ISIT'2013 1569717475

Rank Spectrum of Propelinear Perfect Binary Codes

George K. Guskov
Sobolev Institute of Mathematics
Novosibirsk, Russia
Email: m1lesnsk@gmail.com

Ivan Yu. Mogilnykh
Sobolev Institute of Mathematics,
Novosibirsk State University
Novosibirsk, Russia
Email: ivmog@math.nsc.ru

Faina I. Solov'eva
Sobolev Institute of Mathematics,
Novosibirsk State University
Novosibirsk, Russia
Email: sol@math.nsc.ru

***Abstract*—It is known [4] that for any numbers $n = 2^m - 1, m \geq 4$ and r, such that $n - \log(n+1) \leq r \leq n$ there exists a perfect binary code of length n and rank r. We show that there exists a propelinear such code of length n, excluding, may be, $n = r = 63$, $n = 127$, $r \in \{126, 127\}$ and $n = r = 2047$.**

I. Introduction

Denote by $\mathbb{F}^n$ a vector space of dimension n over the Galois field $GF(2)$ with respect to the *Hamming distance* $d(\cdot,\cdot)$, which is defined as the number of coordinates in which vectors differ.

By an *automorphism* of $\mathbb{F}^n$ we mean a distance-preserving automorphism of the corresponding vector space. It is known that the action of any automorphism of $\mathbb{F}^n$ can be described using a translation $v \in \mathbb{F}^n$ and a permutation π in the following way:

$$(v, \pi)(x) = v + \pi(x)$$

for any $x \in \mathbb{F}^n$. The set of all automorphisms $Aut(\mathbb{F}^n)$ of $\mathbb{F}^n$:

$$Aut(\mathbb{F}^n) = \{(v, \pi) \mid v \in \mathbb{F}^n, \pi \in S_n\}$$

forms a group under the composition $(u, \pi) \circ (v, \tau) = (u + \pi(v), \pi\tau)$ for all $(u, \pi), (v, \tau) \in Aut(\mathbb{F}^n)$. Here, and throughout the entire paper, we use $\pi\tau(x) = \pi(\tau(x))$ for $x \in \mathbb{F}^n$.

An arbitrary subset of $\mathbb{F}^n$ is called a *binary code* of length n. The *minimum distance* of a code C is the minimum value of the Hamming distance between any two different codewords from C. Two codes C and D are said to be *equivalent* if $C = \phi(D)$, for some automorphism ϕ of $\mathbb{F}^n$. By $Sym(C)$ we denote the group of all coordinate permutations that fix C set-wise and call it the *symmetry group* of C. By $Aut(C)$ we denote the group of all automorphisms of $\mathbb{F}^n$ fixing the code set-wise, and we call it the *automorphism group* of C. Note that in some papers, code automorphisms are defined as coordinate permutations fixing the code set-wise.

A code C is called *single-error-correcting perfect* (or perfect, for the sake of brevity) if for any vector $x \in \mathbb{F}^n$ there exists exactly one vector $y \in C$ such that $d(x, y) \leq 1$. It is well known that such codes exist if and only if $n = 2^m - 1, m \geq 1$. For any $n = 2^m - 1, m \geq 1$, there is exactly one, up to equivalence, linear perfect code of length n and it is called the *Hamming code*.

Throughout the paper we assume that $C \in \mathbb{F}^n$ is a perfect code of length n containing the all-zero vector $\mathbf{0}^n$ with n coordinates. For such code C, its kernel K is defined as the set of all codewords that leave C invariant under translation, that is,

$$K = \{x \in C \mid x + C = C\}.$$

The kernel K of C is a linear subspace of $\mathbb{F}^n$ and the code C is a union of the cosets of K. The rank $rank(C)$ of a code C is the dimension of the linear span $< C >$.

Let Π be a mapping of the codewords from C into the admissible permutations: $x \mapsto \pi_x$: $(x, \pi_x) \in Aut(C)$, such that $\pi_{(x,\pi_x)y} = \pi_x\pi_y$. Then we can define a group operation on C:

$$x \star y = (x, \pi_x)y.$$

A code equipped with the operation defined above is called *a propelinear structure* on C and is denoted by $(C, \Pi, \star)$ (simply $(C, \star)$ if we do not need any information on Π). A code is called *propelinear* if it has a propelinear structure.

