S©MR ISSN 1813-3304

СИБИРСКИЕ ЭЛЕКТРОННЫЕ
МАТЕМАТИЧЕСКИЕ ИЗВЕСТИЯ

Siberian Electronic Mathematical Reports
http://semr.math.nsc.ru

Том 17, стр. 1451–1462 (2020) УДК 519.725
DOI 10.33048/semi.2020.17.101 MSC 94B60

COORDINATE TRANSITIVITY OF A CLASS OF EXTENDED PERFECT CODES AND THEIR SQS

I.YU. MOGILNYKH, F.I. SOLOV'EVA

Abstract. We continue the study of the class of binary extended perfect propelinear codes constructed in the previous paper and consider their permutation automorphism (symmetry) groups and Steiner quadruple systems. We show that the automorphism group of the SQS of any such code coincides with the permutation automorphism group of the code. In particular, the isomorphism classes of these SQS's are complete invariants for the isomorphism classes of these codes. We obtain a criterion for the point transitivity of the automorphism group of SQS of proposed codes in terms of GL-equivalence (similar to EA-type equivalence for permutations of F^r). Based on these results we suggest a new construction for coordinate transitive and neighbor transitive extended perfect codes.

Keywords: extended perfect code, concatenation construction, transitive code, neighbor transitive code, transitive action, regular subgroup, isomorphism problem, transitive Steiner quadruple system, coordinate transitive code.

1. Introduction

Propelinear and linear codes share many similar properties and concepts. Among propelinear codes there are several important classes of optimal and optimal-related codes such as Z_4 and Z_2Z_4-linear, some binary perfect and extended perfect, Preparata, Kerdock codes, etc. For more details we refer to the survey in the introductory part of [17].

The topic of this paper is concerned to the classical problem in coding theory: can a linear (cyclic, propelinear) code in a particular class be compactly represented, e.g. by its

Mogilnykh, I.Yu., Solov'eva, F.I., Coordinate transitivity of a class of extended perfect codes and their SQS.

This work was supported by the Ministry of Science and Higher Education of Russia (agreement No. 075-02-2020-1479/1).

Received March, 30, 2020, published September, 14, 2020.

minimum weight codewords? This is true for the Hamming codes, the Reed-Muller codes and the class of extended cyclic codes related to Gold functions [4], [16]. We refer to these works for the surveys on this question. These type of problems often arise in testing theory [11] and can find an application in cryptography.

Another property of interest is the k-transitivity of the permutation automorphism group of a code. An analogous concept for designs is known as the k-point transitivity of their automorphism groups. The *permutation automorphism group* of a code C denoted by $\mathrm{PAut}(C)$ (also called the symmetry group of C) is the setwise stabilizer of C in S_n, i.e.

$$\mathrm{PAut}(C) = \{\pi : \pi(C) = C\}.$$

As far as perfect codes with minimum distance 3 are concerned, the Hamming codes are the only known examples with transitive permutation automorphism group (actually 2-transitive). In the case of extended perfect codes the only known nonlinear examples are the Z_4-linear extended perfect codes with transitive permutation automorphism group [12]. Other well-known families of binary codes with the k-transitive permutation automorphism groups include Reed–Muller codes for $k = 3$ (in particular extended Hamming codes), extended BCH codes when $k = 2$, classes of extended Preparata codes for $k = 1$. In the q-ary case there are affine-invariant codes with 2-transitive permutation automorphism group [3]. In the paper we are focused on the case of 1-transitive action, and a code is called *coordinate transitive* if its permutation automorphism group acts transitively on the set of its coordinate positions.

Gillespie and Praeger [5] suggested the following concept. A code C is called *k-neighbor transitive* if its automorphism group acts transitively on C_i, for any i, $0 \leq i \leq k$, where C_i is the set of words at distance exactly i from C. When k equals the covering radius of the code it is called completely transitive (originally Solé [21] considered only linear codes). In what follows we call a Steiner quadruple system with a 1-point transitive automorphism group and a 1-neighbor transitive code briefly a point transitive SQS and a neighbor transitive code respectively.

It is easy to see that a binary transitive code containing the all-zero vector with k-transitive permutation automorphism group is k-neighbor transitive, where k is not larger than the covering radius of the code. Moreover in case of minimum distance at least three a binary code is neighbor transitive if and only if the code is transitive and coordinate transitive, see [7]. We see that Reed–Muller and extended BCH codes [14] are k-neighbor transitive, where k is 3 and 2 respectively and known extended Preparata codes [9], [8] are neighbor transitive. The Nordstrom–Robinson code, which is completely transitive, is an exceptional case, see [5]. Note that for any known extended Preparata code P which is not the Nordstrom–Robinson code, its automorphism group also acts transitively on P_4, see [15], but not transitively on P_2, see [5].

We note that the Mollard construction [19] applied to any coordinate transitive (neighbor transitive) extended perfect codes with trivial function gives a coordinate transitive (neighbor transitive) extended perfect code. In the previous paper [17] we constructed a class of extended perfect propelinear codes utilizing regular subgroups of the general affine group of the binary vector space in the concatenation construction [22]. We also solved the rank and the kernel problems for these codes. Any code of length n and dimension of the kernel $n - 2\log_2 n$ from this class was shown to be a non-Mollard, i.e. can not be obtained by the Mollard construction [19] with arbitrary function.

In the current paper we investigate the permutation automorphism groups of the codes from [17] and their Steiner quadruple systems and find a new construction for coordinate transitive and neighbor transitive extended perfect codes. The Steiner quadruple systems of these codes can be described by a particular case of Construction A* in the survey of Lindner and Rosa [13]. We prove that the permutation automorphism group of the codes and of their Steiner quadruple systems coincide. Moreover, we prove that the Steiner quadruple systems are complete invariants for the isomorphism classes of these codes. As a consequence we are able to find that there are exactly 64 isomorphism classes of such codes of length 32 with the kernels of dimension 22. All these codes are non-Mollard.

