) is *completely unsplittable* if it contains (as a subset) no onefold perfect code (extended perfect code, MDS code).

A onefold perfect code (onefold extended perfect code, onefold MDS code) is precisely a perfect code (respectively, extended perfect code, MDS code). On the other hand, a union of ℓ disjoint perfect codes (MDS codes) is an ℓ-fold perfect code (MDS code). The goal of the present paper is to show, first, the existence of unsplittable multifold MDS codes and, second, the existence of unsplittable ℓ-fold perfect codes of length n, where $n + 1$ is a power of two. Moreover, it will be proved that, if k is divisible by 4 and $m \geq 3$, then a completely unsplittable $k/2$-fold k-ary MDS code of length m exists; if $n + 1 \geq 16$ and $\ell \leq (n + 1)/8$ are powers of two, then a completely unsplittable ℓ-fold perfect code of length n (ℓ-fold extended perfect code of length $n + 1$) exists.

Remark 3. The condition $m \geq 3$ is necessary for an unsplittable MDS code to exist. To each ℓ-fold MDS code of length 2 corresponds in a natural way a square $(0, 1)$-matrix with ℓ ones in each column and each row. A well-known consequence of the König–Frobenius theorem (see, e.g., [4, Section 3.3]) is the fact that such matrices have all-one diagonals. Hence, there are no unsplittable MDS codes of length 2.

In Section 2, multifold MDS codes are considered. In Section 2.1, existence of unsplittable ℓ-fold k-ary MDS codes of length 3 with $\ell < k/2$ is shown; in Section 2.2, a completely unsplittable $k/2$-fold k-ary MDS code of length 3 is constructed (k is a multiple of 4). Section 2.3 extends the results to an arbitrary length $n \geq 3$. In Section 3, with the use of the concatenation construction and unsplittable (completely unsplittable) multifold MDS codes, unsplittable (completely unsplittable) multifold perfect codes are constructed.

2. MULTIFOLD MDS CODES

Let $\Omega \subseteq F_k^n$. A function $f^n \colon \Omega \to F_k$ is called a *partial n-quasigroup of order k* if the condition $d(\bar{x}, \bar{y}) = 1$ implies $f^n(\bar{x}) \neq f^n(\bar{y})$. The function f^n is called an *n-quasigroup* if $\Omega = F_k^n$.

Remark 4. A table of values of an n-quasigroup is precisely a Latin n-cube (the n-dimensional generalization of a Latin square).

Proposition 1. 1. *A function $f^{n-1} \colon F_k^{n-1} \to F_k$ is an $(n-1)$-quasigroup if and only if its graph*

$$C = \left\{(\bar{x}, f^{n-1}(\bar{x})) : \ \bar{x} \in F_k^{n-1}\right\}$$

is an $(n, k^{n-1}, 2)_k$ MDS code.

2. *The projection*

$$M = \bigcup_{j=0}^{\ell-1} \Big\{ (\bar{x}, f^n(j, \bar{x})) : \ \bar{x} \in F_k^{n-1} \Big\}$$

of the graph of a partial n-quasigroup $f^n\colon F_\ell \times F_k^{n-1} \to F_k$ is an ℓ-fold MDS code.

Proof. 1. A known and simple consequence of definitions.

2. Since f^n is a quasigroup,

$$g_j^{n-1}(x_1, \ldots, x_{n-1}) \stackrel{\text{def}}{=} f^n(j, x_1, \ldots, x_{n-1})$$

is an $(n-1)$-quasigroup for any j from 0 to $\ell - 1$. Furthermore, for any $\bar{x} \in F_k^{n-1}$, we have $g_i^{n-1}(\bar{x}) \neq g_j^{n-1}(\bar{x})$ if $i \neq j$. Then item 1 implies that

$$C_j = \{ (\bar{x}, g_j^{n-1}(\bar{x})) : \ \bar{x} \in F_k^{n-1} \}, \quad j = 0, \ldots, \ell - 1,$$

are disjoint MDS codes. $\triangle$

A partial n-quasigroup $f^n\colon \Omega \to F_k$ is called *extendable* if $f^n = g^n|_\Omega$ for some n-quasigroup $g^n\colon F_k^n \to F_k$.

2.1. Nonsplittable ℓ-fold MDS Codes of Length 3, $\ell < k/2$.

In [5], the following statement is proved.

