On the number of nonequivalent propelinear extended perfect codes

J. Borges
Department of Information and Communications Engineering
Universitat Autònoma de Barcelona
08193-Bellaterra, Spain
joaquim.borges@uab.cat

I. Yu. Mogilnykh
Sobolev Institute of Mathematics and Novosibirsk State University
Novosibirsk, Russia.
ivmog@math.nsc.ru

J. Rifà
Department of Information and Communications Engineering
Universitat Autònoma de Barcelona
08193-Bellaterra, Spain
josep.rifa@uab.cat

F. Solov'eva
Sobolev Institute of Mathematics and Novosibirsk State University
Novosibirsk, Russia.
sol@math.nsc.ru

Submitted: Mar 19, 2013; Accepted: May 15, 2013; Published: May 24, 2013
Mathematics Subject Classifications: 94B25, 94B60, 94A99

Abstract

The paper proves that there exists an exponential number of nonequivalent propelinear extended perfect binary codes of length growing to infinity. Specifically, it is proved that all transitive extended perfect binary codes found by Potapov (2007) are propelinear. All such codes have small rank, which is one more than the rank of the extended Hamming code of the same length. We investigate the properties of these codes and show that any of them has a normalized propelinear representation.

Keywords: binary codes; extended perfect codes; normalized propelinear structures; propelinear codes

1 Preliminaries

Let E_q be the set $\{0, 1, \ldots, q-1\}$, where we distinguish one element as 0. We call *words* the elements of the cartesian product E_q^n. The word $(0, \ldots, 0)$ is denoted by $\mathbf{0}$. Given two words $u = (u_1, u_2, \cdots, u_n), v = (v_1, v_2, \cdots, v_n) \in E_q^n$, the *Hamming distance* $d(u, v)$ is the number of positions where they differ. In some cases, when we are interested in an algebraic structure inside E_q we will take the q-ary finite field $\mathbb{F}_q$ instead of E_q, with

$q = p^m$ and p prime. The action of an isometry of E_q^n can be presented as the action of a permutation π on the coordinate positions $\{1, \ldots, n\}$ followed by the action of n permutations $\sigma_1, \ldots, \sigma_n$ of E_q:

$$\pi(x_1, \ldots, x_n) = (x_{\pi^{-1}(1)}, \ldots, x_{\pi^{-1}(n)}),$$

$$(\sigma_1, \ldots, \sigma_n)(x_1, \ldots, x_n) = (\sigma_1(x_1), \ldots, \sigma_n(x_n)).$$

The permutation $\sigma = (\sigma_1, \ldots, \sigma_n)$ is called a *multi-permutation.* The composition $\sigma \circ \sigma'$ of two multi-permutations σ and σ' is the following multi-permutation: $(\sigma_1 \circ \sigma'_1, \ldots, \sigma_n \circ \sigma'_n)$, where $\sigma_i \circ \sigma'_i$ is the composition $\sigma_i \circ \sigma'_i(x_i) = \sigma_i(\sigma'_i(x_i))$, for any $i \in \{1, 2, \ldots, n\}$.

By $(\sigma; \pi)(x)$ we denote the image of x under an isometry $(\sigma; \pi)$:

$$(\sigma; \pi)(x) = \sigma(\pi(x)).$$

A q-ary *code* C of length n is a subset of E_q^n. We denote by $\mathrm{Iso}(C)$ the largest subgroup of isometries of E_q^n that fix the code C and we call it the *isometry group* of the code C.

Definition 1. *A q-ary code C of length n, $\mathbf{0} \in C$, is called* propelinear *if for any codeword x there exists a coordinate permutation π_x and a multi-permutation $\sigma_x = (\sigma_{x,1}, \ldots, \sigma_{x,n})$ satisfying:*

(i) for any $x \in C$ it holds $(\sigma_x; \pi_x)(C) = C$ and $(\sigma_x; \pi_x)(\mathbf{0}) = x$,

(ii) if $y \in C$ and $z = (\sigma_x; \pi_x)(y)$, then:
$\pi_z = \pi_x \circ \pi_y$ and $\sigma_{z,i} = \sigma_{x,i} \circ \sigma_{y,\pi_x^{-1}(i)}$, for any $i \in \{1, \ldots, n\}$; or, equivalently, $(\sigma_z; \pi_z) = (\sigma_x; \pi_x)(\sigma_y; \pi_y)$.

A q-ary code is called *transitive* if the isometry group of the code acts transitively on its codewords, i. e., the code satisfies the property (i) in Definition 1. Transitive codes are studied in [10, 11].

In the binary case, when $q = 2$, taking the usual addition on $E_2 = \mathbb{F}_2$, the above definition is reduced to the following:

A binary code C is *propelinear* [8] if for each $x \in C$ there exists a coordinate permutation π_x such that:

(i) $x + \pi_x(C) = C$;

(ii) if $x + \pi_x(y) = z$, then $\pi_z = \pi_x \circ \pi_y$, for any $y \in C$.

As in the binary case, where we can define a group structure $\star$ on C which is compatible with the Hamming distance, that is, such that $d(x \star u, x \star v) = d(u, v)$, also in the q-ary case, given a q-ary propelinear code we define the operation $\star$ as

$$x \star v = (\sigma_x; \pi_x)(v) \quad \text{for any } x \in C, \quad \text{for any } v \in E_q^n. \tag{1}$$

In [1, 7, 8, 9], properties of binary propelinear codes are deeply studied. Linear codes and $\mathbb{Z}_2\mathbb{Z}_4$-linear codes are propelinear but, perhaps, one much more interesting example of propelinear code is the original Preparata code [9] wich is not a $\mathbb{Z}_4$-linear code (although there is a $\mathbb{Z}_4$-linear code with the same parameters [4]). In [2, 3], the relations between classes of propelinear and transitive codes are investigated. The problem of distinguishing these classes had been open since 2006. In [3] it was established that these classes are different. In fact, it was found that the binary Best code of length 10 is transitive, but not propelinear.

In this paper we establish a new lower bound $\frac{1}{8n^2\sqrt{3}}e^{\pi\sqrt{2n/3}}(1+o(1))$ on the number of nonequivalent propelinear extended perfect binary codes of length $4n$ for n going to infinity. This bound is obtained by showing propelinearity of transitive Potapov codes [6], the rank of which is one more than the rank of the extended Hamming code of the same length. The previous lower bound on the number of nonequivalent propelinear extended perfect binary codes of length $n = 2^m, m \geqslant 4$ was $\lfloor \log_2(n/2) \rfloor^2$, see [2, 3]. Despite the fact that the new class of propelinear codes is larger than the old class from [2, 3], it does not cover the old one (the ranks of codes from [2, 3] and from [6] do not coincide), so the result [2, 3] keeps current. We investigate in this paper the properties of new propelinear codes and show that any of them has a normalized propelinear representation.