We obtain an expression for the point transitivity of Steiner quadruple systems of proposed codes in terms similar to extended affine equivalence for permutations of the vectors of the binary vector space [2]. For length $n = 16$ and 32 all codes with the kernels of dimension $n-2\log_2 n$ and ranks $n-1$ or $n-2$ have transitive permutation automorphism groups. Exploitation of these codes having relatively small kernels gives a series of new neighbor transitive extended perfect codes of any admissible length $n, n \neq 8, 64$ different from Mollard and Z_4-linear codes. We also note that similar properties hold for a class of propelinear Hadamard codes, which suits an informal "duality" concept.

2. Preliminaries

2.1. **Codes.** We omit here some definitions that can be found in [17]. By F^n we denote the vector space of dimension n over the Galois field F of two elements with respect to the Hamming metric.

Let π be a permutation of the coordinate positions of vectors in F^n that acts as follows: $\pi(y) = (y_{\pi^{-1}(1)}, \dots, y_{\pi^{-1}(n)})$ for $y \in F^n$. Let S_n be the symmetric group of the set of coordinate positions $\{1, \dots, n\}$. Consider the transformation (x, π), where $x \in F^n$, that maps a binary vector y as

$$(x, \pi)(y) = x + \pi(y).$$

The *composition* of two transformations (x, π) and (y, π') is defined as follows:

$$(x, \pi) \cdot (y, \pi') = (x + \pi(y), \pi \circ \pi'),$$

where $\pi \circ \pi'$ is the composition of permutations π and π' acting as

$$\pi \circ \pi'(i) = \pi(\pi'(i))$$

for any $i \in \{1, \dots, n\}$. The *automorphism group* $\mathrm{Aut}(F^n)$ of F^n is defined as the group of all such transformations (x, π) with respect to the composition. Codes C and D are *isomorphic* if there are $x \in F^n$ and $\pi \in S_n$ such that $x + \pi(C) = D$. We write it as follows: $C \sim_{(x,\pi)} D$ and $C \sim_{\pi} D$ if x is the all-zero vector. *The automorphism group* $\mathrm{Aut}(C)$ of a code C is the setwise stabilizer of C in $\mathrm{Aut}(F^n)$. A code C is *transitive* (*propelinear*) if there is a subgroup of $\mathrm{Aut}(C)$ acting transitively (regularly) on the codewords of C.

The Hamming code is an example when the code and its complement [15] are propelinear codes. For the extended Nordstrom–Robinson code we have the following result obtained by a computer (the results for N and N_4 are known [15]).

Proposition 1. *Let N be the extended Nordstrom–Robinson code, $N = N_0$, N_1, N_2, N_3 and N_4 be the distance partition with respect to N. For any $i \in \{0, 1, 3, 4\}$ there is a subgroup of* $\mathrm{Aut}(N)$ *that acts regularly on N_i and there is no such subgroup for N_2.*

Let us consider one simple property of transitive codes which will be useful for our further investigations.

Proposition 2. *Let C and D be transitive codes of length n containing the all-zero vector such that $C \sim_{(x,\pi)} D$. Then $C \sim_{\pi'} D$ for some permutation π' of S_n.*

Proof. Let $C \sim_{(x,\pi)} D$, i.e. we have $\pi(C) = x + D$. Since C and D contain all-zero vectors, the latter equality implies that x is in D. Taking into account that D is transitive we have $x + D = \pi''(D)$ for some permutation $\pi'' \in S_n$. Hence we have $C = \pi^{-1}\pi''(D)$. □

Let the coordinates of the vector space F^{2^r} be indexed by the vectors of F^r. The all-zero vector is denoted by $\mathbf{0}$ and its length will always be clear from the context. Define an extended Hamming code of length 2^r as follows:

$$\mathcal{H} = \{x \in F^{2^r} : \sum_{a : x_a = 1} a = \mathbf{0}, \ \mathrm{wt}(x) \equiv 0 (\mathrm{mod}\ 2)\}.$$

The concatenation of two vectors $x \in F^{r'}$ and $y \in F^{r''}$ is denoted by $x|y$. For codes C and D by $C \times D$ we denote the code $\{x|y : x \in C,\, y \in D\}$. Let π', π'' be permutations on the vectors of $F^{r'}$ and $F^{r''}$ respectively. By $\pi'|\pi''$ we denote the permutation on the vectors of $F^{r'+r''}$ acting on the concatenations $x|y$ of the vectors $x \in F^{r'}$ and $y \in F^{r''}$ as follows: $(\pi'|\pi'')\,(x|y) = \pi'(x)|\pi''(y)$. In particular, if π' and π'' are permutations of the coordinate positions of $F^{r'}$ and $F^{r''}$, then $(\pi'|\pi'')$ is a permutation of the coordinate positions of $F^{r'+r''}$.

Let e_a be the vector in F^{2^r} with the only one nonzero position indexed by a vector $a \in F^r$.

Consider the following particular case of the concatenation construction for extended perfect codes [22]:

$$S_\tau = \bigcup_{a \in F^r} (\mathcal{H} + e_a + e_{\mathbf{0}}) \times (\mathcal{H} + e_{\tau(a)} + e_{\tau(\mathbf{0})}), \tag{1}$$

where τ is a permutation of the vectors of F^r. In throughout of what follows we suppose that τ fixes $\mathbf{0}$, so the code S_τ contains the all-zero vector. Note that in [17] the code S_τ is denoted by $S_{\mathcal{H},\tau}$.