Lemma 1. *Let $k \geq 5$ and $k/2 < \ell < k - 1$. Then there exists a nonextendable partial 3-quasigroup $f^3\colon F_\ell \times F_k^2 \to F_k$.*

Proposition 2. *Let $M \subset F_k^n$ be an ℓ-fold MDS code. Then $F_k^n \setminus M$ is a $(k-\ell)$-fold MDS code.*

Proof. This follows from Definition 1 and the equality

$$k = |\mathcal{E}_i(\bar{x})| = |\mathcal{E}_i(\bar{x}) \cap M| + |\mathcal{E}_i(\bar{x}) \cap (F_k^n \setminus M)|. \quad \triangle$$

Proposition 3. *Let $k \geq 5$ and $2 \leq \ell < k/2$. Then there exists an unsplittable ℓ-fold MDS code $M \subset F_k^3$.*

Proof. From Lemma 1, we have a nonextendable partial 3-quasigroup $f^3\colon F_{k-\ell} \times F_k^2 \to F_k$. Proposition 1 implies that the set

$$M = \bigcup_{j=0}^{k-\ell-1} \Big\{ (\bar{x}, f^3(j, \bar{x})) : \ \bar{x} \in F_k^2 \Big\}$$

is a $(k-\ell)$-fold MDS code. Let us show that the ℓ-fold MDS code $F_k^3 \setminus M$ is unsplittable. Assume the contrary: let $F_k^3 \setminus M = C_1 \cup \ldots \cup C_\ell$, where C_i are pairwise disjoint MDS codes in F_k^3. Consider the 2-quasigroups $f_{C_i}^2$ which corresponds to the MDS codes C_i according to Proposition 1, item 1. Define the function $g^3\colon F_k^3 \to F_k$ as

$$g^3(x, y, z) = f^3(x, y, z) \quad \text{if} \quad 0 \leq x \leq k - \ell - 1,$$
$$g^3(x, y, z) = f_{C_{k-x}}^3(y, z) \quad \text{if} \quad k - \ell \leq x \leq k - 1.$$

It can easily be checked that the function g^3 is a 3-quasigroup and that g^3 is an extension of the partial 3-quasigroup f^3. A contradiction. $\triangle$

2.2. Completely Unsplittable $k/2$-fold MDS Codes of Length 3.

A *face* in F_k^3 obtained by fixing the ith coordinate is denoted by

$$\mathcal{F}_i(y) \stackrel{\text{def}}{=} \{(x_1, x_2, x_3) : \ x_i = y\}, \quad y \in F_k.$$

A set $C \subset F_k^3$ is called a *diagonal* if $|\mathcal{F}_i(y) \cap C| = 1$ for any $i \in \{1, 2, 3\}$ and $y \in F_k$. In other words, $C = \{(0, y_0, z_0), \ldots, (k-1, y_{k-1}, z_{k-1})\}$, where $\{y_0, \ldots, y_{k-1}\} = \{z_0, \ldots, z_{k-1}\} = F_k$.

Proposition 4. *Let ℓ be even. Then the $(3, \ell^2, 2)_\ell$ MDS code*

$$G_\ell \stackrel{\text{def}}{=} \Big\{(x, y, z) \in F_\ell^3 : \ x + y + z = 0 \mod \ell\Big\}$$

contains no diagonal.

Proof. Assume the contrary: let a diagonal $H \subset G_\ell$ exist. For any (x, y, z) in G_ℓ, we have $x + y + z = 0 \bmod \ell$; therefore,

$$\begin{aligned} 0 \stackrel{\bmod \ell}{=} \sum_{(x,y,z)\in H} (x + y + z) &= \sum_{(x,y,z)\in H} x + \sum_{(x,y,z)\in H} y + \sum_{(x,y,z)\in H} z \\ &= \sum_{x=0}^{\ell-1} x + \sum_{y=0}^{\ell-1} y + \sum_{z=0}^{\ell-1} z = \frac{\ell(\ell-1)}{2} + \frac{\ell(\ell-1)}{2} + \frac{\ell(\ell-1)}{2} \stackrel{\bmod \ell}{=} \frac{\ell}{2} \neq 0, \end{aligned}$$

a contradiction. $\triangle$

Remark 5. Proposition 4 is a particular case of the theorem on transversal-free Latin squares (see [6]).