Now, we give a generalization of the most relevant properties of propelinear codes to the q-ary case.

Let C be a propelinear code; let Π and Σ be the set of permutations and the set of multi-permutations, respectively, assigned to the codewords of C (Definition 1) and let $\star$ be the afore defined operation in C. To emphasize this particular propelinear structure of C we write $(C, \Pi, \Sigma, \star)$ or, simply $(C, \star)$ when we do not require any information about the set of associated permutations.

The next lemmas are easy to prove from elementary group theory.

Lemma 2. *Let $(C, \Pi, \Sigma, \star)$ be a q-ary propelinear code of length n.*

(i) Let $x \in C$ and $u, v \in E_q^n$. If $x \star u = x \star v$, then $u = v$.

(ii) The all-zeroes word $\mathbf{0}$ is a codeword, $\mathbf{0} \in C$.

(iii) For any codeword $x \in C$, there exists a unique codeword $x' \in C$ such that $x \star x' = \mathbf{0}$.

Note: Not always the defined operation $\star$ can be generalized in a proper way over all E_q^n. That is, from $x, y \in C$, $u \in E_q^n$ such that $x \star u = y \star u$, we do not necessarily have $x = y$.

Lemma 3. *Let $(C, \Pi, \Sigma, \star)$ be a q-ary propelinear code. Then C equipped with this operation $\star$ is a group.*

Note that, apart from the group structure on C given by the operation $\star$, there can exist a lot of different group structures on a propelinear code, including nonisomorphic ones (for binary case see [3]).

Clearly, $\mathbf{0}$ is the identity element in $(C, \star)$ and we denote by x^{-1} the inverse element of the codeword x. Denote by Id_n the identity permutation over any set of cardinal n. Now, we can link the coordinate permutations and the multi-permutations of inverse elements.

Lemma 4. *Let $(C,\star)$ be a q-ary propelinear code. Then,*

(i) The codeword $\mathbf{0}$ has the identities as the associated coordinate permutation $\pi_{\mathbf{0}} = \mathrm{Id}_n$ and multi-permutation $\sigma_{\mathbf{0}} = (\mathrm{Id}_q, \mathrm{Id}_q, \ldots, \mathrm{Id}_q)$, respectively.

(ii) We have $\pi_{x^{-1}} = \pi_x^{-1}$ and $\sigma_{x^{-1},i} = \sigma_{x,\pi_x(i)}^{-1}$, for any codeword $x \in C$ and any $i \in \{1,\ldots,n\}$.

Finally, as we said before, the action of $\star$ over E_q^n is Hamming distance compatible.

Lemma 5. *Let $(C,\star)$ be a q-ary propelinear code. Then,*

$$d(x\star u, x\star v) = d(u,v) \quad \text{for any } x \in C, \ \text{ for any } u,v \in E_q^n.$$

2 Isotopically propelinear MDS codes

A q-ary code of length n, satisfying the property (i) in Definition 1 with $\pi_x = \mathrm{Id}_n$ for any x in the code is called an *isotopically transitive code*. A notion of isotopic transitivity was introduced by Potapov in [6] and used for constructing an exponential number of nonequivalent transitive extended binary perfect codes of length n as n goes to infinity. We call a q-ary propelinear structure on a code C of length n *isotopically propelinear*, if for any $x \in C$ it holds $\pi_x = \mathrm{Id}_n$. If there is an isotopically propelinear structure on a code C, we call C *isotopically propelinear*.

A q-ary code C of length m with minimum distance 2 of size q^{m-1} is a kind of MDS code. All MDS-codes we use in this paper are of this kind. A *quaternary MDS code* is a code with $q=4$. A function $f : E_q^{m-1} \to E_q$ is called a $(m-1)$-ary *quasigroup* of order q if $f(x_1,\ldots,x_{m-1}) \neq f(y_1,\ldots,y_{m-1})$ for any words $(x_1,\ldots,x_{m-1})$ and $(y_1,\ldots,y_{m-1})$ from E_q^{m-1} that differs in only one position.

It is known that there exists a one-to-one correspondence between $(m-1)$-ary quasigroups of order q and MDS q-ary codes of length m. Given a $(m-1)$-ary quasigroup f we can construct the code $\{(x, f(x)) : x \in E_q^{m-1}\}$.

Concerning MDS codes, we mainly consider the quaternary case, i.e., $q = 4$. We use two different group operations in E_4. First, we use $*$ to refer to the addition when we see the elements in E_4 as elements in $\mathbb{Z}_4$. Second, we use $\oplus$ to refer to the addition when we see the elements in E_4 as elements in $\mathbb{Z}_2 \times \mathbb{Z}_2$ through the Gray map given by $0 \to (0,0), 1 \to (0,1), 2 \to (1,1), 3 \to (1,0)$.

Both next examples were used in [6] to construct extended perfect transitive codes.

Example 1. Let us consider the function $x_1 * x_2$ from E_4^2 to E_4. From the correspondence between MDS codes and quasigroups we have that $\{(x_1, x_2, x_1 * x_2) : x_1, x_2 \in E_4\}$ is a MDS code. It is straightforward to see that this code is an isotopically propelinear code with the corresponding permutations $\sigma_{x,1}(y) = x_1 * y$, $\sigma_{x,2}(y) = x_2 * y$, $\sigma_{x,3}(y) = x_3 * y$ for any $y \in E_4$, where $x_3 = x_1 * x_2$.

Example 2. Let $x_1 \oplus x_2$ be the function from E_4^2 to E_4. The corresponding MDS code is isotopically propelinear with the following permutations $\sigma_{x,1}(y) = x_1 \oplus y$, $\sigma_{x,2}(y) = x_2 \oplus y$, $\sigma_{x,3}(y) = x_3 \oplus y$ for $y \in E_4$, where $x_3 = x_1 \oplus x_2$.