It is easy to see that any propelinear code is transitive. Recall that a code C is called *transitive* if $Aut(C)$ acts transitively on C. Some transitive codes were constructed and studied in [14], [15]. Propelinear codes were introduced in 1989 by Rifà et al. [10] and investigated further in [11], [2], [3]. It is proven that perfect propelinear codes can be obtained by using the well known Vasil'ev construction, see [12], and by the Mollard construction, see the proof in [2]. In [3] an exponential number of nonequivalent propelinear perfect codes having small ranks is presented.

By the rank or kernel spectrum of a perfect code we mean the set of all possible values of one of these characteristics for codes of the fixed length n. In 1994 Etzion and Vardy [4] solved the rank problem of perfect binary codes for any length $n \geq 15$ using switchings of minimal i-components. They showed that the rank spectrum is $\{n-log(n+1), \ldots, n\}$, where $n - log(n+1)$ is the rank of the Hamming code and n is the so-called *full rank*. The same approach was used by Phelps and LeVan [9] in 1995 to solve the kernel problem of perfect codes of length n with $n \geq 15$. The kernel spectrum is $\{1, 2, \ldots, n-m-2, n-m\}$, notice that there are no perfect binary codes of length n with the kernel dimension $n-m-1$. The rank and kernel problem can be formulated as following: find the spectrum of pairs (r, k) that are attainable as the rank r and the kernel dimension k of some propelinear perfect code of length n. The rank and kernel problem for perfect binary codes was solved in [1] with the exception of one case of full

rank perfect codes of length $n = 31$ with kernel dimension 21 which was covered by Heden later in [6].

In this paper we solve the rank problem for propelinear perfect codes: we show that the rank spectra of perfect codes and propelinear perfect codes coincide, except, possibly, full ranks for lengths 63, 127, 2047 and the rank 126 for codes of length 127.

II. Propelinear full rank perfect codes of lengths 15 and 31

Let us recall the Vasil'ev construction [16]. Let C be a perfect binary code of length $(n-1)/2$. Let λ be any mapping from C into the set $\{0,1\}$ and $|x| = x_1 + \cdots + x_{\frac{n-1}{2}}$, where $x = (x_1, \ldots, x_{\frac{n-1}{2}})$, $x_i \in \{0,1\}$. The code

$$C^n = \{(x+y, |x| + \lambda(y), x) \mid x \in \mathbb{F}^{(n-1)/2}, y \in C\} \quad (1)$$

of length n is perfect and called *Vasil'ev code*.

Let $(C, \star)$ be a propelinear structure on C, then a homomorphism λ from $(C, \star)$ into Z_2 is called a *propelinear homomorphism* (or *propelinear function*).

Theorem 1: (See [12]) Let $(C, \star)$ be a propelinear structure on a perfect binary code C of length $(n-1)/2$, λ be a propelinear function. Then the Vasil'ev code C^n is propelinear perfect.

In general, the problem of checking propelinearity of a given code seems to be rather hard. In order to avoid the issue, the concept of a normalized propelinear code was introduced in [2]. Recall that a propelinear structure $(C, \Pi, \star)$ is called *normalized propelinear* if the same permutation is assigned to the codewords from the same coset by kernel: $|\{\pi_x : x \in K + u\}| = 1$, for any $u \in C$.

Computer search for a propelinear structure in [2] is carried out in a way that the number of possible candidates for propelinear structures increases exponentially as the dimension of the kernel decreases by unity, meaning that full rank codes seem to be out of a computational reach (as they have relatively small kernels). To solve this problem, we require codes to have trivial symmetry groups. In this case, there is just one opportunity for a assignment of permutations, in other words, $Aut(C)$ is acting regularly on codewords of C, which implies propelinearity of C (see [13]).

Lemma 1: A transitive code with trivial symmetry group is normalized propelinear.

Among perfect codes of length 15 from the database [8], we found 44 transitive codes with trivial symmetry groups, 39 of them having full rank and 5 having rank 14. Note that the existence of propelinear perfect codes of length 15 of all possible ranks, with the exception of a full rank code, was previously shown in [2].