Proposition 5. *For any k divisible by 4 there exists a completely unsplittable $k/2$-fold MDS code $M \subset F_k^3$.*

Proof. Let $\ell \geq 2$ be even, and let $k = 2\ell$. For $C \subset F_\ell^3$, introduce the following notations:

$$\widehat{C} \stackrel{\text{def}}{=} F_\ell^3 \setminus C,$$

$$C + (a, b, c) \stackrel{\text{def}}{=} \{(x + a, y + b, z + c) : \ (x, y, z) \in C\}.$$

Define the set $G_\ell \subset F_\ell^3$ as in Proposition 4, and define the sets $B_1, B_2, B_3 \subset F_\ell^3$ by the equalities

$$B_1 \stackrel{\text{def}}{=} \{(x, y, y) : \ x, y \in F_\ell\}, \qquad B_2 \stackrel{\text{def}}{=} \{(y, x, y) : \ x, y \in F_\ell\}, \qquad B_3 \stackrel{\text{def}}{=} \{(y, y, x) : \ x, y \in F_\ell\}.$$

Let

$$\begin{aligned} M \stackrel{\text{def}}{=} G_\ell &\cup (\widehat{B}_3 + (\ell, 0, 0)) \cup (\widehat{B}_1 + (0, \ell, 0)) \cup (\widehat{B}_2 + (0, 0, \ell)) \\ &\cup (B_3 + (\ell, 0, \ell)) \cup (B_1 + (\ell, \ell, 0)) \cup (B_2 + (0, \ell, \ell)) \cup (\widehat{G}_\ell + (\ell, \ell, \ell)). \end{aligned}$$

An example of a set M (with $\ell = 4$) is shown in Fig. 1 (note that the example is not a minimal one; ℓ may equal 2). One can easily verify that M is an ℓ-fold MDS code. Let us prove that M is completely unsplittable. Assume the contrary: let a onefold MDS code $D \subset M$ exist.

Let $x \in F_\ell$. Consider the set $D_1(x) \stackrel{\text{def}}{=} D \cap \mathcal{F}_1(x) \subset M \cap \mathcal{F}_1(x)$ (see Fig. 2). By the construction, the intersection of M and the edge $\mathcal{E}_2((x, 0, x + \ell))$ is contained in $F_\ell^3 + (0, \ell, \ell)$. Hence, the only element of D (and also of $D_1(x)$) that belongs to this edge lies in $F_\ell^3 + (0, \ell, \ell)$. Similarly, the intersection of each of the $\ell - 1$ edges $\mathcal{E}_2((x, 0, z + \ell))$, $z \in F_\ell$, $z \neq x$, and the code M is contained in $F_\ell^3 + (0, 0, \ell)$. Hence, $\ell - 1$ elements of D (and also of $D_1(x)$) that belong to these edges lie in

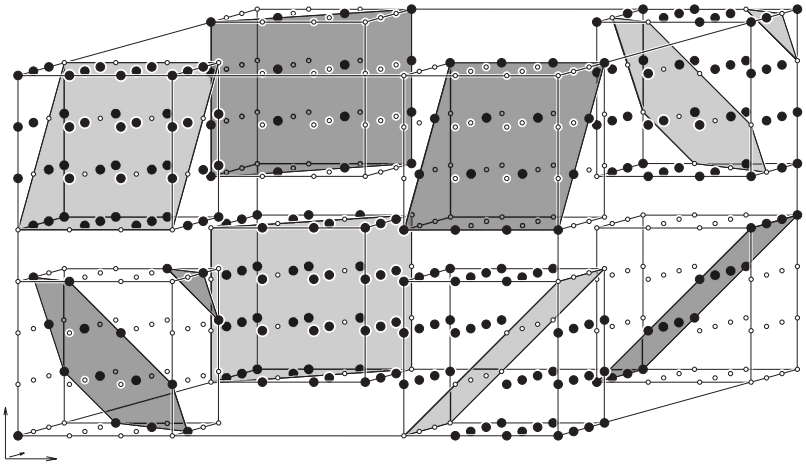

Fig. 1. Completely unsplittable 4-fold 8-ary MDS code M.