Potapov [6] proved the isotopic transitivity of quaternary MDS codes obtained from an isotopically transitive MDS code M and the MDS code from Example 2 using the following concatenated construction:

$$\{(x_1,\dots,x_{i-1},y_1,\dots,y_r,x_{i+1},\dots,x_m): \\ y_1\oplus y_2\oplus\dots\oplus y_r = x_i,\ x=(x_1,\dots,x_m)\in M\}, \tag{2}$$

for some fixed i, $1\leqslant i\leqslant m-1$, and for any $r=1,2,\dots$

If the initial code corresponds to a quasigroup f, that is, $M=\{(x,f(x)):x\in E_4^{m-1}\}$ then the constructed code corresponds to the following composition of the quasigroup f and the quasigroup from Example 2:

$$g(x_1,\dots,x_{i-1},y_1,\dots,y_r,x_{i+1},\dots,x_{m-1}) = \\ f(x_1,\dots,x_{i-1},y_1\oplus\dots\oplus y_r,x_{i+1},\dots,x_{m-1}).$$

The main result of this section is Proposition 8, where we show that the constructed code is, in fact, isotopically propelinear given that M is isotopically propelinear. Below, without restricting generality, i is equal to 1.

First of all we recall two technical lemmas.

Lemma 6. *[6] Let φ be a permutation on the elements of E_4. Then $\varphi(a\oplus b)=\varphi(a)\oplus\varphi(b)\oplus\varphi(0)$.*

Given a permutation σ on the elements of E_4 and a word $y=(y_1,\dots,y_r)$ in E_4^r such that $y_1\oplus\dots\oplus y_r=\sigma(0)$ we define the permutations $\tau_{y,1},\dots,\tau_{y,r}$ in E_4 in the following way:

$$\tau_{y,s}(\alpha)=\sigma(\alpha)\oplus y_1\oplus\dots\oplus y_r\oplus y_s=\sigma(\alpha)\oplus\sigma(0)\oplus y_s, \text{ where } s\in\{1,2,\dots,r\}. \tag{3}$$

The above defined permutations satisfy the following statement:

Lemma 7. *[6, Prop. 7] For any $x_1,\dots,x_r\in E_4$ we have $\tau_{y,1}(x_1)\oplus\dots\oplus\tau_{y,r}(x_r)=\sigma(x_1\oplus\dots\oplus x_r)$.*

Proposition 8. *Let M be a quaternary* MDS *code of length m with an isotopically propelinear structure $(M,\Sigma,\star)$ and $M'=\{(y_1,\dots,y_r,x_2,\dots,x_m):(y_1,\dots,y_r)\in E_4^r,\ y_1\oplus y_2\oplus\dots\oplus y_r=x_1,\ (x_1,\dots,x_m)\in M\}$.*

Then $(M',\Delta,\star)$ is an isotopically propelinear structure on the MDS *code M' with the multi-permutation $\delta_z=(\tau_{y,1},\dots,\tau_{y,r},\sigma_{x,2},\dots,\sigma_{x,m})$ assigned to $z=(y_1,\dots,y_r,x_2,\dots,x_m)$, where $\tau_{y,s}$ is defined in (3) taken $\sigma_{x,1}$ as the permutation σ, for any $s\in\{1,2,\dots,r\}$.*

Proof. It is easy to see that the code M' has minimum distance 2, length $m+r-1$ and size 4^{r+m-2}, i.e., it is an MDS code over E_4. Recall that, by definition, $\sigma_{x,1}$ is the multi-permutation assigned to a codeword $x=(x_1,\dots,x_m)$.

By definition of a propelinear structure if a codeword z of M' is obtained from a codeword x of M by replacing the first coordinate x_1 with the sequence of elements $y_1,\dots,y_r$ from E_4, such that $y_1\oplus\dots\oplus y_r=x_1$, then $\delta_z=(\tau_{y,1},\dots,\tau_{y,r},\sigma_{x,2},\dots,\sigma_{x,m})$.

The code M' equipped with the permutations defined above was proved to be isotopically transitive, see [6]. Now, we show that this structure is isotopically propelinear. In order to do so, following Definition 1, we need to show that $\delta_{\delta_z(z')} = \delta_z \circ \delta_{z'}$, where $\delta_z, \delta_{z'}, \delta_{\delta_z(z')}$ are the assigned permutations to the elements $z, z', \delta_z(z')$, respectively.

Let $z = (y_1, \dots, y_r, x_2, \dots, x_m)$ and $z' = (y'_1, \dots, y'_r, x'_2, \dots, x'_m)$ be two codewords of M', i.e.

$$
\begin{aligned}
y_1 \oplus \dots \oplus y_r &= x_1, \\
y'_1 \oplus \dots \oplus y'_r &= x'_1,
\end{aligned} \tag{4}
$$

where $x = (x_1, \dots, x_m), x' = (x'_1, \dots, x'_m) \in M$. The permutations assigned to z and z' are:

$$
\begin{aligned}
\delta_z &= (\tau_{y,1}, \dots, \tau_{y,r}, \sigma_{x,2}, \dots, \sigma_{x,m}) \\
\delta_{z'} &= (\tau_{y',1}, \dots, \tau_{y',r}, \sigma_{x',2}, \dots, \sigma_{x',m}).
\end{aligned}
$$

We have $\delta_z(z') = (\tau_{y,1}(y'_1), \dots, \tau_{y,r}(y'_r), \sigma_{x,2}(x'_2), \dots, \sigma_{x,m}(x'_m))$ and, using Lemma 7: $\tau_{y,1}(y'_1) \oplus \dots \oplus \tau_{y,r}(y'_r) = \sigma_{x,1}(y'_1 \oplus \dots \oplus y'_r)$. From this equality and (4) we see that $\delta_z(z')$ is obtained by substituting the first coordinate of $\sigma_x(x') = (\sigma_{x,1}(x'_1), \dots, \sigma_{x,m}(x'_m))$ with the sequence of elements $\tau_{y,1}(y'_1), \dots, \tau_{y,r}(y'_r)$ and $\tau_{y,1}(y'_1) \oplus \dots \oplus \tau_{y,r}(y'_r) = \sigma_{x,1}(x'_1)$. Therefore, $\delta_z(z')$ belongs to M'. From the isotopic propelinearity of $(M, \Sigma, \star)$, we have that the permutation $\sigma_x \circ \sigma_{x'}$ is assigned to the codeword $\sigma_x(x')$ of M, so the multi-permutation $\delta_{\delta_z(z')}$ coincides with $\delta_z \circ \delta_{z'}$ in each one of the jth positions, for $r+1 \leqslant j \leqslant m+r-1$.