Denote the *general linear group* that consists of the nonsingular $r \times r$ matrices over F by $\mathrm{GL}(r,2)$. Consider an affine transformation (a, M), $a \in F^r, M \in \mathrm{GL}(r,2)$. Its action on F^r is defined as

$$(a, M)(b) = a + Mb, \tag{2}$$

$b \in F^r$. The *general affine group* of the space F^r whose elements are $\{(a, M) : a \in F^r, M \in \mathrm{GL}(r,2)\}$ with respect to the composition is denoted by $\mathrm{GA}(r,2)$. The group $\mathrm{GA}(r,2)$ naturally acts on the positions indexed by the vectors of F^r. Let $\sigma_{a,M}$ denote the permutation on the positions of F^{2^r} that corresponds to the affine transformation (a, M). It is well-known that the automorphism group of an extended Hamming code is isomorphic to the general affine group, i.e.

$$\mathrm{Aut}(\mathcal{H}) = \{\sigma_{a,M} : (a, M) \in \mathrm{GA}(r,2)\}.$$

For $a \in F^r$, $M \in \mathrm{GL}(r,2)$ we denote the linear map $\sigma_{\mathbf{0},M}$ by σ_M and denote $C \sim_M D$ if $C \sim_{\sigma_M} D$. When M is the identity matrix we denote the translation $\sigma_{a,M}$ by σ_a. We have the following result.

Proposition 3. *Let τ be a permutation on the vectors of F^r, $\tau(\mathbf{0}) = \mathbf{0}$. The code S_τ is an extended Hamming code if and only if τ is σ_M for some $M \in \mathrm{GL}(r,2)$.*

2.2. **Steiner quadruple systems.** A *Steiner quadruple system of order n* (briefly SQS if we know the order by the context) is a set of quadruples (subsets of size 4) of a point set of size n where every three points from the point set are contained in exactly one quadruple. It is well-known that the supports of the codewords of weight 4 of any extended perfect code containing the all-zero vector form a Steiner quadruple system.

The *automorphism group* of a Steiner quadruple system Q of order n, denoted by $\mathrm{Aut}(Q)$ is the setwise stabilizer of the quadruples of Q in the symmetric group of the pointset of Q. Steiner quadruple systems Q and Q' are *isomorphic* if there is a bijection π between their point sets that sends the quadruples of Q to these of Q'. In this case we write $Q \sim_\pi Q'$. A Steiner quadruple system is called *point transitive* if its permutation automorphism group acts transitively on the set of its points.

By an *affine Steiner quadruple system*, briefly *affine SQS*, we mean the Steiner quadruple system of an extended Hamming code. It is well-known that the Hamming codes of fixed length are unique up to a permutation and therefore any extended Hamming code is spanned by its codewords of weight 4 by Glagolev theorem. We conclude that all affine Steiner quadruple systems are isomorphic.

We now describe the Steiner quadruple system of the code S_τ (see (1)), which we denote by SQS_τ. For any $x, y \in F^{2^r}$ the support of $x|y \in F^{2^{r+1}}$ is denoted by the ordered pair $(\mathrm{supp}(x), \mathrm{supp}(y))$. The pointset of SQS_τ consists of $(\{a\}, \emptyset)$, $(\emptyset, \{a\})$, for all a in F^r and SQS_τ is $Q_0 \cup Q_1 \cup Q_\tau$, where

$$Q_0 = \{(\{a,b,c,d\}, \emptyset) : a,b,c,d \text{ are pairwise distinct vectors of } F^r, a+b+c+d = \mathbf{0}\},$$
$$Q_1 = \{(\emptyset, \{a,b,c,d\}) : a,b,c,d \text{ are pairwise distinct vectors of } F^r, a+b+c+d = \mathbf{0}\},$$
$$Q_\tau = \{(\{a,c\}, \{b,d\}) : a,b,c,d \in F^r, \tau(a+c) = b+d \neq \mathbf{0}\}.$$

For a pair of distinct vectors $a, b \in F^r$ we define the following sets of quadruples:

$$\begin{aligned} Q_0(a,b) = \{(\{a,b,c,d\}, \emptyset) &: c,d \in F^r, c \neq d, a+b+c+d = \mathbf{0}\} \\ \cup\{(\{a,b\}, \{c,d\}) &: c,d \in F^r, \tau(a+b) = c+d \neq \mathbf{0}\}, \\ Q_1(a,b) = \{(\emptyset, \{a,b,c,d\}) &: c,d \in F^r, c \neq d, a+b+c+d = \mathbf{0}\}, \\ \cup\{(\{c,d\}, \{a,b\}) &: c,d \in F^r, \tau(c+d) = a+b \neq \mathbf{0}\}, \end{aligned}$$

and for a pair of vectors $a, b \in F^r$ we define

$$Q_\tau(a,b) = \{(\{a,c\}, \{b,d\}) : c,d \in F^r, \tau(a+c) = b+d \neq \mathbf{0}\}.$$

In other words, $Q_0(a,b)$, $Q_1(a,b)$ and $Q_\tau(a,b)$ are the sets of all quadruples in SQS_τ, that contain the pairs of points $(\{a\}, \emptyset)$ and $(\{b\}, \emptyset)$; $(\emptyset, \{a\})$ and $(\emptyset, \{b\})$; $(\{a\}, \emptyset)$ and $(\emptyset, \{b\})$ respectively.

2.3. **Coordinate transitive Mollard extended perfect codes.** Let C and D be extended perfect codes of lengths t and m respectively, ϕ be a function from C to F^m. The coordinates of the Mollard extended perfect code are pairs (r,s), where $r \in \{1,\dots,t\}$ and $s \in \{1,\dots,m\}$. For a vector $z = (z_{11},\dots,z_{1m},\dots,z_{t1},\dots,z_{tm})$ in F^{tm} we consider

$$p_1(z) = (\sum_{s=1}^{m} z_{1s}, \dots, \sum_{s=1}^{m} z_{ts}), \quad p_2(z) = (\sum_{r=1}^{t} z_{r1}, \dots, \sum_{r=1}^{t} z_{rm}).$$

The Mollard extended perfect code is defined as follows:

$$M(C,D) = \{z \in F^{tm} : p_1(z) \in C, \quad p_2(z) \in \phi(p_1(z)) + D\}.$$

It is not hard to see that $M(C,D)$ is the extension of the Mollard perfect code by overall parity check (the original construction [19] used perfect codes). Analogously to the previous works [23], [18], [1] we now consider embeddings of the permutation automorphism groups of C and D into that of the Mollard code with the all-zero function ϕ. For permutations $\pi \in \mathrm{PAut}(C)$ and $\pi' \in \mathrm{PAut}(D)$ we define $Dub_1(\pi)$ and $Dub_2(\pi')$ acting on the positions of $M(C,D)$ as follows:

$$Dub_1(\pi)(r,s) = (\pi(r), s), \quad Dub_2(\pi')(r,s) = (r, \pi'(s)).$$

It is not hard to see that $Dub_1(\pi)$ and $Dub_2(\pi')$ are permutation automorphisms of $M(C,D)$, see [23], [18], [1].