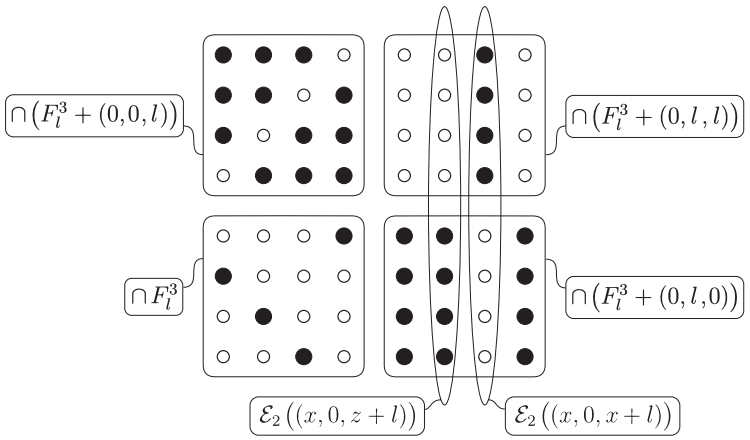

Fig. 2. The set $\mathcal{F}_1(x)\cap M$, $\ell=4$, $x=2$.

$F_\ell^3+(0,0,\ell)$. Thus, $D_1(x)$ intersects $F_\ell^3+(0,\ell,\ell)$ by one element and intersects $F_\ell^3+(0,0,\ell)$ by $\ell-1$ elements. The set

$$\left(F_\ell^2\times F_{2\ell}\right)\cap\mathcal{F}_1(x)=\left(\mathcal{F}_1(x)\cap F_\ell^3\right)\cup\left(\mathcal{F}_1(x)\cap\left(F_\ell^3+(0,0,\ell)\right)\right)$$

intersects D by ℓ elements (since it is split into ℓ edges). Of them, as is already shown, $\ell-1$ elements are contained in $F_\ell^3+(0,0,\ell)$. Hence, $|D_1(x)\cap F_\ell^3|=|D\cap\mathcal{F}_1(x)\cap F_\ell^3|=1$.

Analogously, it can be shown that $|D\cap\mathcal{F}_i(x)\cap F_\ell^3|=1$ for any $i\in\{1,2,3\}$ and $x\in F_\ell$. Thus, the set D has one element in each face from F_ℓ^3. Hence, $D\cap F_\ell^3$ is a diagonal by the definition. This contradicts Proposition 4 since $D\cap F_\ell^3\subset G_\ell$. $\triangle$

2.3. Multifold MDS Codes of an Arbitrary Length

Proposition 6. *If $M^3\subset F_k^3$ is an unsplittable (completely unsplittable) ℓ-fold MDS code of length* 3*, then*

$$M^n\stackrel{\text{def}}{=}\left\{(x_1,x_2,x_3,\ldots,x_n)\in F_k^n:\ (x_1,x_2,(x_3+\ldots+x_n)\bmod k)\in M^3\right\},\quad n\ge 3,$$

is an unsplittable (completely unsplittable) ℓ-fold MDS code of length n.

Proof. Obviously, M^n is an ℓ-fold MDS code. Since

$$M^3 = \Big\{(x_1, x_2, x_3) : \ (x_1, x_2, x_3, 0, \ldots, 0) \in M^n\Big\},$$

it is easy to prove by contradiction that unsplittability (complete unsplittability) of M^3 implies unsplittability (complete unsplittability) of M^n. $\triangle$

Propositions 3, 5, and 6 imply the following theorem.

Theorem 1. 1. *Let $n \geq 3$, $k \geq 5$, and $2 \leq \ell < k/2$. Then there exists an unsplittable ℓ-fold MDS code $M \subset F_k^n$.*

2. *Let $n \geq 3$ and let k be a multiple of 4. Then there exists a completely unsplittable $k/2$-fold MDS code $M \subset F_k^n$.*

3. MULTIFOLD PERFECT CODES

Definitions 1 and 2 imply the following fact.

Proposition 7. *Let $C \subseteq E^n$, $\overline{C} \subseteq E^{n+1}$, and let $\overline{C}$ be obtained from C by adding the parity-check bit. Then C is an ℓ-fold perfect code (unsplittable ℓ-fold perfect code, completely unsplittable ℓ-fold perfect code) if and only if $\overline{C}$ is an ℓ-fold extended perfect code (respectively, unsplittable ℓ-fold perfect code, completely unsplittable ℓ-fold perfect code).*

Proposition 8. *A subset C of the set E^n is an ℓ-fold extended perfect code if $|C| = \ell\dfrac{2^n}{2n}$ and $|\mathcal{B}_1(\bar{x}) \cap C| \geq \ell$ for any $\bar{x}$ in $\underline{E}^n$.*

Proof. By the condition,

$$\sum_{\bar{x} \in \underline{E}^n} |\mathcal{B}_1(\bar{x}) \cap C| \geq \ell |\underline{E}^n| = \ell 2^{n-1}, \tag{1}$$

and this inequality is strict if $|\mathcal{B}_1(\bar{x}) \cap C| > \ell$ for at least one $\bar{x}$ from $\underline{E}^n$.