For the first r positions, by the definition of $(M', \Delta, \star)$, we have

$$
\delta_{\delta_z(z'),s}(\alpha) = \tau_{\delta_z(z'),s}(\alpha) = \sigma_{x,1} \circ \sigma_{x',1}(\alpha) \oplus \tau_{y,1}(y'_1) \oplus \dots \oplus \tau_{y,r}(y'_r) \oplus \tau_{y,s}(y'_s) \tag{5}
$$

for $s = 1, \dots, r$. It remains to prove that the permutation (5) coincides with $\tau_{z,s} \circ \tau_{z',s}$ for $s = 1, \dots, r$. For any s above, using Lemma 6 and Lemma 7, the above equality (5) comes to:

$$
\begin{aligned}
\tau_{\delta_z(z'),s}(\alpha) &= \sigma_{x,1}(\sigma_{x',1}(\alpha)) \oplus \sigma_{x,1}(y'_1 \oplus \dots \oplus y'_r) \oplus \sigma_{x,1}(y'_s) \oplus \sigma_{x,1}(0) \oplus y_s \\
&= \sigma_{x,1}(\sigma_{x',1}(\alpha)) \oplus \sigma_{x,1}(x'_1 \oplus y'_s) \oplus y_s \\
&= \sigma_{x,1}\big(\sigma_{x',1}(\alpha) \oplus x'_1 \oplus y'_s\big) \oplus \sigma_{x,1}(0) \oplus y_s \\
&= \tau_{z,s}(\sigma_{x',1}(\alpha) \oplus \sigma_{x',1}(0) \oplus y'_s) = \tau_{z,s}(\tau_{z',s}(\alpha)).
\end{aligned}
$$

□

Potapov [6] considered quasigroups of the following form:

$$
f(x_1, \dots, x_{n-1}) = (x_1 \oplus \dots \oplus x_{i_1}) * (x_{i_1+1} \oplus \dots \oplus x_{i_2}) * \dots * (x_{i_{m-2}+1} \oplus \dots \oplus x_{n-1}),
$$

where $1 \leqslant i_1 \leqslant \dots \leqslant i_{m-1} \leqslant n-1$ (in throughout what follows, we denote this quasigroup with $f_{i_1,\dots,i_{m-2}}$), and proved the transitivity property of any MDS code corresponding to a quasigroup of this type. In this section we show the isotopic propelinearity of these MDS codes.

Indeed, let M be the code $\{(y_1,\ldots,y_{m-1},y_1*\ldots*y_{m-1}) : y_j\in E_4, j=1,2,\ldots,m-1\}$. This code is isotopically propelinear with the permutation $\sigma_y=(\sigma_{y,1},\ldots,\sigma_{y,m-1},\sigma_{y,m})$ assigned to the codeword $y=(y_1,\ldots,y_{m-1},y_1*\ldots*y_{m-1})$, where $\sigma_{y,j}(\alpha)=\alpha*y_j$, for $1\leqslant j\leqslant m-1$ and $\sigma_{y,m}(\alpha)=\alpha*y_1*\ldots*y_{m-1}$. In order to obtain the code $M'=\{(x,f_{i_1,\ldots,i_{m-2}}(x) : x\in E_4^{n-1}\}$ we apply $m-1$ times the construction (2) to every coordinate j, $1\leqslant j\leqslant m-1$. By Proposition 8, the code M' is isotopically propelinear. In other words, we obtain the following statement.

Corollary 9. *Let $M'=\{(x,f_{i_1,\ldots,i_{m-2}}(x)) : x\in E_4^{n-1}\}$. Then there exists an isotopically propelinear structure $(M',\Sigma,\star)$, with the multi-permutation σ_x assigned to a codeword x being such that*

$$\sigma_{x,i_j+t}(\alpha)=(\alpha*(x_{i_j+1}\oplus\ldots\oplus x_{i_{j+1}}))\oplus x_{i_j+t}, \tag{6}$$

for $1\leqslant t\leqslant i_{j+1}-i_j$ and $0\leqslant j\leqslant m-2$, $i_0=0$.

As a consequence of the isotopic propelinearity of these codes we have the same lower bound for the number of nonequivalent isotopically propelinear codes as the one in [6] for the isotopically transitive codes.

Corollary 10. *There exist at least $\frac{1}{4(n-1)\sqrt{3}}e^{\pi\sqrt{2(n-1)/3}}(1+o(1))$ nonequivalent quaternary isotopically propelinear* MDS *codes of length n, for n going to infinity.*

3 Propelinear extended perfect codes

In this section we prove that binary extended perfect Phelps codes [5] constructed from isotopically propelinear MDS codes are propelinear.

First of all, we give some additional notations from [6] and prove some necessary statements. Let C_0 be the binary extended Hamming code of length 4:

$$C_0=\{(0,0,0,0),(1,1,1,1)\}.$$

Bellow, we follow the same notations as in [6]. We identify the elements $0,1,2,3$ of E_4 with the 4th, 1st, 2nd, 3rd coordinate positions of $\mathbb{F}_2^4$, respectively, so we have $e_0=(0,0,0,1)$, $e_1=(1,0,0,0)$ $e_2=(0,1,0,0)$ $e_3=(0,0,1,0)$. Now, define the codes in $\mathbb{F}_2^4$:

$$C_a^r=C_0+(1+r)e_0+e_a,\ \text{for } r\in\{0,1\},\ a\in E_4. \tag{7}$$

The codes $\{C_a^r\}_{r=0,1;a\in E_4}$ give a partition of $\mathbb{F}_2^4$ into extended perfect codes and the codes $\{C_a^0\}_{a\in E_4}$ give a partition of the binary full even weight code into extended perfect codes.

All extended perfect codes of length 4 can be represented as the cosets of C_0 and, more specifically, if b is in $C_{a'}^{r'}$ then:

$$b+C_a^r=C_{a\oplus a'}^{r+r'}. \tag{8}$$

Let S_4 be the symmetric group of permutations over E_4. In [6] it was shown that the action of a permutation of coordinates (fixing the 4th coordinate) on the partition $\{C_a^0\}_{a\in E_4}$ can be represented as the action of a permutation of the cosets in this partition.

Proposition 11. *For every $\sigma \in S_4$ the following holds:*

$$C^r_{\sigma(a)} + e_{\sigma(0)} + e_0 = \pi(C^r_a),$$

for all $a \in E_4$ and $r \in \{0, 1\}$, where $\pi(\alpha) = \sigma(\alpha) \oplus \sigma(0)$ fixes the 4th coordinate.