Proposition 4. *If C and D are coordinate transitive (neighbor transitive) extended perfect codes then $M(C,D)$ with the all-zero function ϕ is a coordinate transitive (neighbor transitive) extended perfect code.*

Proof. If $\mathrm{PAut}(C)$ and $\mathrm{PAut}(D)$ act transitively on the coordinates of C and D, then the group generated by $\{Dub_1(\pi) : \pi \in \mathrm{PAut}(C)\}$ and $\{Dub_2(\pi') : \pi' \in \mathrm{PAut}(D)\}$ acts transitively on the coordinates of $M(C,D)$. Moreover, if C and D are transitive then $M(C,D)$ is transitive, see [23]. We conclude that $\mathrm{Aut}(M(C,D))$ acts transitively on the codewords of $M(C,D)$ and its coordinates, i.e. $M(C,D)$ is neighbor transitive code. □

We say that a code is *non-Mollard* if it is not isomorphic to a Mollard code with arbitrary ϕ. In Section 4 we obtain an infinite series of neighbor transitive extended perfect non-Mollard codes.

3. The automorphism groups of a class of Steiner quadruple systems

The following lemma reveals the discrepancy in the "linearity" of the quadruples from $Q_0(a,b)$ and $Q_1(a,b)$ and the nonlinearity of that of $Q_\tau(a,b)$.

Lemma 1. *Let τ be a permutation on the vectors of F^r that fixes $\mathbf{0}$ and SQS_τ be non-affine. Then*

1. For any $a,b \in F^r$, $a \neq b$ the symmetric difference of any pair of distinct quadruples from $Q_0(a,b)$ $(Q_1(a,b))$ is in SQS_τ.

2. For any $a,b \in F^r$ there are distinct quadruples in $Q_\tau(a,b)$ whose symmetric difference is not in SQS_τ.

Proof. 1. Consider two arbitrary quadruples from $Q_0(a,b)$. We have three different cases.

Case A. Let $(\{a,b,c,d\},\emptyset)$ and $(\{a,b,e,f\},\emptyset)$ be distinct quadruples of Q_0. Then their symmetric difference is obviously in Q_0, because these are the supports of the codewords of weight four of the extended Hamming code $\mathcal{H}$ of length 2^r.

Case B. Let $(\{a,b\},\{c,d\})$ and $(\{a,b\},\{e,f\})$ be distinct quadruples from $Q_0(a,b)$, where $\tau(a+b) = c+d = e+f$. Then their symmetric difference $(\emptyset,\{c,d,e,f\})$ is in Q_1, because c+d+e+f=$\mathbf{0}$.

Case C. Let $(\{a,b,c,d\},\emptyset)$ and $(\{a,b\},\{e,f\})$ be from $Q_0(a,b)$, where $a+b = c+d$ and $\tau(a+b) = e+f$. Then their symmetric difference $(\{c,d\},\{e,f\})$ is in Q_τ, because $\tau(c+d) = \tau(a+b) = e+f$.

Similar considerations hold for any pair of quadruples of $Q_1(a,b)$.

2. Consider any two distinct quadruples from $Q_\tau(a,b)$:

$$(\{a,c\},\{b,d\}),(\{a,e\},\{b,f\}). \tag{3}$$

By the definition of $Q_\tau(a,b)$ we have:

$$\tau(a+c) = b+d,\ \tau(a+e) = b+f. \tag{4}$$

The symmetric difference of the quadruples from (3) is $(\{c,e\},\{d,f\})$. It belongs to Q_τ if and only if $\tau(c+e) = d+f$, which taking into account (4) holds if and only if $\tau(c+e) = \tau(a+c)+\tau(a+e)$. It is easy to see that the latter equality holds for any distinct c and e different from a if and only if $\tau(c+e) = \tau(c)+\tau(e)$. We conclude that the symmetric difference of any pair of distinct quadruples from $Q_\tau(a,b)$ is in SQS_τ if and only if τ is a linear mapping, i.e. $\tau = \sigma_M$ for some $M \in \mathrm{GL}(r,2)$, so SQS_τ is affine by Proposition 3. □

Proposition 5. *Let τ be a permutation on the vectors of F^r, $\tau(\mathbf{0}) = \mathbf{0}$. Then for any $a,b \in F^r$ we have $(\sigma_a|\sigma_b) \in \mathrm{Aut}(SQS_\tau)$. In particular, $\mathrm{Aut}(SQS_\tau)$ either acts transitively on the points of SQS_τ or has two orbits of points that are $(\{a : a \in F^r\},\emptyset)$ and $(\emptyset,\{a : a \in F^r\})$.*

Proof. Obviously $(\sigma_a|\sigma_b)$ fixes the quadruples from Q_0 and Q_1. Let $(\{u,v\},\{g,f\})$ be a quadruple of Q_τ, so $\tau(u+v) = g+f$. From the latter equality, we have that

$$(\sigma_a|\sigma_b)(\{u,v\},\{g,f\}) = (\{u+a,v+a\},\{g+b,f+b\})$$

is in Q_τ. □

We denote by ξ the permutation that swaps the points (coordinate positions) $(\{a\},\emptyset)$ and $(\emptyset,\{a\})$ for any $a \in F^r$.

Remark 1. Let A be a matrix from $GL(r,2)$ and let τ be a permutation of the vectors of F^r. In below we use $A\tau$ and τA to denote the permutations of the vectors of F^r that are compositions of the linear mapping A and τ, i.e $\sigma_A\tau$ and $\tau\sigma_A$ respectively.