Since each word y in C (as well as any other word) belongs to spheres with centers in at most n vertices from $\underline{E}^n$ (more precisely, in one vertex if $y \in \underline{E}^n$, and in n vertices if $y \in \overline{E}^n$), we have

$$\sum_{\bar{x} \in \underline{E}^n} |\mathcal{B}_1(\bar{x}) \cap C| \leq n|C| = \ell 2^{n-1}, \tag{2}$$

and this inequality is strict if at least one word from C belongs to $\underline{E}^n$.

Strictness of either of inequalities (1) and (2) results in the contradiction $\ell 2^{n-1} < \ell 2^{n-1}$; therefore, C is an ℓ-fold extended perfect code by the definition. $\triangle$

The construction described below is a particular case of the generalized concatenation construction [7]. In [8], it is applied (in a more general form) to construct extended perfect codes from MDS codes. We will use this construction to obtain unsplittable (completely unsplittable) multifold perfect codes from unsplittable (completely unsplittable) multifold MDS codes.

Let m, k, and $n = mk$ be powers of two; H and C be reduced extended perfect codes of length m and k respectively; B be a subset of F_k^m.

Denote by $\widetilde{e}_i$ the word from E^k with unity in the $(i+1)$st position and zeros in all the others, $i = 0, \ldots, k-1$. Define the codes C_i^a, $a \in \{0, 1\}$, $i \in \{0, \ldots, k-1\}$, by the equalities $C_i^1 \stackrel{\text{def}}{=} C \oplus \widetilde{e}_i$ and $C_i^0 \stackrel{\text{def}}{=} C_i^1 \oplus \widetilde{e}_0$, $i = 0, \ldots, k-1$. Note that $C_i^a \cap C_{i'}^{a'} = \varnothing$ if $(i, a) \neq (i', a')$. Since

$$\sum_{i=0}^{k-1} |C_i^0| = 2^{k-1} = |\overline{E}^k| \qquad \text{and} \qquad C_i^0 \subset \overline{E}^k,$$

we have $\overline{E}^k = \bigcup\limits_i C_i^0$ and, analogously, $\underline{E}^k = \bigcup\limits_i C_i^1$. Define the set

$$D = \bigcup_{(a_1,\ldots,a_m)\in H} \; \bigcup_{(i_1,\ldots,i_m)\in B} C_{i_1}^{a_1} \times C_{i_2}^{a_2} \times \ldots \times C_{i_m}^{a_m}. \tag{3}$$

Proposition 9. *If B is an ℓ-fold MDS code, then the set D defined by* (3) *is an ℓ-fold extended perfect code.*

Before proving the proposition, let us define for an arbitrary word $\bar{x} = (x_1, \ldots, x_n) \in E^n = E^{mk}$ the *generalized parity check*

$$p(\bar{x}) = \Big((x_1 \oplus \ldots \oplus x_k),\ (x_{k+1} \oplus \ldots \oplus x_{2k}),\ \ldots,\ (x_{(m-1)k+1} \oplus \ldots \oplus x_{mk}) \Big).$$

