Eighth International Workshop on Optimal Codes and Related Topics
July 10-14, 2017, Sofia, Bulgaria *pp. 73-80*

Further results on binary codes obtained by doubling construction

Alexander A. Davydov[1] adav@iitp.ru
Kharkevich Institute for Information Transmission Problems, Russian Academy of Sciences, Bol'shoi Karetnyi pereulok 19, GSP-4, Moscow, 127994, Russian Federation
Stefano Marcugini[2], Fernanda Pambianco[2]
{stefano.marcugini,fernanda.pambianco}@unipg.it
Dipartimento di Matematica e Informatica, Università degli Studi di Perugia
Via Vanvitelli 1, Perugia, 06123, Italy

Abstract. Binary codes created by doubling construction, including quasi-perfect ones with distance $d = 4$, are investigated. All $[17\cdot 2^{r-6}, 17\cdot 2^{r-6} - r, 4]$ quasi-perfect codes are classified. Weight spectrum of the codes dual to quasi-perfect ones with $d = 4$ is obtained. The automorphism group $\mathrm{Aut}(\mathcal{C})$ of codes obtained by doubling construction is studied. A subgroup of $\mathrm{Aut}(\mathcal{C})$ is described and it is proved that the subgroup coincides with $\mathrm{Aut}(\mathcal{C})$ if the starting matrix of doubling construction has an odd number of columns. (It happens for all quasi-perfect codes with $d = 4$ except for Hamming one.) The properness and t-properness for error detection of codes obtained by doubling construction are considered.

1 Introduction

Let an $[n, n - r, d]$ code be a linear binary code of length n, redundancy r, and minimum distance d. A code with $d = 4$ is *quasi-perfect* if its covering radius is equal to 2. Addition of any column to a parity check matrix of a quasi-perfect code decreases the code distance. A parity check matrix of a quasi-perfect $[n, n - r, 4]$ code can be treated as a complete n-cap in the projective space $\mathrm{PG}(r - 1, 2)$ of dimension $r - 1$. A cap in $\mathrm{PG}(N, 2)$ is a set of points no three of which are collinear. A cap is complete if no point can be added to it.

An arbitrary $[n, n - r, 4]$ *code is either a quasi-perfect code or shortening of some quasi-perfect code with* $d = 4$ *and redundancy* r*.*

So, studying quasi-perfect codes is important. The $[2^{r-1}, 2^{r-1} - r, 4]$ extended Hamming code is deeply investigated. The $[5 \cdot 2^{r-4}, 5 \cdot 2^{r-4} - r, 4]$ Panchenko code [1, 2, 4, 5, 10] draws attention as in it the number of weight

[1]The research of A.A. Davydov was carried out at the IITP RAS at the expense of the Russian Foundation for Sciences (project 14-50-00150).
[2]The research of S. Marcugini and F. Pambianco was supported in part by Ministry for Education, University and Research of Italy (MIUR) (Project "Geometrie di Galois e strutture di incidenza") and by the Italian National Group for Algebraic and Geometric Structures and their Applications (GNSAGA - INDAM).

4 codewords is small and, in a number of cases, the smallest possible among all codes with $d = 4$. This essentially increases the error detection capability of Panchenko code. Nevertheless, Panchenko code is studied insufficiently. The same can be said about other quasi perfect $[n, n-r, 4]$ codes (not about Hamming one).

All quasi-perfect $[n, n-r, 4]$ *codes of length* $n \geq 2^{r-2}+2$ *can be described by doubling construction* (1), see [4].

So, it is appropriate to study quasi-perfect $[n, n-r, 4]$ codes from the point of view of doubling construction, see [1,2,4,5]. In *this work* we continue investigations of codes created by doubling construction, including quasi-perfect ones.

In Section 2, we classified all quasi-perfect $[17, 17-6, 4]$ codes and thereby all quasi-perfect $[n_r, n_r - r, 4]$ codes with $n_r = 17 \cdot 2^{r-6}$, $r \geq 6$. Also, we proved a general theorem on weight spectrum of the code dual to quasi perfect one and obtained all these spectra for $n_r = 2^{r-2} + 2^{r-2-g}$, $g = 2, 3, 4$, $r \geq g+2$. In Section 3, we investigate the automorphism group $\mathrm{Aut}(\mathcal{C})$ of codes obtained by doubling construction. We describe a subgroup G of $\mathrm{Aut}(\mathcal{C})$. We prove that if the starting matrix of doubling construction has an odd number of columns then $G = \mathrm{Aut}(\mathcal{C})$. It happens for all quasi perfect codes with $d = 4$ except for Hamming one. In Section 4, we consider the properness and t-properness for error detection of codes obtained by doubling construction.