Theorem 1. *Let τ and τ' be permutations on the vectors of F^r that fix $\mathbf{0}$. Two SQS_τ and $SQS_{\tau'}$ of order 2^{r+1} satisfy $SQS_\tau \sim_\pi SQS_{\tau'}$ if and only if one of the following conditions holds:*

1) both SQS_τ and $SQS_{\tau'}$ are affine;

2) the permutation π is equal to $(\sigma_{a,A}|\sigma_{b,B})$, where (a,A), $(b,B) \in \mathrm{GA}(r,2)$ and $\tau' = B\tau A^{-1}$;

3) the permutation π is equal to $(\sigma_{a,A}|\sigma_{b,B})\xi$, where (a,A), $(b,B) \in \mathrm{GA}(r,2)$ and $\tau' = B\tau^{-1}A^{-1}$.

Proof. Sufficiency. Case 1. It is well known that if both SQS_τ and $SQS_{\tau'}$ are affine, then they are isomorphic.

We can factor out the permutations $(\sigma_a|\sigma_b)$ as they are common automorphisms for SQS_τ and $SQS_{\tau'}$ by Proposition 5. Throughout cases 2 and 3 below we consider an arbitrary quadruple $(\{e,f\},\{c,d\})$ from Q_τ where $e,f \in F^r$ are distinct and fulfill

$$\tau(e+f) = c+d. \tag{5}$$

Case 2. We show that

$$(\sigma_A|\sigma_B)(SQS_\tau) = SQS_{B\tau A^{-1}}, \tag{6}$$

for any $A,B \in \mathrm{GL}(r,2)$.

Obviously, $(\sigma_A|\sigma_B)$ fixes Q_0 and Q_1. We have

$$(\sigma_A|\sigma_B)(\{e,f\},\{c,d\}) = (\{Ae,Af\},\{Bc,Bd\}).$$

From (5) this vector is in $Q_{B\tau A^{-1}}$ because $B\tau A^{-1}(Ae+Af) = B\tau(e+f) = Bc+Bd$, so (6) holds.

Case 3. We are to show that

$$(\sigma_A|\sigma_B)\xi(SQS_\tau) = SQS_{B\tau^{-1}A^{-1}}, \tag{7}$$

for any $A,B \in \mathrm{GL}(r,2)$.

We note that $\xi(SQS_\tau) = SQS_{\tau^{-1}}$. Indeed, it is obvious that $\xi(Q_0) = Q_1$. Let

$$(\{e,f\},\{c,d\})$$

be from Q_τ. Then $\xi(\{e,f\},\{c,d\}) = (\{c,d\},\{e,f\})$ is in $SQS_{\tau^{-1}}$ because $\tau^{-1}(c+d)$ is $e+f$ by (5).

From $\xi(SQS_\tau) = SQS_{\tau^{-1}}$ and (6) we have that

$$(\sigma_A|\sigma_B)\xi(SQS_\tau) = (\sigma_A|\sigma_B)(SQS_{\tau^{-1}}) = SQS_{B\tau^{-1}A^{-1}},$$

i.e. (7) holds.

Necessity. It is enough to consider non-affine SQS_τ and $SQS_{\tau'}$, $SQS_\tau \sim_\pi SQS_{\tau'}$. By Lemma 1 for any $a,b \in F^r$ the subsets $Q_0(a,b)$ and $Q_1(a,b)$ of $SQS_{\tau'}$ could not be $\pi(Q_\tau(a,b))$. In other words, $\pi(\{a : a \in F^r\},\emptyset)$ is either $(\{a : a \in F^r\},\emptyset)$ or $(\emptyset,\{a : a \in F^r\})$, so $\pi(Q_0 \cup Q_1) = Q_0 \cup Q_1$. It is easy to see that $\pi(Q_0 \cup Q_1) = Q_0 \cup Q_1$ if and only if π is $(\sigma_{a,A}|\sigma_{b,B})\xi^t$, where $(a,A),(b,B) \in \mathrm{GA}(r,2)$, $t \in \{0,1\}$.

□

Corollary 1. *Let τ be the permutation on the vectors of F^r that fixes $\mathbf{0}$. The Steiner quadruple system SQS_τ is point transitive if and only if $\tau^{-1} \in \mathrm{GL}(r,2)\tau\mathrm{GL}(r,2)$.*

Proof. By Proposition 5 for any permutation τ the points of $(\{a : a \in F^r\},\emptyset)$ and $(\emptyset,\{a : a \in F^r\})$ are in one orbit of $\mathrm{Aut}(SQS_\tau)$. So, SQS_τ is point transitive if and only if there is $\pi \in \mathrm{Aut}(SQS_\tau)$, such that $\pi(\emptyset,\{a\}) = \pi(\{b\},\emptyset)$ for some $a,b \in F^r$. We have the following description for all such π and τ from Theorem 1:

$$\{(\sigma_A|\sigma_B)\xi : A,B \in GL(r,2)\} \text{ and } \tau^{-1} \in \mathrm{GL}(r,2)\tau\mathrm{GL}(r,2).$$

□

Theorem 2. *Let τ and τ' be permutations on the vectors of F^r that fix $\mathbf{0}$. For a permutation π we have $SQS_\tau \sim_\pi SQS_{\tau'}$ if and only if $S_\tau \sim_\pi S_{\tau'}$.*

Proof. The sufficiency is clear, we show the necessity. Each code S_τ could be represented as follows:

$$S_\tau = \{x + y : supp(x) \in SQS_\tau, y \in \mathcal{H} \times \mathcal{H}\}.$$

From the proof of Theorem 1 we see that the permutation π such that $SQS_\tau \sim_\pi SQS_{\tau'}$ preserves $Q_0 \cup Q_1$. We conclude that π also preserves $\mathcal{H} \times \mathcal{H}$, which is spanned by the characteristic vectors of the quadruples from $Q_0 \cup Q_1$. Therefore we have $S_\tau \sim_\pi S_{\tau'}$. □

Corollary 2. *The groups* $\mathrm{PAut}(S_\tau)$ *and* $\mathrm{Aut}(SQS_\tau)$ *are isomorphic.*

The necessity of the following statement is by Proposition 2 and the sufficiency is by Theorem 2.

