Thirteenth International Workshop on Algebraic and Combinatorial Coding Theory
June 15-21, 2012, Pomorie, Bulgaria *pp. 93–98*

A lower bound on the number of nonequivalent propelinear extended perfect codes*

J. Borges, J. Rifà {joaquim.borges,josep.rifa}@autonoma.edu
Universitat Autònoma de Barcelona, Spain

I.Yu. Mogilnykh, F.I. Solov'eva {ivmog84,fainasoloveva}@gmail.com
Sobolev Institute of Mathematics, Novosibirsk State University, Russia

Abstract. In this paper we prove that there exists an exponential number of nonequivalent propelinear extended perfect binary codes of length growing to infinity. All such codes have small rank, which is one unit greater than the dimension of the extended Hamming code of the same length. We investigate the properties of these codes.

1 Introduction

Let $E_q = \{0, 1, \ldots, q-1\}$ be a set of q elements, where we distinguish one of them and write it as 0. We call *words* the elements of the cartesian product E_q^n equipped with the *Hamming distance d*. Denote by $\mathbf{0}$ the word $(0, \ldots, 0)$. 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 $\sigma = (\sigma_1, \ldots, \sigma_n)$ will be called a *multi-permutation*. The composition $\sigma \circ \sigma'$ of multi-permutations σ and σ' is the 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. Denote by $\mathrm{Iso}(C)$ the *isometry group* of the code C, that is, the subgroup of all isometries of E_q^n fixing C.

Definition 1. A q-ary code C of length n is called *propelinear* if for any codeword x there exists a 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, $(\sigma_z; \pi_z) = (\sigma_x; \pi_x)(\sigma_y; \pi_y)$.

*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 third author was supported by the Grant of the President of the Russian Federation for Young Russian Researchers (project no. MK-1700.2011.1), by the Grants RFBR 09-01-00244; 10-01-00616-a. The fourth author was supported by the Grants RFBR 10-01-00424-a; 12-01-00631-a.

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]. As in the binary case, in the q-ary case, given a q-ary propelinear code C we can define the operation $\star$ as $x \star v = (\sigma_x; \pi_x)(v)$ for any $x \in C$, and any $v \in E_q^n$. We denote by $(C, \pi, \sigma, \star)$ the *propelinear structure*, and sometimes by $(C, \star)$ when we do not require any information about permutations. The code C with operation $\star$ form a group. Note that there can exist many different propelinear structures on a propelinear code, including nonisomorphic ones (for binary case see [3]).

In [1, 7–9], some properties of binary propelinear codes are studied. In [2,3], the relations between classes of propelinear and transitive codes are investigated, the classes of propelinear and transitive codes are different – the binary Best code of length 10 is shown to be transitive, but not propelinear. The previous lower bound on the number of nonequivalent propelinear extended perfect binary codes of length $n = 2^m, m \geq 4$ was $\lfloor \log_2(m/2) \rfloor^2$, see [2, 3], the codes have different ranks. In the paper we prove that all transitive extended perfect binary codes from [6] are propelinear. Despite the fact that the new class of propelinear codes obtained in this paper is larger than the old class from [2,3], it does not cover the old one, since all the codes in the new class have small rank, which is one unit greater than the dimension of the extended Hamming code of the same length. In [2,3] there were found propelinear codes with bigger ranks, therefore the result [2, 3] keeps current.

2 Isotopic propelinear MDS codes

A q-ary code of length n, satisfying the property (i) in Definition 1 with $\pi_x = Id_n$ for any x in the code is called an *isotopic 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 *isotopic propelinear*, if for any $x \in C$ it holds $\pi_x = Id_n$. If there is an isotopic propelinear structure on a code C, we call C *isotopic propelinear*.

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 $\{(x, f(x)) : x \in E_q^{m-1}\}$.

Consider $E_4 = \{0, 1, 2, 3\}$. We use two operations defined in E_4: $*$ to refer to the addition considering the elements in E_4 as elements in $\mathbb{Z}_4$, and $\oplus$ 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 $0 \to (0,0), 1 \to (0,1), 2 \to (1,1), 3 \to (1,0)$.

Next examples were used in [6] to obtain 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 isotopic 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 isotopic propelinear with the 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 isotopic transitive MDS code M and the MDS code from Example 2, using the following concatenation construction:

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

for some fixed i, $1 \le i \le m-1$, and for any $r = 1, 2, \ldots$

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: $g(x_1, \ldots, x_{i-1}, y_1, \ldots, y_r, x_{i+1}, \ldots, x_{m-1}) = f(x_1, \ldots, x_{i-1}, y_1 \oplus y_2 \oplus \ldots \oplus y_r, x_{i+1}, \ldots, x_{m-1})$. Given a permutation σ on the elements of E_4 and a word $y = (y_1, \ldots, y_r)$ in E_4^r such that $y_1 \oplus \ldots \oplus y_r = \sigma(0)$ we define the permutations $\tau_{y,1}, \ldots, \tau_{y,r}$ in E_4:

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

Proposition 1. *Let $(M, \sigma, \star)$ be a quaternary isotopic propelinear MDS code of length m and $M' = \{(y_1, \ldots, y_r, x_2, \ldots, x_m)\}$, where $(y_1, \ldots, y_r) \in E_4^r$, $y_1 \oplus y_2 \oplus \ldots \oplus y_r = x_1$, $(x_1, \ldots, x_m) \in M$. Then $(M', \delta, \star)$ is an isotopic propelinear structure on the MDS code M' with $\delta_z = (\tau_{y,1}, \ldots, \tau_{y,r}, \sigma_{x,2}, \ldots, \sigma_{x,m})$, assigned to the word $z = (y_1, \ldots, y_r, x_2, \ldots, x_m)$, where $\tau_{y,s}$ is defined in (2) with $\sigma_{x,1}$ as the permutation σ, for any $s \in \{1, 2, \ldots, r\}$.*

Potapov [6] considered quasigroups of the following form: $f(x_1, \ldots, x_{n-1}) = (x_1 \oplus \ldots \oplus x_{i_1}) * (x_{i_1+1} \oplus \ldots \oplus x_{i_2}) * \ldots * (x_{i_{m-2}+1} \oplus \ldots \oplus x_{n-1})$, where $1 \le i_1 \le \ldots \le i_{m-1} \le n-1$ (we denote this quasigroup by $f_{i_1,\ldots,i_{m-2}}$), and proved the transitivity of any MDS code corresponding to a quasigroup of this type. Applying construction (1) and Proposition 1 a proper number of times, we prove that the code $M' = \{(x, f_{i_1,\ldots,i_{m-2}}(x) : x \in E_4^{n-1}\}$ is isotopic propelinear:

Corollary 1. *Let $M' = \{(x, f_{i_1,\ldots,i_{m-2}}(x)) : x \in E_4^{n-1}\}$. Then there exists an isotopic propelinear structure $(M', \sigma, \star)$, with the multi-permutation σ_x assigned to a codeword x being such that $\sigma_{x,i_j+t}(\alpha) = (\alpha * (x_{i_j+1} \oplus \ldots \oplus x_{i_{j+1}})) \oplus x_{i_j+t}$, for $1 \le t \le i_{j+1} - i_j$ and $0 \le j \le m-2$, $i_0 = 0$.*

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

3 Propelinear extended perfect codes

Let C_0 be the binary extended Hamming code of length 4: $C_0 = \{(0,0,0,0), (1,1,1,1)\}$. Let e_a mean the all-zeroes vector in E_2^4, except for the ath coordinate which is 1, $e_0 = e_4$. Define the codes in E_2^4:

$$C_a^r = C_0 + (1+r)e_0 + e_a, \text{ for } r \in \{0,1\},\ a \in E_4. \tag{3}$$

Now consider the Phelps concatenation construction [5], see also [11]:

$$C = \bigcup_{(h_1,\ldots,h_n)\in H} \bigcup_{(a_1,\ldots,a_n)\in M} C_{a_1}^{h_1} \times \ldots \times C_{a_n}^{h_n}, \tag{4}$$

where H is an extended Hamming code of length n, M is a quaternary MDS code of length n and codes $C_{a_i}^{h_i}, i = 1,\ldots,n$, are defined in (3). Using the construction (4), Potapov [6] found a large class of transitive extended perfect codes taking M to be one of the MDS codes corresponding to quasigroups

$$f_{i_1,\ldots,i_{m-2}}(x_1,\ldots,x_{n-1}) = (x_1\oplus\ldots\oplus x_{i_1})*(x_{i_1+1}\oplus\ldots\oplus x_{i_2})*\ldots*(x_{i_{m-2}+1}\oplus\ldots\oplus x_{n-1}), \tag{5}$$

for any $i_1,\ldots,i_{m-2}$, such that $1 \le i_1 < \ldots < i_{m-2} < n-1$.

In the following theorem we show that extended perfect Phelps code [5] constructed from an isotopic propelinear MDS codes is propelinear. The proof is based on a constructive approach, which we omit here and can be found in [4].

Theorem 1. *Let* M *be a quaternary isotopic propelinear MDS code of length* n*,* H *be a binary extended Hamming code of length* n*. Then, the code (4) is a binary propelinear extended perfect code of length* $4n$*.*

And finally considering Potapov MDS codes corresponding to quasigroups of the type $f_{i_1,\ldots,i_{m-2}}(a_1,\ldots,a_{n-1}) = (a_1 \oplus \ldots \oplus a_{i_1}) * (a_{i_1+1} \oplus \ldots \oplus a_{i_2}) * \ldots * (a_{i_{m-2}+1} \oplus \ldots \oplus a_{n-1})$ and applying the results of the previous section we obtain:

Theorem 2. *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. These are the codes (4), corresponding to Potapov MDS codes:*

$$\bigcup_{h\in H} \bigcup_{(a_1,\ldots,a_{n-1})\in E_4^{n-1}} C_{a_1}^{h_1} \times \ldots \times C_{a_{n-1}}^{h_{n-1}} \times C_{f_{i_1,\ldots,i_{m-2}}(a_1,\ldots,a_{n-1})}^{h_n}.$$

All such codes have small rank, which is one unit greater than the dimension of the extended Hamming code of the same length.