Proof. Using (7), we get that

$$C^r_{\sigma(a)} + e_{\sigma(0)} + e_0 = C_0 + (1 + r)e_0 + e_{\sigma(a)} + e_{\sigma(0)} + e_0.$$

Since $e_0 + e_{\sigma(a)} + e_{\sigma(0)} + e_{\sigma(0)\oplus\sigma(a)}$ is the all-zeros or the all-ones vector, we obtain the desired property:

$$C^r_{\sigma(a)} + e_{\sigma(0)} + e_0 = C_0 + (1 + r)e_0 + e_{\pi(a)} = \pi(C_0 + (1 + r)e_0 + e_a) = \pi(C^r_a).$$

□

Proposition 12. *The mapping $\sigma \to \pi$ is a homomorphism from S_4 to S_3. The kernel of the homomorphism is the set of permutations of type $\sigma(\alpha) = \alpha \oplus b$, for some $b \in E_4$ and for any α.*

Proof. Let $\pi(\alpha) = \sigma(\alpha) \oplus \sigma(0)$ and $\pi'(\alpha) = \sigma'(\alpha) \oplus \sigma'(0)$ for any $\alpha \in E_4$. Using Lemma 6, we have

$$\pi'(\pi(\alpha)) = \sigma'(\sigma(\alpha) \oplus \sigma(0)) \oplus \sigma'(0) = \sigma'(\sigma(\alpha)) \oplus \sigma'(\sigma(0))$$

for any $\alpha \in E_4$.

The claim about the kernel is trivial. □

Now, consider the Phelps concatenation construction [5], see also [12]:

$$C = \bigcup_{(h_1,\ldots,h_n)\in H} \bigcup_{(a_1,\ldots,a_n)\in M} C^{h_1}_{a_1} \times \ldots \times C^{h_n}_{a_n}, \tag{9}$$

where H is an extended Hamming code of length n, M is a quaternary MDS code of length n and codes $C^{h_i}_{a_i}, i = 1, \ldots, n$, are defined in (7). Using the construction (9), Potapov in [6] found a large class of transitive codes taking M being isotopically transitive. These MDS codes correspond to quasigroups

$$f(x_1, \ldots, x_{n-1}) = (x_1 \oplus \ldots \oplus x_{i_1}) * (x_{i_1+1} \oplus \ldots \oplus x_{i_2}) * \ldots * (x_{i_{m-2}+1} \oplus \ldots \oplus x_{n-1}), \tag{10}$$

for any $i_1, \ldots, i_{m-2}$, such that $1 \leqslant i_1 < \ldots < i_{m-2} < n - 1$. In the previous section we proved that all these isotopically transitive MDS codes are isotopically propelinear. Now, we show that all Potapov's transitive extended perfect binary codes are propelinear too.

Theorem 13. *Let M be a quaternary isotopically propelinear MDS code of length n, H be a binary extended Hamming code of length n. Then, the code*

$$C = \bigcup_{(h_1,\ldots,h_n)\in H} \bigcup_{(a_1,\ldots,a_n)\in M} C^{h_1}_{a_1} \times \ldots \times C^{h_n}_{a_n}$$

is a binary propelinear extended perfect code of length $4n$.

Proof. Let $(M, \Sigma, \star)$ be an isotopically propelinear structure on the code M. Let $\sigma_a = (\sigma_{a,1}, \ldots, \sigma_{a,n})$ be the multi-permutation assigned to a codeword $a = (a_1, \ldots, a_n)$ of M. For any $i \in \{1, \ldots, n\}$, let π_{a_i} be the permutation defined by Proposition 11 when σ is equal to $\sigma_{a,i}$:

$$C^r_{\sigma_{a,i}(b)} + e_{a_i} + e_0 = \pi_{a_i}(C^r_b), \text{ for any b} \in E_4, \text{ and any } r \in \{0, 1\}.$$

To every codeword c in the class $C^{h_1}_{a_1} \times \ldots \times C^{h_n}_{a_n}$, where $(h_1, \ldots, h_n) \in H$ we assign the permutation $\pi_a = (\pi_{a_1}, \ldots, \pi_{a_n})$ acting on $4n$ coordinates in the following way: if $x = (x_1, \ldots, x_n)$ is a word of length $4n$ such that x_i is a word of length 4 for any i, then $\pi_a(x_1, \ldots, x_n) = (\pi_{a_1}(x_1), \ldots, \pi_{a_n}(x_n))$. In [6] it is proved that the code C with these permutations is transitive. We now show that it is propelinear too.

Let $c \in C^{h_1}_{a_1} \times \ldots \times C^{h_n}_{a_n}$; $c' \in C^{h'_1}_{a'_1} \times \ldots \times C^{h'_n}_{a'_n}$ and let π_a and $\pi_{a'}$ be the permutations assigned to the codewords c and c', respectively. To show that C is propelinear it is enough to show that the permutation assigned to the class $c + \pi_a(C^{h'_1}_{a'_1} \times \ldots \times C^{h'_n}_{a'_n})$ is $\pi_a \circ \pi_{a'}$.

Let us find more convenient representation for the class $c + \pi_a(C^{h'_1}_{a'_1} \times \ldots \times C^{h'_n}_{a'_n})$. By the definition of π_a we have the following equalities:

$$\pi_a(C^{h'_1}_{a'_1} \times \ldots \times C^{h'_n}_{a'_n}) = \pi_{a_1}(C^{h'_1}_{a'_1}) \times \ldots \times \pi_{a_n}(C^{h'_n}_{a'_n})$$

$$= (C^{h'_1}_{\sigma_{a,1}(a'_1)} + e_{a_1} + e_0) \times \ldots \times (C^{h'_n}_{\sigma_{a,n}(a'_n)} + e_{a_n} + e_0).$$

Since $c \in C^{h_1}_{a_1} \times \ldots \times C^{h_n}_{a_n}$, from the last equality and using (8) we obtain

$$c + \pi_a(C^{h'_1}_{a'_1} \times \ldots \times C^{h'_n}_{a'_n}) = C^{h'_1+h_1}_{\sigma_{a,1}(a'_1)} \times \ldots \times C^{h'_n+h_n}_{\sigma_{a,n}(a'_n)}.$$

Thus, we have to find the permutation corresponding to the codewords of the class $C^{h'_1+h_1}_{\sigma_{a,1}(a'_1)} \times \ldots \times C^{h'_n+h_n}_{\sigma_{a,n}(a'_n)}$. By propelinearity of M, the multi-permutation assigned to $(\sigma_{a,1}(a'_1), \ldots, \sigma_{a,n}(a'_n)) \in M$ is $\sigma_a \circ \sigma_{a'} = (\sigma_{a,1} \circ \sigma_{a',1}, \ldots, \sigma_{a,n} \circ \sigma_{a',n})$. Finally, from Proposition 12 and the definitions of permutations on C, we obtain that $\pi_a \circ \pi_{a'}$ is the permutation assigned to the codewords of the class $C^{h'_1+h_1}_{\sigma_{a,1}(a'_1)} \times \ldots \times C^{h'_n+h_n}_{\sigma_{a,n}(a'_n)} = c + \pi_a(C^{h'_1}_{a'_1} \times \ldots \times C^{h'_n}_{a'_n})$. □