Corollary 3. *Let τ and τ' be permutations on the vectors of F^r that fix $\mathbf{0}$. Let S_τ and $S_{\tau'}$ be transitive codes of length 2^{r+1}. Then $S_\tau \sim_{(x,\pi)} S_{\tau'}$ for a vector x and a permutation π if and only if $SQS_\tau \sim_{\pi'} SQS_{\tau'}$ for some permutation π'.*

4. An infinite series of coordinate transitive and neighbor transitive extended perfect codes

We recall some concepts from [17]. A subgroup G of the general affine group $\mathrm{GA}(r, 2)$ is called *regular* if it is regular with respect to the action (2) on the vectors of F^r. By the definition for any regular subgroup G of the group $\mathrm{GA}(r, 2)$ and any $a \in F^r$ there is a unique affine transformation that maps $\mathbf{0}$ to a, which we denote by g_a. Obviously, g_a is (a, M) for some matrix M in $\mathrm{GL}(r, 2)$. Let T be an automorphism of a regular subgroup G of the group $\mathrm{GA}(r, 2)$. By τ we denote the permutation on the vectors of F^r *induced* by the action of the automorphism T, i.e.

$$T(g_a) = g_{\tau(a)}.$$

Obviously we always have $\tau(\mathbf{0}) = \mathbf{0}$. The following class of propelinear codes was obtained in [17].

Theorem 3. [17] *Let G be a regular subgroup of $\mathrm{GA}(r, 2)$ and τ be the permutation induced by an automorphism of G. The following hold:*

1. The code S_τ is a propelinear extended perfect binary code of length 2^{r+1}.

2. Let τ' be the permutation induced by an automorphism of $\mathrm{GA}(r', 2)$. Then $(\tau|\tau')$ is the permutation induced by an automorphism of $\mathrm{GA}(r + r', 2)$, in particular $S_{\tau|\tau'}$ is a propelinear extended perfect binary code of length $2^{r+r'+1}$.

3. If S_τ has the kernel of dimension $2^{r+1} - 2r - 2$, then S_τ is not a Mollard code. If additionally τ' is a permutation of the vectors of $F^{r'}$, $\tau'(\mathbf{0}) = \mathbf{0}$ and $S_{\tau'}$ has the kernel of dimension $2^{r'+1} - 2r' - 2$ then $S_{\tau|\tau'}$ is a non-Mollard code with the kernel of dimension $2^{r'+r+1} - 2(r' + r) - 2$.

4. Propelinear non-Mollard codes S_τ of length 2^{r+1} with the kernel of dimension $2^{r+1} - 2r - 2$ exist for any $r, r \geq 3$.

We first consider neighbor transitive extended perfect codes of small length. Then we iteratively construct coordinate transitive (neighbor transitive) extended perfect codes of any admissible length not equal to 64.

Theorem 4. *For any permutation τ on the vectors of F^3, $\tau(\mathbf{0}) = \mathbf{0}$, the extended perfect code S_τ of length 16 is neighbor transitive. There are exactly four isomorphism classes for these codes and they are characterized by their ranks that take values 11, 12, 13, 14. The code of rank 14 has dimension of kernel 8.*

Proof. We now show the following natural description of the double cosets of $\mathrm{GL}(r,2)$ in terms of intersections of Hamming codes.

Lemma 2. *Let τ and τ' be permutations on the vectors of F^r that fix $\mathbf{0}$. We have $\tau' \in \mathrm{GL}(r,2)\tau\mathrm{GL}(r,2)$ if and only if $\tau(\mathcal{H}) \cap \mathcal{H} \sim_A \tau'(\mathcal{H}) \cap \mathcal{H}$ for some $A \in \mathrm{GL}(r,2)$.*

Proof. Let τ' be $A^{-1}\tau B$, A and B be in $\mathrm{GL}(r,2)$. We have $A(\mathcal{H}) = B(\mathcal{H}) = \mathcal{H}$ and the following:

$$\tau'(\mathcal{H}) \cap \mathcal{H} = A^{-1}\tau B(\mathcal{H}) = A^{-1}\tau(\mathcal{H}) \cap \mathcal{H} \sim_A \tau(\mathcal{H}) \cap \mathcal{H}.$$

$\square$

For the extended Hamming code $\mathcal{H}$ of length 8 and arbitrary permutation τ on the vectors of F^3 there are exactly four possible values for the dimension of $\tau(\mathcal{H})\cap\mathcal{H}$: 1, 2, 3, 4. Moreover, it is easy to see that for any fixed dimension $k \in \{1,2,3,4\}$ there is τ such that the code $\tau(\mathcal{H}) \cap \mathcal{H}$ has dimension k and is unique up to a permutation of $\mathrm{GL}(3,2)$.

In view of Lemma 2 we see that there are exactly four double cosets by $\mathrm{GL}(3,2)$ in the group of all permutations of F^3 that fix $\mathbf{0}$. By Theorems 1 and 2 we conclude that there are not more than 4 isomorphism classes for the codes. From [17], see e.g. Table 1, there are exactly 4 different values $\{11,12,13,14\}$ for the ranks for the propelinear codes S_τ of length 16 where τ runs through the permutations induced by the automorphisms of the regular subgroups of $\mathrm{GA}(3,2)$. Therefore we have exactly 4 isomorphism classes and each code is propelinear.