Proof. Consider an arbitrary odd word $\bar{x} \in \underline{E}^n$. The word $p(\bar{x})$ is also odd. Since H is an extended perfect code, there exists a unique $\bar{z}$ in H such that $d(p(\bar{x}), \bar{z}) = 1$. Let j be the number of positions in which $p(\bar{x})$ and $\bar{z}$ differ. Denote $\widetilde{x}^t \stackrel{\text{def}}{=} (x_{(t-1)k+1}, x_{(t-1)k+2}, \ldots, x_{tk})$. For each t in $\{1, \ldots, m\} \setminus \{j\}$, let i_t be such that $\widetilde{x}^t \in C_{i_t}^{z_t}$. By the definition of an ℓ-fold MDS code, there are pairwise distinct $i^{(1)}, i^{(2)}, \ldots, i^{(\ell)}$ such that $(i_1, i_2, \ldots, i_{j-1}, i^{(s)}, i_{j+1}, \ldots, i_m) \in B$ for each $s \in \{1, \ldots, \ell\}$. Since the words $p(\bar{x})$ and $\bar{z}$ differ in position j, there exists a word $\widetilde{y}^{(s)} \in C_{i^{(s)}}^{z_j}$ such that $d(\widetilde{x}^j, \widetilde{y}^{(s)}) = 1$. Denote $\bar{y}^{(s)} = (\widetilde{x}^1, \ldots, \widetilde{x}^{j-1}, \widetilde{y}^{(s)}, \widetilde{x}^{j+1}, \ldots, \widetilde{x}^m)$. By the construction, we have $d(\bar{x}, \bar{y}^{(s)}) = 1$ and at the same time $\bar{y}^{(s)} \in D$. Thus, $|\{\bar{y} \in D :\ d(\bar{x}, \bar{y}) = 1\}| \geq |\{\bar{y}^{(s)}\}_{s=1}^{\ell}| = \ell$ for each $\bar{x} \in \underline{E}^n$.

On the other hand,

$$|D| = |H||B||C|^m = \frac{2^m}{2m}\, \ell k^{m-1} \left(\frac{2^k}{2k}\right)^m = \frac{\ell 2^n}{2n}.$$

Applying Proposition 8 completes the proof. $\triangle$

We have the following statement.

Proposition 10. 1. *For each $\bar{x}$ in D, we have $p(\bar{x}) \in H$.*

2. *$(\widetilde{e}_{i_1}, \ldots, \widetilde{e}_{i_m}) \in D$ if and only if $(i_1, \ldots, i_m) \in B$.*

3. *Let $A \subset D$ be an extended perfect code of length n; let $B_0 = \{(i_1, \ldots, i_m) \mid (\widetilde{e}_{i_1}, \ldots, \widetilde{e}_{i_m}) \in A\}$. Then B_0 is an $(m, k^{m-1}, 2)_k$ MDS code and $B_0 \subset B$.*

Proof. Items 1 and 2 immediately follow from formula (3). Item 2 implies that $B_0 \subseteq B$. Let us show that B_0 is an $(m, k^{m-1}, 2)_k$ MDS code.

Code distance. If $(i_1, \ldots, i_m)$ and $(j_1, \ldots, j_m)$ from B_0 differ in one coordinate only, then $(\widetilde{e}_{i_1}, \ldots, \widetilde{e}_{i_m})$ and $(\widetilde{e}_{j_1}, \ldots, \widetilde{e}_{j_m})$ from A differ in two coordinates only. This contradicts the fact that A is an extended perfect code.

Cardinality. For arbitrary $i_2, \ldots, i_m$, consider the word $\bar{x} = (0, \ldots, 0, \widetilde{e}_{i_2}, \ldots, \widetilde{e}_{i_m}) \in E^n$. Since $\bar{x} \in \underline{E}^n$, there exists a unique word $\bar{y}$ in A which differs from $\bar{x}$ in exactly one coordinate. The words $p(\bar{x})$ and $p(\bar{y})$ also differ in exactly one coordinate. Since $p(\bar{x}) = (0, 1, \ldots, 1)$ and $p(\bar{y}) \in H \ni (1, 1, \ldots, 1)$ (it is known [9] that a reduced (extended) perfect code contains the word $(1, 1, \ldots, 1)$), we have $p(\bar{y}) = (1, 1, \ldots, 1)$. Hence, $\bar{y} = (\widetilde{e}_{i_1}, \widetilde{e}_{i_2}, \ldots, \widetilde{e}_{i_m})$ for some i_1. Since $\bar{y} \in A$, we have $(i_1, i_2, \ldots, i_m) \in B_0$. Therefore, $|B_0| = k^{m-1}$. $\triangle$

Theorem 2. 1. *If $n = 2^s \geq 16$ and $1 < \ell < n/8$, then there exists an unsplittable ℓ-fold extended perfect code in E^n.*

2. *If $n = 2^s \geq 16$ and $1 < \ell = 2^t \leq n/8$, then there exists a completely unsplittable ℓ-fold extended perfect code in E^n.*

Proof. 1. Let $m = 4$ and $k = n/4$. By item 1 of Theorem 1, there is an unsplittable ℓ-fold MDS code $B \subset F_k^m$ ($2 \le \ell < n/8 = k/2$). Due to Proposition 9, the set D obtained from B by formula (3) is an ℓ-fold extended perfect code. Let us show that D is unsplittable.