And, finally, considering MDS codes corresponding to quasigroups of type

$$f_{i_1 \ldots i_{m-2}}(a_1 \ldots a_{n-1}) = (a_1 \oplus \ldots \oplus a_{i_1}) * (a_{i_1+1} \oplus \ldots \oplus a_{i_2}) * \ldots * (a_{i_{m-2}+1} \oplus \ldots \oplus a_{n-1}),$$

applying the results of the previous section, and using the same considerations as in [6] we obtain:

Corollary 14. *There exist at least* $\frac{1}{8n^2\sqrt{3}} e^{\pi\sqrt{2n/3}}(1 + o(1))$ *nonequivalent propelinear extended perfect binary codes of length* $4n$*, for* n *going to infinity.*

4 Normality

The concept of binary normalized propelinear codes was introduced in [3]. A propelinear structure on a binary code C is called *normalized* if the codewords of the same coset of the code C by the kernel have the same assigned permutation.

In this section we analyze the propelinear structure defined in Theorem 13, when MDS code corresponds to the quasigroup

$$f_{i_1 \dots i_{m-2}}(a_1 \dots a_{n-1}) = (a_1 \oplus \dots \oplus a_{i_1}) * (a_{i_1+1} \oplus \dots \oplus a_{i_2}) * \dots * (a_{i_{m-2}+1} \oplus \dots \oplus a_{n-1}).$$

We show that the structure is normalized if and only if m is odd. For even m it is not normalized, however we can find an exponential number of propelinear representations of the Phelps codes, which are normalized propelinear.

By $\mathrm{Ker}(M)$, the *kernel* of an arbitrary MDS code M over E_4 we mean the collection of all its codewords a such that

$$a \oplus M = M.$$

We begin with describing the kernel of the MDS and Phelps codes.

Proposition 15. *Let M be a* MDS *code of length n, H be an extended Hamming code of length n,*

$$C = \bigcup_{h \in H} \bigcup_{a \in M} C_{a_1}^{h_1} \times \dots \times C_{a_n}^{h_n}.$$

Then a codeword c from the code $C_{a'_1}^{h'_1} \times \dots \times C_{a'_n}^{h'_n}$ belongs to $\mathrm{Ker}(C)$ if and only if the word $a' = (a'_1, \dots, a'_n)$ belongs to $\mathrm{Ker}(M)$.

Proof. Let c be a codeword in $C_{a'_1}^{h'_1} \times \dots \times C_{a'_n}^{h'_n}$. We know that $(h'_1, h'_2, \dots, h'_n) + H = H$, so

$$C = \bigcup_{h \in H} \bigcup_{a \in M} C_{a_1}^{h_1 + h'_1} \times \dots \times C_{a_n}^{h_n + h'_n}.$$

From (8) we have:

$$c + C = c + \bigcup_{h \in H} \bigcup_{a \in M} C_{a_1}^{h_1 + h'_1} \times \dots \times C_{a_n}^{h_n + h'_n} = \bigcup_{h \in H} \bigcup_{a \in M} C_{a_1 \oplus a'_1}^{h_1} \times \dots \times C_{a_n \oplus a'_n}^{h_n}.$$

Therefore, c is in $\mathrm{Ker}(C)$ if and only if a' is in $\mathrm{Ker}(M)$. □

From this point and further on we represent a codeword of a MDS code corresponding to a quasigroup f as $(a, f(a))$.

Proposition 16. *Let f be a (n-1)-quasigroup of order 4 and M the* MDS *code $M = \{(a, f(a)) : a \in E_4^{n-1}\}$. The codeword $(a', f(a'))$ belongs to $\mathrm{Ker}(M)$ if and only if $f(a \oplus a') = f(a) \oplus f(a')$, for all $a \in E_4^{n-1}$.*

Proof. If $(a', f(a')) \in \mathrm{Ker}(M)$ then $(a', f(a')) \oplus M = M$, so, for all $a \in E_4^{n-1}$ we have $(a' \oplus a, f(a') \oplus f(a)) \in M$. So $(a' \oplus a, f(a') \oplus f(a))$ and $(a \oplus a', f(a \oplus a'))$ both belong to M, therefore, $f(a) \oplus f(a') = f(a \oplus a')$ and vice versa. □

Now, we focus on the case when MDS code corresponds to the quasigroup

$$f_{i_1\dots i_{m-2}}(a_1\dots a_{n-1})=(a_1\oplus\dots\oplus a_{i_1})*(a_{i_1+1}\oplus\dots\oplus a_{i_2})*\dots*(a_{i_{m-2}+1}\oplus\dots\oplus a_{n-1}).$$

We need a technical lemma. In through out what follows, u^{-1} denotes the inverse element of u in the group $(E_4,*)$.

Lemma 17.

(i) For all $u\in E_4$ it is true $u'\oplus u=\begin{cases} u'*u & \text{for } u'\in\{0,2\};\\ u'*u^{-1} & \text{for } u'\in\{1,3\}.\end{cases}$

(ii) There is no $u'\in E_4$ such that the equality

$$u'\oplus(u*v)=u'*u^{-1}*v$$

holds for any u and v from E_4.

Proof. The first statement follows directly from the definitions of operations $\oplus$ and $*$.

Let us prove the second statement. If u' belongs to $\{0,2\}$, then by the first statement we have $u'\oplus(u*v)=u'*u*v$ for any u and v in E_4, but for $u\in\{1,3\}$ we have: $u'*u*v\neq u'*u^{-1}*v$.

If u' belongs to $\{1,3\}$, then by the first statement we obtain $u'\oplus(u*v)=u'*u^{-1}*v^{-1}$ for any u and v in E_4, but for $v\in\{1,3\}$ we have $u'*u^{-1}*v^{-1}\neq u'*u^{-1}*v$. □

We now describe the kernel of a particular MDS code.