Obviously for any permutation τ on the vectors of F^3, $\tau(\mathbf{0}) = \mathbf{0}$ we have that $\tau^{-1}(\mathcal{H})\cap\mathcal{H}$ has the same dimension as $\tau(\mathcal{H}) \cap \mathcal{H}$. Taking into account what was declared at the beginning of the proof, there is $A \in \mathrm{GL}(3,2)$ such that $\tau^{-1}(\mathcal{H}) \cap \mathcal{H} \sim_A \tau(\mathcal{H}) \cap \mathcal{H}$. Then using Lemma 2 we see that τ^{-1} is in $\mathrm{GL}(3,2)\tau\mathrm{GL}(3,2)$. By Corollaries 1 and 2 we conclude that the code S_τ is coordinate transitive for any τ. Since S_τ is transitive, it is neighbor transitive. The code of rank 14 has the dimension of the kernel 8 (see [17]) and therefore is a non-Mollard code by Theorem 3. $\square$

Theorem 5. *There are exactly 64 isomorphism classes of propelinear extended perfect codes S_τ of length 32 with the dimension of kernel 22, where τ is a permutation induced by an automorphism of a regular subgroup of $GA(4,2)$. All these codes are neighbor transitive non-Mollard.*

Proof. Let τ run through the permutations induced by the automorphisms of the regular subgroups of $\mathrm{GA}(4,2)$ such that the corresponding codes S_τ of length 32 have kernels of dimension 22. These codes are transitive non-Mollard codes by Theorem 3. Their isomorphism problem is equivalent to the isomorphism problem of their SQS's by Corollary 3. This problem for SQS of order 32 with 1240 quadruples could be solved by a computer. By MAGMA we find that there are exactly 64 isomorphism classes of the SQS's of these codes. Moreover, again by a computer we see that for any such code S_τ the permutations τ and τ^{-1} are in the same double coset of $\mathrm{GL}(4,2)$. By Corollary 1 we see that all these codes are neighbor transitive. $\square$

The following could be considered as a direct product construction for permutations providing coordinate transitive and neighbor transitive codes.

Theorem 6. *Let τ and τ' be permutations on the vectors of F^r and $F^{r'}$ that fix all-zero vectors. We have the following:*

1. If SQS_τ and $SQS_{\tau'}$ are point transitive Steiner quadruple systems of orders 2^{r+1} and $2^{r'+1}$ respectively then $SQS_{\tau|\tau'}$ is a point transitive Steiner quadruple system of order $2^{r+r'+1}$.

2. If S_τ and $S_{\tau'}$ are coordinate transitive codes then the code $S_{\tau|\tau'}$ is coordinate transitive.

3. If τ and τ' are induced by automorphisms of regular subgroups of $\mathrm{GA}(r,2)$ *and* $\mathrm{GA}(r',2)$ *respectively and S_τ, $S_{\tau'}$ are coordinate transitive codes then the code $S_{\tau|\tau'}$ is neighbor transitive.*

Proof. 1. By Corollary 1 we have $\tau^{-1} = A\tau B$ and ${\tau'}^{-1} = A'\tau' B'$ for appropriate matrices A, B in $\mathrm{GL}(r,2)$ and A', B' in $\mathrm{GL}(r',2)$. Therefore

$$(\tau|\tau')^{-1} = \begin{pmatrix} A & \mathbf{0}_{r,r'} \\ \mathbf{0}_{r',r} & A' \end{pmatrix} \circ (\tau|\tau') \circ \begin{pmatrix} B & \mathbf{0}_{r,r'} \\ \mathbf{0}_{r',r} & B' \end{pmatrix},$$

here $\mathbf{0}_{r,r'}$ and $\mathbf{0}_{r',r}$ are the all-zero $r\times r'$ and $r'\times r$ matrices respectively and $\circ$ denotes the composition of the permutations of the vectors from $F^{r+r'}$. Hence according to Corollary 1 we see that $\mathrm{SQS}_{\tau|\tau'}$ is point transitive.

2. Follows from Corollary 2 and the first statement of this theorem.

3. From the second statement of the current theorem we see that the code $S_{\tau|\tau'}$ is coordinate transitive. From the second statement of Theorem 3 we see that the code $S_{\tau|\tau'}$ is transitive, so it is neighbor transitive. □

Theorem 7. *For any $r \geq 3$, $r \neq 5$ there exists a neighbor transitive extended perfect code $S_{\tau|\tau'}$ of length 2^{r+1} that is non-Mollard.*

Proof. The proof will be done by induction. For the induction base we use Theorems 4 and 5 with the exception of the codes of length 64. Let τ and τ' be permutations induced by automorphisms of regular subgroups of $\mathrm{GA}(r_1,2)$ and $\mathrm{GA}(r_2,2)$, $r = r_1 + r_2$ such that neighbor transitive codes S_τ and $S_{\tau'}$ are of length 2^{r_1+1} and 2^{r_2+1}, with kernels of dimension $2^{r_1+1} - 2r_1$ and $2^{r_2+1} - 2r_2$ respectively. Applying Theorem 6 we obtain a neighbor transitive extended perfect code $S_{\tau|\tau'}$ of length 2^{r+1} that is non-Mollard by the third statement of Theorem 3. □

Remark 2. Analogously to the approach described in Theorem 7 new class of codes could be separated from Z_4-linear codes via ranks. From Theorem 4 we see that the non-Mollard code has the dimension of the kernel 8 and rank 14, whereas at least one of the codes classified in Theorem 5 has rank 30 (see [17]). By induction as in Theorem 7 we obtain non-Mollard codes with large (prefull or deprefull) ranks, see [17, Corollary 2]. We conclude that the obtained neighbor transitive codes are inequivalent to Z_4-linear codes from [10] and the Mollard codes.

Remark 3. We note that almost all results of this work and [17] hold for the following construction of Hadamard codes.

Let us consider the following representation of a linear $(2^r, r+1, 2^{r-1})$ Hadamard code. We index the positions of F^{2^r} by the binary vectors of length r. Let C_a, $a \in F^r$, be the code of length 2^r with the codewords that have the following supports:

$$\{x \in F^r : < x, a >= 0\},\ \{x \in F^r : < x, a >= 1\},$$

where $< \cdot, \cdot >$ is a scalar product. Obviously the set $\bigcup_{a\in F^r} C_a$ is a Hadamard code of length 2^r.