Lemma 2: The rank spectra of perfect codes and propelinear perfect codes of length 15 coincide.

We give two more lemmas concerning the Vasil'ev codes. Note that for a given propelinear code of length n the set of the assigned permutations $\Pi(C) = \{\pi_x : x \in C\}$ forms a subgroup of S_n, see [2]. Some of the propelinear homomorphisms of C into Z_2 can be described using those of the group $\Pi(C)$.

Lemma 3: Let $(C, \Pi, \star)$ be a propelinear code. Any group homomorphism λ' of $(\Pi(C), \circ)$ into Z_2 yields a propelinear homomorphism λ of $(C, \Pi, \star)$ defined in the following way: $\lambda(x) := \lambda'(\pi_x)$.

Lemma 4: Let C^n be a code given by the Vasil'ev construction (1) with the function λ. Then

$rank(C^n) = rank(\{(y, \lambda(y)) : y \in C\}) + (n-1)/2$ and $rank(C) + (n-1)/2 \le rank(C^n) \le rank(C) + (n+1)/2$.

By Lemma 2 we have propelinear perfect codes of length 15 of any rank. If we take $\lambda \equiv 0$ for these codes in the Vasil'ev construction, we get the rank spectrum for length 31, with the exception of the full rank.

In order to construct a full rank propelinear perfect binary code of length 31, another computer search was carried out. We considered propelinear homomorphisms of propelinear full rank perfect codes of length 15 from Lemma 3 and using Lemma 4 checked if the Vasil'ev codes with these functions are full rank codes. The search turned out to give a positive result:

Theorem 2: There exists a full rank normalized propelinear perfect binary code of length 31.

III. Rank problem

In this section we solve the rank problem for propelinear perfect codes using the results of the previous section as well as the Vasil'ev and the Mollard constructions. Recall the Mollard construction for binary codes. Let C^t and C^m be any two perfect codes of lengths t and m, respectively, containing all-zero vectors.

Let $x = (x_{11}, \ldots, x_{1m}, x_{21}, \ldots, x_{2m}, \ldots, x_{t1}, \ldots, x_{tm}) \in \mathbb{F}^{tm}$. The generalized parity-check functions $p_1(x)$ and $p_2(x)$ are defined as $p_1(x) = (\sigma_1, \sigma_2, \ldots, \sigma_t) \in \mathbb{F}^t$, $p_2(x) = (\sigma'_1, \sigma'_2, \ldots, \sigma'_m) \in \mathbb{F}^m$, where $\sigma_i = \sum_{j=1}^m x_{ij}$ and $\sigma'_j = \sum_{i=1}^t x_{ij}$. Let f be any function from C^t to $\mathbb{F}^m$. The code

$$\mathcal{M}(C^t, C^m) = \{(x, y + p_1(x), z + p_2(x) + f(y))\},$$

where $x \in \mathbb{F}^{tm}, y \in C^t, z \in C^m$, is a perfect binary Mollard code of length $n = tm + t + m$, see [7]. The abbreviation $\mathcal{M}(C^t, C^m)$ indicates the initial codes C^t and C^m and their lengths. It is clear that the codes of other lengths t' and m' can also yield a perfect code $\mathcal{M}(C^{t'}, C^{m'})$ with the same parameters as the code $\mathcal{M}(C^t, C^m)$. Both these codes could be equal, different, or even nonequivalent.

Theorem 3: (See [2]) Let C^t and C^m be arbitrary propelinear perfect binary codes of lengths t and m, respectively. Let f be a propelinear homomorphism from C^t to $\mathbb{F}^m$. Then the Mollard code $\mathcal{M}(C^t, C^m)$ is a propelinear perfect binary code of length $n = tm + t + m$.

Further we consider the Mollard codes with the function $f \equiv \mathbf{0}^m$.

Lemma 5: (See [15]) The perfect binary Mollard code $\mathcal{M}(C^t, C^m)$ of length $n = tm + t + m$ with $f \equiv \mathbf{0}^m$ has rank $tm + r(C^t) + r(C^m)$.