Proposition 18. *Let $M=\{(a,a_1*\dots*a_{m-1}):a=(a_1,\dots,a_{m-1})\in E_4^{m-1}\}$. Then*

$$\mathrm{Ker}(M)=\begin{cases}\{(a',a'_1*\dots*a'_{m-1})\mid a'\in\{0,2\}^{m-1}\}, & \text{if } m \text{ is odd},\\ \{(a',a'_1*\dots*a'_{m-1})\mid a'\in\{0,2\}^{m-1}\cup\{1,3\}^{m-1}\}, & \text{if } m \text{ is even}.\end{cases}$$

Proof. By Proposition 16 it is true that $(a',a'_1\dots a'_{m-1})\in\mathrm{Ker}(M)$ if and only if for any $a\in E_4^{m-1}$:

$$(a'_1\oplus a_1)*\dots*(a'_{m-1}\oplus a_{m-1})=(a'_1*\dots*a'_{m-1})\oplus(a_1*\dots*a_{m-1}). \tag{11}$$

Let the first k coordinates of a' be from $\{0,2\}$ and the last $m-1-k$ coordinates be from $\{1,3\}$. Now, from Lemma 17 we can express the operation $\oplus$ in (11) by the operation $*$: $(a'_1\oplus a_1)*\dots*(a'_{m-1}\oplus a_{m-1})=a'_1*a_1*\dots*a'_k*a_k*a'_{k+1}*a_{k+1}^{-1}*\dots*a'_{m-1}*a_{m-1}^{-1}$, so the condition (11) of belonging to the kernel of M can be rewritten as:

$$(a'_1*\dots*a'_{m-1})\oplus(a_1*\dots*a_{m-1})=a'_1*\dots*a'_{m-1}*a_1*\dots*a_k*a_{k+1}^{-1}*\dots*a_{m-1}^{-1},$$

for any $a\in E_4^{m-1}$.

Let u' be equal to $a'_1*\dots*a'_{m-1}$; u be equal to $a_1*\dots*a_k$ and v be equal to $a_{k+1}*\dots*a_{m-1}$. Using these notations, the property of belonging to the kernel is equivalent to:

(i) If $k=0$, then $a' \in \{1,3\}^{m-1}$ and $u' \oplus v = u' * v^{-1}$ implying, by Lemma 17, that $u' \in \{1,3\}$. Therefore m is even.

(ii) If $k=m-1$, then $a' \in \{0,2\}^{m-1}$ and $u' \oplus u = u' * u$ implying, by Lemma 17, that $u' \in \{0,2\}$, which is true for any m.

(iii) If $0<k<m-1$, then $u' \oplus (u*v) = u' * u * v^{-1}$, which is impossible, again according to Lemma 17.

□

For the general case we have the following description for the kernels:

Theorem 19. *Let $M = \{(a, f_{i_1,\dots,i_{m-2}}(a)) : a \in E_4^{n-1}\}$ be a* MDS *code. Then, $(a, f_{i_1,\dots,i_{m-2}}(a))$ belongs to* Ker(M) *if and only if the word of partial sums*

$$(\oplus_{j=1}^{i_1} a_j, \oplus_{j=i_1+1}^{i_2} a_j, \dots, \oplus_{j=i_{m-2}+1}^{n-1} a_j)$$

belongs to $\{0,2\}^{m-1}$ for odd m and to $\{0,2\}^{m-1} \cup \{1,3\}^{m-1}$ for even m.

Proof. Directly from Proposition 18. □

From Theorem 19 and Proposition 15 we obtain:

Corollary 20. *Let C be the code obtained by Phelps construction*

$$C = \bigcup_{h \in H} \bigcup_{(a, f_{i_1,\dots,i_{m-2}}(a)) \in M} C_{a_1}^{h_1} \times \dots \times C_{a_{n-1}}^{h_{n-1}} \times C_{f_{i_1,\dots,i_{m-2}}(a_1,\dots,a_{n-1})}^{h_n}.$$

If m is odd then $|\mathrm{Ker}(C)| = 2^{3n-2-\log_2(n)}$ and if m is even $|\mathrm{Ker}(C)| = 2^{3n-1-\log_2(n)}$.

Theorem 21. *Let*

$$C = \bigcup_{h \in H} \bigcup_{(a, f_{i_1,\dots,i_{m-2}}(a)) \in M} C_{a_1}^{h_1} \times \dots \times C_{a_{n-1}}^{h_{n-1}} \times C_{f_{i_1,\dots,i_{m-2}}(a_1,\dots,a_{n-1})}^{h_n},$$

and let $(C, \Pi, \star)$ be the propelinear structure on C, defined in Theorem 13. Then

(i) $(C, \Pi, \star)$ is normalized, if m is odd;

(ii) $(C, \Pi, \star)$ is not normalized and there exist at least 2^{n-2} different normalized propelinear structures on C, if m is even.

Proof. Let M' be the MDS code $\{(a, f_{i_1,\dots,i_{m-2}}(a)) : a \in E_4^{n-1}\}$ and $(a', f_{i_1,\dots,i_{m-2}}(a')) \in \mathrm{Ker}(M')$. Let the multi-permutation $(\sigma_{a',1}, \dots, \sigma_{a',n-1}, \sigma_{a',n})$ be assigned to the word $(a', f_{i_1,\dots,i_{m-2}}(a'))$ of M'. Let t be such that $i_s + 1 \leqslant t \leqslant i_{s+1}$, for $s = 0, \dots, m$, $i_0 = 0, i_{m-1} = n-1$. Then, by the definition of the propelinear structure on M', see Corollary 9, we have

$$\sigma_{a',t}(\alpha) = ((a_{i_s+1} \oplus \dots \oplus a_{i_{s+1}}) * \alpha) \oplus a_t \oplus a_{i_s+1} \oplus \dots \oplus a_{i_{s+1}},$$

$$\sigma_{a',n}(\alpha) = (a_1 \oplus \ldots \oplus a_{i_1}) * (a_{i_1+1} \oplus \ldots \oplus a_{i_2}) * \ldots * (a_{i_{m-2}+1} \oplus \ldots \oplus a_{n-1}) * \alpha.$$

By Theorem 19, $a_{i_s+1} \oplus \ldots \oplus a_{i_{s+1}}$ belongs to $\{0,2\}$ or $\{1,3\}$ simultaneously for any $s = 0, \ldots, m-2$.