Let $D = C_1 \cup \ldots \cup C_\ell$, where C_i are pairwise disjoint extended perfect codes. Then Proposition 10 implies that, for $1 \le j \le \ell$, the sets $B_j = \{(i_1, \ldots, i_m) \mid (\widetilde{e}_{i_1}, \ldots, \widetilde{e}_{i_m}) \in C_j\}$ are MDS codes. Moreover, the codes B_j are subsets of B and, as well as the codes C_j, are pairwise disjoint. Then the equality

$$|B| = \ell k^{m-1} = \sum_{j=1}^{\ell} |B_j|$$

implies that $B = B_1 \cup \ldots \cup B_\ell$. The contradiction proves that D is unsplittable.

2. Let $m = n/2\ell$ and $k = 2\ell$. By item 2 of Theorem 1, there is a completely unsplittable ℓ-fold MDS code $B \subset F_k^m$. Due to Proposition 9, the set D obtained from B by formula (3) is an ℓ-fold extended perfect code. Let us prove by contradiction that D does not contain a onefold subcode. Let $C \subset D$ be a onefold extended perfect code. Then Proposition 10 implies that the set $B' = \{(i_1, \ldots, i_m) : (\widetilde{e}_{i_1}, \ldots, \widetilde{e}_{i_m}) \in C\}$ is an MDS code and is contained in B, a contradiction. $\triangle$

Theorem 2 and Proposition 7 imply the following theorem.

Theorem 3. 1. *If $n = 2^s - 1 \ge 15$ and $1 < \ell < (n+1)/8$, then there exists an unsplittable ℓ-fold perfect code in E^n.*

2. *If $n = 2^s - 1 \ge 15$ and $1 < \ell = 2^t \le (n+1)/8$, then there exists a completely unsplittable ℓ-fold perfect code in E^n.*

REFERENCES

1. MacWilliams, F.J. and Sloane, N.J.A., *The Theory of Error-Correcting Codes*, Amsterdam: North-Holland, 1977. Translated under the title *Teoriya kodov, ispravlyayushchikh oshibki*, Moscow: Svyaz', 1979.

2. Krotov, D.S. and Potapov, V.N., On the Reconstruction of n-Quasigroups of Order 4 and the Upper Bounds on Their Numbers, in *Trans. of the Conf. Devoted to the 90th Anniversary of Alexei A. Lyapunov*, Novosibirsk, 2001, pp. 323–327. Available from `http://www.sbras.ru/ws/Lyap2001/2363/`.

3. Krotov, D.S., On Decomposition of $(n, 4^{n-1}, 2)_4$ MDS Codes and Double-Codes, *Proc. 8th Int. Workshop on Algebraic and Combinatorial Coding Theory, Tsarskoe Selo, Russia, 2002*, pp. 168–171.

4. Minc, H., *Permanents*, Reading: Addison-Wesley, 1978. Translated under the title *Permanenty*, Moscow: Mir, 1982.

5. Kochol, M., Relatively Narrow Latin Parallelepipeds That Cannot Be Extended to a Latin Cube, *Ars Comb.*, 1995, vol. 40, pp. 247–260.

6. Denes, J. and Keedwell, A.D., *Latin Squares and Their Applications*, Budapest: Acad. Kiado, 1974.

7. Zinoviev, V.A., Generalized Concatenated Codes, *Probl. Peredachi Inf.*, 1976, vol. 12, no. 1, pp. 5–15 [*Probl. Inf. Trans.* (Engl. Transl.), 1976, vol. 12, no. 1, pp. 2–9].

8. Phelps, K.T., A General Product Construction for Error-Correcting Codes, *SIAM J. Algebr. Discrete Methods*, 1984, vol. 5, no. 2, pp. 224–228.

9. Shapiro, G.S. and Slotnik, D.L., On the Mathematical Theory of Error-Correcting Codes, *IBM J. Res. Develop.*, 1959, vol. 3, no. 1, pp. 25–34 [Russian Transl. in *Kibern. Sb.*, Vol. 5, Moscow: Inostr. Lit., 1962, pp. 7–32].