Let τ be a permutation induced by an automorphism of a regular subgroup of $\mathrm{GA}(r,2)$. Then the following code

$$A_\tau = \bigcup_{a\in F^r} C_a \times C_{\tau(a)}$$

is a propelinear Hadamard code of length 2^{r+1}. Analogously to the proof of Theorem 1 we have that the codes A_τ and $A_{\tau'}$ are isomorphic if and only if τ or τ^{-1} is in $\mathrm{GA}(r,2)\tau'\mathrm{GA}(r,2)$. Thus the isomorphism classes of these Hadamard codes and those of the extended perfect codes are in one-to-one correspondence.

References

[1] J. Borges, I. Yu. Mogilnykh, J. Rifà, F. I. Solov'eva, Structural properties of binary propelinear codes, *Advances in Mathematics of Communication*, **6** (2012), 329–346. Zbl 1260.94089

[2] C. Carlet, P. Charpin and V. A. Zinoviev, Codes, bent functions and permutations suitable for DES-like cryptosystems, *Designs, Codes and Cryptography*, **15** (1998), 125–156. Zbl 0938.94011

[3] P. Charpin, *Handbook of Coding Theory*, Chapter 11, North Holland, 1998. Zbl 0907.94001

[4] E. Grigorescu, T. Kaufman, Explicit low-weight bases for BCH codes, *IEEE Transactions on Information Theory*, **58** (2011), 78–81. Zbl 1365.94624

[5] N. I. Gillespie, C. E. Praeger, New characterisations of the Nordstrom–Robinson codes, *Bulletin of the London Mathematical Society*, **58** (2017), 320–330. Zbl 1421.94094

[6] N. I. Gillespie, C. E. Praeger, Neighbour transitivity on codes in Hamming graphs, *Designs, Codes and Cryptography*, **67** (2013), 385–393. Zbl 1296.94160

[7] N. I. Gillespie, M. Giudici, D. R. Hawtin, C. E. Praeger, Entry-faithful 2-neighbour transitive codes, *Designs, Codes and Cryptography*, **79** (2016), 549–564. Zbl 1338.94112

[8] A. R. Hammons, Jr, P. V. Kumar, A. R. Calderbank, N. J. A. Sloane and P. Solé, The Z4-linearity of Kerdock, Preparata, Goethals, and related codes, *IEEE Transactions on Information Theory*, **40**(2) (1994), 301–319. Zbl 0811.94039

[9] W. Kantor, On the inequivalence of generalized Preparata codes, *IEEE Transactions on Information Theory*, **29**(2) (1983), 345–348. Zbl 0521.94016

[10] D. S. Krotov, Z4-linear Hadamard and extended perfect codes, WCC2001, International Workshop on Coding and Cryptography, *Electronic Notes in Discrete Mathematics*, **6** (2001), 107–112. Zbl 0987.94513

[11] T. Kaufman and S. Litsyn, Almost orthogonal linear codes are locally testable, *FOCS, IEEE Computer Society*, (2005), 317–326. Zbl 1359.68009

[12] D. S. Krotov, On the automorphism groups of the Z2Z4-linear 1-perfect and Preparata-like codes, *Designs, Codes and Cryptography*, **83**(1) (2017), 169–177. Zbl 1379.94063

[13] C. C. Lindner, A. Rosa, Steiner quadruple systems – a survey, *Discrete Mathematics*, **22**(2) (1978), 147–181. Zbl 0398.05015

[14] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland Publishing Company, 1977. Zbl 0369.94008

[15] I. Yu. Mogilnykh, F. I. Solov'eva, Propelinear codes related to some classes of optimal codes, *Problems of Information Transmission*, **53**(3) (2017), 251–259. Zbl 1387.94117

[16] I. Yu. Mogilnykh, F.I . Solov'eva. On explicit minimum weight bases for extended cyclic codes related to Gold functions, *Designs, Codes and Cryptography*, **86**(11) (2018), 2619–2627. Zbl 1397.94120

[17] I. Yu. Mogilnykh, F. I. Solov'eva, A concatenation construction for propelinear perfect codes from regular subgroups of GA(r,2), *Siberian Electronic Mathematical Reports*, **16** (2019), 1689–1702. Zbl 07143076

[18] I. Yu. Mogilnykh, F. I. Solov'eva, On the symmetry group of the Mollard code, *Problems of Information Transmission*, **52** (2016), 265–275. Zbl 1369.94608

[19] M. Mollard, A generalized parity function and its use in the construction of perfect codes, *SIAM J. Alg. Discrete Math.*, **7**(1) (1986), 113–115. Zbl 0585.94015

[20] K. T. Phelps, J. Rifà, On binary 1-perfect additive codes: some structural properties, *IEEE Transactions on Information Theory*, **48** (2002), 2587–2592. Zbl 1062.94048

[21] P. Solé, Completely regular codes and completely transitive codes, *Discrete Mathematics*, **81** (1990), 193–201. Zbl 0696.94021

[22] F. I. Solov'eva, On binary nongroup codes, *Methody Discretnogo Analiza*, **37** (1981), 65–75 (in Russian). Zbl 0524.94014

[23] F. I. Solov'eva, On construction of transitive codes, *Problems of Information Transmission*, **41**(3) (2005), 23–31. Zbl 0524.94014

Ivan Yurevich Mogilnykh
Tomsk State University,
Regional Scientific and Educational Mathematical Center,
36, Lenin ave.,
Tomsk, 634050, Russia,
Novosibirsk State University,
1, Pirogova str.,
Novosibirsk, 630090, Russia
Sobolev Institute of Mathematics,
4, Acad. Koptyuga ave.,
Novosibirsk, 630090, Russia
Email address: ivmog@math.nsc.ru

Faina Ivanovna Solov'eva
Sobolev Institute of Mathematics,
4, Acad. Koptyuga ave.,
Novosibirsk, 630090, Russia
Novosibirsk State University,
1, Pirogova str.,
Novosibirsk, 630090, Russia
Email address: sol@math.nsc.ru