Let $a_{i_s+1} \oplus \ldots \oplus a_{i_{s+1}}$ be from $\{0,2\}$. Then, by Lemma 17, $\sigma_{a',t}(\alpha) = (a_{i_s+1} \oplus \ldots \oplus a_{i_{s+1}}) \oplus \alpha \oplus a_t \oplus a_{i_s+1} \oplus \ldots \oplus a_{i_{s+1}} = \alpha \oplus a_t$. Therefore, according to the assignment of permutations to the codewords of C (see Theorem 13) and by Proposition 12 (ii), the permutation $\pi_{(a',f_{i_1,\ldots,i_{m-2}}(a'))} = (\pi_{(a',f_{i_1,\ldots,i_{m-2}}(a')),1}, \ldots, \pi_{(a',f_{i_1,\ldots,i_{m-2}}(a')),n})$ assigned to a codeword c in the class $C^{h'_1}_{a'_1} \times \ldots \times C^{h'_{n-1}}_{a'_{n-1}} \times C^{h'_n}_{f_{i_1,\ldots,i_{m-2}}(a')}$ is the identity. Taking into account the description of kernel given in Theorem 19, the structure is normalized for odd m.

Let $a_{i_s+1} \oplus \ldots \oplus a_{i_{s+1}}$ be from the set $\{1,3\}$. Then, by Lemma 17, $\sigma_{a',t}(\alpha) = ((a_{i_s+1} \oplus \ldots \oplus a_{i_{s+1}}) \oplus \alpha^{-1} \oplus a_t \oplus a_{i_s+1} \oplus \ldots \oplus a_{i_{s+1}} = \alpha^{-1} \oplus a_t$. It is easy to see that the permutation $\sigma_{a',t}(\alpha) = \alpha^{-1} \oplus a_t$ is not a permutation of "linear type", i.e. cannot be expressed as $\alpha \oplus u$ for some fixed u from E_4. So, according to the assignment of permutations to the codewords of C (see Theorem 13), and again by Proposition 12(ii), the permutation $\pi_{(a',f_{i_1,\ldots,i_{m-2}}(a'))} = (\pi_{(a',f_{i_1,\ldots,i_{m-2}}(a')),1}, \ldots, \pi_{a',f_{i_1,\ldots,i_{m-2}}(a'),n})$ assigned to the codeword c in $C^{h'_1}_{a'_1} \times \ldots \times C^{h'_{n-1}}_{a'_{n-1}} \times C^{h'_n}_{f_{i_1,\ldots,i_{m-2}}(a')}$ is not the identity.

Hence, for even m, one half of the codewords of the kernel have assigned the identity permutation, and the second half have assigned the same non-identity permutation.

Note that in case of even m, there exist several normalized propelinear structures. According to the proof of the Theorem 13, every codeword is assigned a permutation of the form $\pi_a = (\pi_{a_1}, \ldots, \pi_{a_n})$, where $\pi_{a_i} \in S_4$ fixes one coordinate (see Proposition 11), for any $i = 1, \ldots, n$. Hence, π_{a_i} could only have order 2 or 3, for all $i = 1, \ldots, n$, so π_a has order 2, 3 or 6. However, orders 3 and 6 can not occur. Given a propelinear code $(D, \Pi, \star)$ with $|D|$ being a power of 2, we have that $|\Pi = \{\pi_x : x \in C\}|$ is also a power of 2. Indeed, the map $x \mapsto \pi_x$ is group homomorphism from the group D onto the permutation group Π. Therefore, for any codeword x, the order of π_x is a power of 2 as well. We conclude that all permutations assigned to the codewords of C are involutions and, in this case, C has $|\{\pi_x : x \in \mathrm{Ker}(C)\}|^{\log(|C|)-\dim(\mathrm{Ker}(C))}$ different normalized propelinear structures (a proof of this fact is given in [3]). Substituting the value of $\dim(\mathrm{Ker}(C))$ obtained from Corollary 20, we obtain 2^{n-2} different structures. □

Acknowledgments

This work was supported in part by the Spanish MICINN under Grants MTM2009-08435 and TIN2010-17358, and by the Catalan AGAUR under Grant 2009SGR1224. The second author was supported by the Grants RFBR 12-01-00448, 12-01-31098 and 13-01-00463. The work of the fourth author was partially supported by the Grant RFBR 12-01-00631-a.

The authors are grateful to the referee for the useful remarks which allowed to improve the presentation of the results.

References

[1] J. Borges, J. Rifà, "A characterization of 1-perfect additive codes", *IEEE Trans. Inform. Theory*, vol. 45, pp. 1688–1697, 1999.

[2] J. Borges, J. Rifà, F. I. Solov'eva, "On properties of propelinear and transitive binary codes", *In Proceedings of the 3rd International Castle Meeting on Coding Theory and Applications (3ICMCTA)*, Cardona, Spain, September 11-15, 2011, pp. 65-70. ISBN: 978-84-490-2688-1.

[3] J. Borges, I. Yu. Mogilnykh, J. Rifà, F. I. Solov'eva, "Structural properties of binary propelinear codes", *Advances in Mathematics of Communications*, Volume 6, No. 3, pp. 329-346, 2012.

[4] A. R. Hammons, P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, P. Solé, "The Z4-linearity of Kerdock, Preparata, Goethals and related codes," *IEEE Trans. Inform. Theory*, vol. 40, n. 1, pp. 301–319, 1994.

[5] K. T. Phelps, "A General Product Construction for Error Correcting Codes", *SIAM J. Algebraic and Discrete Methods* vol. 5, pp. 224–228, 1984.

[6] V. N. Potapov, "A lower bound for the number of transitive perfect codes", *J. of Appl.and Industrial Math.*, vol. 1, n. 3, pp. 373–379, 2007.

[7] K. T. Phelps, J. Rifà, "On binary 1-perfect additive codes: some structural properties", *IEEE Trans. on Inform. Theory*, vol. 48, pp. 2587–2592, 2002.

[8] J. Rifà, J. M. Basart, L. Huguet, "On completely regular propelinear codes", in *Proc. 6th Int. Conference, AAECC-6*, n. 357 LNCS, pp. 341–355, 1989.

[9] J. Rifà, J. Pujol, "Translation invariant propelinear codes", *IEEE Trans. on Inform. Theory*, vol. 43, pp. 590–598, 1997.

[10] F. I. Solov'eva, "On transitive codes", in *Proc. Int. Workshop on Discrete Analysis and Operation Research*, Novosibirsk, Russia, p. 99, 2004.

[11] F. I. Solov'eva, "On the construction of transitive codes", *Problems of Information transmission*, vol. 41, n. 3, pp. 204–211, 2005.

[12] V. A. Zinov'ev, "Generalized Concatenated Codes". *Problems of Information transmission*, vol. 12, n. 3, pp. 23–31, 1976.