4 Kernels

In this section we describe the kernels of Phelps codes, considered by Potapov in [6] and establish whether the propelinear structures of the codes defined in Theorem 2 are normalized or not.

Further on, we consider only quaternary MDS codes. The *kernel* of a quaternary MDS code M is the collection of the codewords preserving the code under translation, $Ker(M) = \{a \in M : a \oplus M = M\}$, where $\oplus$ means component-wise "addition": $a \oplus b = (a_1 \oplus b_1, \ldots, a_n \oplus b_n)$.

Proposition 2. *Let M be a quaternary MDS code of length n, H be an extended Hamming code of length n, $C = \bigcup_{h \in H} \bigcup_{a \in M} C_{a_1}^{h_1} \times \ldots \times C_{a_n}^{h_n}$. Then a codeword from the code $C_{a'_1}^{h'_1} \times \ldots \times C_{a'_n}^{h'_n}$ belongs to $Ker(C)$ if and only if the word $a' = (a'_1, \ldots, a'_n)$ belongs to $Ker(M)$.*

From now on, we consider a codeword of a MDS code corresponding to a quasigroup f as $(a, f(a))$. For the case of Potapov MDS codes, i.e., MDS code corresponding to the quasigroup $f_{i_1,\ldots,i_{m-2}}(a_1, \ldots, a_{n-1}) = (a_1 \oplus \ldots \oplus a_{i_1}) * (a_{i_1+1} \oplus \ldots \oplus a_{i_2}) * \ldots * (a_{i_{m-2}+1} \oplus \ldots \oplus a_{n-1})$, we obtain the following criterion:

Theorem 3. *Let $M = \{(a, f_{i_1,\ldots,i_{m-2}}(a)) : a \in E_4^{n-1}\}$ be a MDS code. Then $(a, f_{i_1,\ldots,i_{m-2}}(a))$ belongs to $Ker(M)$ if and only if the word of partial sums $(\oplus_{j=1}^{i_1} a_j, \oplus_{j=i_1+1}^{i_2} a_j, \ldots, \oplus_{j=i_{m-2}+1}^{n-1} a_j)$ belongs to $\{0,2\}^{m-1}$ for odd m and to $\{0,2\}^{m-1} \cup \{1,3\}^{m-1}$ for even m.*

From Theorem 3 and Proposition 2 we obtain the values for the size of kernel of Phelps codes, corresponding to Potapov MDS codes:

Corollary 3. *Let C be the code obtained by Phelps construction*

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

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

5 Normality

A propelinear structure on a binary code is called *normalized* if the codewords of the same coset of the code by the kernel have the same assigned permutation [3]. Analyzing the propelinear structure on Phelps codes corresponding to Potapov MDS code from Theorem 2 (see [4]), and using the description of kernels obtained in previous section, we obtain

Theorem 4. *Let $(C, \pi, \sigma, \star)$ be the propelinear structure in (4), where*

$$C = \bigcup_{h \in H} \bigcup_{(a_1,\ldots,a_{n-1}) \in E_4^{n-1}} C_{a_1}^{h_1} \times \ldots \times C_{a_{n-1}}^{h_{n-1}} \times C_{f_{i_1,\ldots,i_{m-2}}(a_1,\ldots,a_{n-1})}^{h_n}.$$

Then, if m is odd, $(C, \pi, \sigma, \star)$ is normalized, otherwise it is not normalized, but there exist at least 2^{n-2} different normalized propelinear structures on C.

References

[1] J. Borges, J. Rifà, "A characterization of 1-perfect additive codes", *IEEE Trans. Inform. Theory*, **45**, 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, 65-70. ISBN: 978-84-490-2688-1.5

[3] J. Borges, I. Yu. Mogilnykh, J. Rifà, F. I. Solov'eva, "Structural properties of binary propelinear codes", *Advanced Math. Commun.*, submitted.

[4] J. Borges, I. Yu. Mogilnykh, J. Rifà, F. I. Solov'eva, "On the number of nonequivalent propelinear extended perfect codes", *Advanced Math. Commun.*, submitted.

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

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

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

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

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

[10] F. I. Solov'eva, "On the construction of transitive codes", *Probl. Inform. Transm.*, **41**, 3, 204–211, 2005.

[11] V. A. Zinov'ev, "Generalized Concatenated Codes". *Probl. Inform. Transm.*, **12**, 3, 23–31, 1976.