2 Doubling construction and classification of binary quasi-perfect codes with distance 4

For a code with redundancy r we introduce the following notations: n_r is length of the code, H_r is its parity check matrix of size $r \times n_r$, and d_r is code distance.

Definition 1. Doubling construction *creates a parity check matrix* H_r *of an* $[n_r, n_r - r, d_r]$ *code from a parity check matrix* H_{r-1} *of an* $[n_{r-1}, n_{r-1} - (r-1), d_{r-1}]$ *code as follows*

$$H_r = \left[\begin{array}{c|c} 0\dots0 & 1\dots1 \\ ---- & --- \\ H_{r-1} & H_{r-1} \end{array}\right]. \tag{1}$$

By (1), $n_r = 2n_{r-1}$. Also, if $d_{r-1} = 3$ then $d_r = 3$; if $d_{r-1} \geq 4$ then $d_r = 4$.

Doubling construction is called also *Plotkin construction*, see [4] and the refences therein.

Let us define matrices M, S, Ω, and $\Phi_1, \dots, \Phi_5$ as

$$M = \begin{bmatrix} 01 \\ 11 \end{bmatrix},\ S = \begin{bmatrix} 10001 \\ 01001 \\ 00101 \\ 00011 \end{bmatrix},\ \Omega = \begin{bmatrix} 00000\ 1111 \\ 10001\ 0000 \\ 01001\ 1001 \\ 00101\ 0101 \\ 00011\ 0011 \end{bmatrix},\ \Phi_1 = \begin{bmatrix} 0000000\ 00000000\ 11 \\ 1111111\ 11111111\ 10 \\ 0000000\ 11111111\ 11 \\ 0001111\ 00001111\ 11 \\ 0110011\ 00110011\ 11 \\ 1010101\ 01010101\ 11 \end{bmatrix},$$

$$\Phi_2 = \begin{bmatrix} 00000\ 00000000\ 1111 \\ 11111\ 11111111\ 1000 \\ 00000\ 11111111\ 1111 \\ 01111\ 00001111\ 1111 \\ 10011\ 00110011\ 1110 \\ 10101\ 01010101\ 1101 \end{bmatrix}, \qquad \Phi_3 = \begin{bmatrix} 0000\ 00000000\ 11111 \\ 1111\ 11111111\ 10000 \\ 0000\ 11111111\ 11111 \\ 0111\ 00001111\ 11110 \\ 1011\ 00110011\ 11101 \\ 1101\ 01010101\ 11011 \end{bmatrix},$$

$$\Phi_4 = \begin{bmatrix} 0000\ 0000000\ 111111 \\ 1111\ 1111111\ 100000 \\ 0000\ 1111111\ 111110 \\ 0111\ 0001111\ 111101 \\ 1011\ 0110011\ 111011 \\ 1101\ 1010101\ 110111 \end{bmatrix}, \qquad \Phi_5 = \begin{bmatrix} 0000\ 000000\ 1111111 \\ 1111\ 111111\ 1000000 \\ 0000\ 111111\ 1111100 \\ 0111\ 000111\ 1111010 \\ 1011\ 011001\ 1110110 \\ 1101\ 101010\ 0010001 \end{bmatrix}.$$

Let $B^{(r)}_{j,g} = [b_j \dots b_j]$ be the $(r-g-2) \times (2^g+1)$ matrix of identical columns b_j, where $r \geq 5$ is code redundancy, b_j is the binary representation of the integer j (with the most significant bit at the top position).

From the results of the paper [4], we have a general description of a parity check matrix for a whole class of quasi-perfect codes with distance 4.

Theorem 1. [4] **(i)** *Let $n_r \geq 2^{r-2}+2$, $r \geq 5$, and let an $[n_r, n_r - r, 4]$ code be quasi-perfect. Then length n_r can take any value from the sequence*

$$n_r = 2^{r-2} + 2^{r-2-g} = (2^g+1)2^{r-2-g} \text{ for } g = 0, 2, 3, 4, 5, \dots, r-3. \tag{2}$$

Moreover, n_r may not take any other value that is not noted in (2)*. Also, for each $g = 0, 2, 3, 4, 5, \dots, r-3$, there exists an $[n_r, n_r - r, 4]$ quasi-perfect code with $n_r = 2^{r-2} + 2^{r-2-g}$.*

(ii) *Let $n_r = 2^{r-2} + 2^{r-2-g} = (2^g+1)2^{r-2-g}$, $g \in \{0, 2, 3, 4, 5, \dots, r-3\}$, $r \geq 5$, and let an $[n_r, n_r - r, 4]$ code be quasi-perfect. Then a parity check matrix H_r of this code can be presented in the form*

$$H_r = \left[\begin{array}{c|c|c|c} B^{(r)}_{0,g} & B^{(r)}_{1,g} & & B^{(r)}_{D,g} \\ --- & --- & \dots & --- \\ H_{g+2} & H_{g+2} & & H_{g+2} \end{array} \right], \tag{3}$$

where $D = 2^{r-g-2} - 1$, $H_2 = M$, $H_4 = S$, $H_5 = \Omega$, H_{g+2} is a parity check matrix of a quasi-perfect $[2^g+1, 2^g+1-(g+2), 4]$ code if $g \geq 4$.