Applying the results of Section II, the Vasil'ev construction for small n, by induction based on the Mollard construction starting with $n = 2^8 - 1$ we get the following

Theorem 4: For any $n = 2^m - 1, m \geq 4$ and arbitrary r, satisfying $n - \log(n+1) \leq r \leq n$ excluding the cases of $n = r = 63$; $n = 127$, $r \in \{126, 127\}$ and $n = r = 2047$, there exists a propelinear perfect binary code of length n and rank r.

IV. Conclusion

In our opinion the open cases $n = r = 63$ and $n = r = 127$ can be covered by the Vasil'ev construction applied to full-rank propelinear perfect codes of lengths 31 and 63 using special propelinear functions. The last two open cases $n = 127$, $r = 126$ and $n = r = 2^{11} - 1$ could then be covered by the Vasil'ev construction with the zero function λ and by the Mollard construction $\mathcal{M}(C^{2^4-1}, C^{2^7-1})$ or $\mathcal{M}(C^{2^5-1}, C^{2^6-1})$ with the zero function f respectively.

The question of nontrivial lower and upper bounds on kernel dimension, as well as the rank and kernel problem for propelinear perfect codes are still open.

All computer searches have been carried out using the Magma [17] software package. Some properties of perfect transitive codes of length 15 and extended perfect transitive codes of length 16 such as rank, dimension of the kernel, order of the automorphism group can be found in [5].

Acknowledgment

The second author was supported by the Grants RFBR 12-01-00448-a, 12-01-31098 and 13-01-00463. The work of the third author was partially supported by the Grant RFBR 12-01-00631-a.

The authors would like to cordially thank Fedor Dudkin for useful discussions.

References

[1] S. V. Avgustinovich, O. Heden, F. I. Solov'eva, "On the rank and kernel problem for perfect codes," *Problems of Inform. Transm.*, vol. 39, no. 4, pp. 341–345, 2003.

[2] J. Borges, I. Yu. Mogilnykh, J. Rifà, F. I. Solov'eva, "Structural properties of binary propelinear codes," *Advances in Math. of Commun.*, vol. 6, no. 3, pp. 329–346, 2012.

[3] J. Borges, I. Yu. Mogilnykh, J. Rifà, F. I. Solov'eva, "On the number of nonequivalent propelinear extended perfect codes," *Electronic Journal of Combinatorics*, submitted, 2013.

[4] T. Etzion, A. Vardy, "Perfect binary codes: Constructions, properties and enumeration," *IEEE Trans. Inform. Theory*, vol. 40, no. 3, pp. 754–763, 1994.

[5] G. K. Guskov, F. I. Solov'eva, "Properties of perfect transitive binary codes of length 15 and extended perfect transitive binary codes of length 16," *ArXiv*, http://arxiv.org/abs/1210.5940, 2012.

[6] O. Heden, "A full rank perfect code of length 31," *Des., Codes and Cryptogr.*, vol. 38, no. 1, pp. 125–129, 2006.

[7] M. Mollard, "A generalized parity function and its use in the construction of perfect codes," *SIAM J. Alg. Discrete Math*, vol. 7, no. 1, pp. 113–115, 1986.

[8] P. R. J. Östergård, O. Pottonen, "The perfect binary one-error-correcting codes of length 15: Part I – Classification," *ArXiv*, http://arxiv.org/src/0806.2513v3/anc/perfect15, 2009.

[9] K. T. Phelps, M. J. LeVan, "Kernels of nonlinear Hamming codes," *Des., Codes and Cryptogr.*, vol. 6, pp. 247–257, 1995.

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

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

[12] J. Rifà, J. Pujol, J. Borges, "1-Perfect Uniform and Distance Invariant Partitions," *Appl. Algebra in Engeneering, Commun. and Computing*, vol. 11, pp. 297–311, 2001.

[13] 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.

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

[15] F. I. Solov'eva, "On the construction of transitive codes," *Problems of Information transmission*, vol. 41, no. 3, pp. 204–211, 2005.

[16] Y. L. Vasil'ev, "On nongroup close-packed codes," *Probl. Kibernetiki*, vol. 8, pp. 92–95, 1962. In Russian, English translation in *Probleme der Kybernetik*, vol. 8, pp. 92–95, 1965.

[17] W. Bosma, J. Cannon, C. Playoust, "The Magma algebra system. I. The user language," *J. Symbolic Comput.*, vol. 24, pp. 235–265, 1997.