By Theorem 1, all quasi-perfect $[n_r, n_r - r, 4]$ codes with $g = 0, 2, 3$, and, respectively, $n_r = 2^{r-1}$, $n_r = 5 \cdot 2^{r-4}$, and $n_r = 9 \cdot 2^{r-4}$, are classified.

The $[2^{r-1}, 2^{r-1} - r, 4]$ code (with starting matrix M) is the extended Hamming code. The $[5 \cdot 2^{r-4}, 5 \cdot 2^{r-4} - r, 4]$ code (with starting matrix S) is the Panchenko code Π_r proposed in [10], see also [2, 5]. The parity check matrix of Π_r is the matrix H_r of (3) with $g = 2$, $D = 2^{r-4} - 1$, $H_{g+2} = S$. We denote with $\mathcal{W}_r$ the $[9 \cdot 2^{r-5}, 9 \cdot 2^{r-5} - r, 4]$ code (with starting matrix Ω).

Corollary 1. *For $g \geq 4$ and $n_r = 2^{r-2} + 2^{r-2-g}$, in order to classify all quasi-perfect $[n_r, n_r - r, 4]$ codes, it is sufficient to classify all quasi-perfect $[2^g+1, 2^g+1-(g+2), 4]$ codes.*

Using the results of this work and of [4,8], we proved the following theorem.

Theorem 2. *Let Φ_j be a parity check matrix of a* $[17, 11, 4]$ *code. The five codes with the parity check matrices $\Phi_1, \ldots, \Phi_5$ are all distinct, up to equivalence,* $[2^4 + 1, 2^4 + 1 - (4 + 2), 4]$ *quasi-perfect codes.*

For a code C, let A_w (resp. $A_w^\perp$) be the number of codewords of weight w in C (resp. in the dual code $C^\perp$). Usually, the code is clear by context. To emphasize the code we can write $A_w(C)$ or $A_w^\perp(C)$.

Let $\mathcal{V}_{r,j}$ be the $[17 \cdot 2^{r-6}, 17 \cdot 2^{r-6} - r, 4]$ code with the parity check matrix H_r of (3) where $g = 4$, $H_{g+2} = H_6 = \Phi_j$, $D = 2^{r-6} - 1$.

We proved the following theorem and proposition.

Theorem 3. *Let $\{A_w^\perp(\mathcal{T}_{g+2}),\ w = 0, 1, \ldots, 2^g + 1\}$ be the weight spectrum of the code dual to the starting* $[2^g + 1, 2^g + 1 - (g + 2), 4]$ *code $\mathcal{T}_{g+2}$ with the parity check matrix H_{g+2} of the construction* (3). *Then the weight spectrum of the code dual to the resultant* $[(2^g + 1)2^{r-2-g}, (2^g + 1)2^{r-2-g} - r, 4]$ *code $\mathcal{C}_r$ with the parity check matrix H_r of* (3) *is as follows.*

$$A^\perp_{w2^{r-2-g}}(\mathcal{C}_r) = A_w^\perp(\mathcal{T}_{g+2}),\ w = 0, 1, \ldots, 2^g + 1;\ A^\perp_{(2^g+1)2^{r-3-g}}(\mathcal{C}_r) = 2^r - 2^{g+2};$$
$$A_u^\perp(\mathcal{C}_r) = 0, u \notin \{0 \cdot 2^{r-2-g}, 1 \cdot 2^{r-2-g}, \ldots, (2^g + 1)2^{r-2-g}\} \cup \{(2^g + 1)2^{r-3-g}\}.$$

Proposition 1. *For the codes Π_r, $\mathcal{W}_r$, and $\mathcal{V}_{r,1}, \ldots, \mathcal{V}_{r,5}$, weight spectrum of the nonzero weigths of the dual codes is as follows.*

$$\Pi_r : A^\perp_{2\cdot 2^{r-4}} = 10,\ A^\perp_{5\cdot 2^{r-5}} = 2^r - 2^4,\ A^\perp_{4\cdot 2^{r-4}} = 5;$$
$$\mathcal{W}_r : A^\perp_{2\cdot 2^{r-5}} = 1,\ A^\perp_{4\cdot 2^{r-5}} = 21,\ A^\perp_{9\cdot 2^{r-6}} = 2^r - 2^5,\ A^\perp_{6\cdot 2^{r-5}} = 7,\ A^\perp_{8\cdot 2^{r-5}} = 2;$$
$$\mathcal{V}_{r,1} : A^\perp_{2\cdot 2^{r-6}} = 1,\ A^\perp_{8\cdot 2^{r-6}} = 45,\ A^\perp_{17\cdot 2^{r-7}} = 2^r - 2^6,\ A^\perp_{10\cdot 2^{r-6}} = 15,\ A^\perp_{16\cdot 2^{r-6}} = 2;$$
$$\mathcal{V}_{r,2} : A^\perp_{4\cdot 2^{r-6}} = 1,\ A^\perp_{6\cdot 2^{r-6}} = 3,\ A^\perp_{8\cdot 2^{r-6}} = 42,\ A^\perp_{17\cdot 2^{r-7}} = 2^r - 2^6,$$
$$A^\perp_{10\cdot 2^{r-6}} = 12,\ A^\perp_{12\cdot 2^{r-6}} = 3,\ A^\perp_{14\cdot 2^{r-6}} = 1,\ A^\perp_{16\cdot 2^{r-6}} = 1;$$
$$\mathcal{V}_{r,3} : A^\perp_{5\cdot 2^{r-6}} = 2,\ A^\perp_{7\cdot 2^{r-6}} = 8,\ A^\perp_{8\cdot 2^{r-6}} = 30,\ A^\perp_{17\cdot 2^{r-7}} = 2^r - 2^6,$$
$$A^\perp_{9\cdot 2^{r-6}} = 12,\ A^\perp_{11\cdot 2^{r-6}} = 8,\ A^\perp_{13\cdot 2^{r-6}} = 2,\ A^\perp_{16\cdot 2^{r-6}} = 1;$$
$$\mathcal{V}_{r,4} : A^\perp_{6\cdot 2^{r-6}} = 6,\ A^\perp_{8\cdot 2^{r-6}} = 40,\ A^\perp_{17\cdot 2^{r-7}} = 2^r - 2^6,\ A^\perp_{10\cdot 2^{r-6}} = 10,$$
$$A^\perp_{12\cdot 2^{r-6}} = 6,\ A^\perp_{16\cdot 2^{r-6}} = 1;$$
$$\mathcal{V}_{r,5} : A^\perp_{7\cdot 2^{r-6}} = 16, A^\perp_{8\cdot 2^{r-6}} = 30, A^\perp_{17\cdot 2^{r-7}} = 2^r - 2^6, A^\perp_{11\cdot 2^{r-6}} = 16, A^\perp_{16\cdot 2^{r-6}} = 1.$$

3 The automorphism group of codes created by doubling construction

In this section we investigate the properties of the automorphism group of the codes obtained applying doubling construction.

Definition 2. *The permutations of coordinate places which send a code $\mathcal{C}$ into itself form the code automorphism group of $\mathcal{C}$, denoted by* $\mathrm{Aut}(\mathcal{C})$.

A code and its dual have the same automorphism group.

Theorem 4. [9, Chapter 8, Problem 29] $\mathrm{Aut}(\mathcal{C})= \mathrm{Aut}(\mathcal{C}^{\perp})$.

Let $\pi \in \mathrm{Aut}(\mathcal{C})$ and let $g_1, \dots, g_{n-r}$ be the rows of a generator matrix G of $\mathcal{C}$. Then $\pi(g_1), \dots, \pi(g_{n-r})$ is a basis of $\mathcal{C}$ too. Therefore a change of basis matrix belonging to the general linear group $\mathrm{GL}(n-r, 2)$ corresponds to π.

On the other hand we can consider the columns c_j of G as points of the projective space $\mathrm{PG}(n-r-1, 2)$. Let $K \in \mathrm{GL}(n-r, 2) = \mathrm{PGL}(n-r, 2)$ belong to the stabilizer group of the set $\Sigma = \{c_j\}_{j=1,\dots,n}$, i.e. $Kc_j \in \Sigma, \forall j \in \{1, \dots, n\}$. Then K induces a permutation of the coordinate place and therefore preserves the weight of each codeword. Then, by [9, Chapter 8, Problem 33], if no coordinate of $\mathcal{C}$ is always zero, K corresponds to a permutation $\pi \in \mathrm{Aut}(\mathcal{C})$.

From the discussion above and Theorem 4, we can represent $\mathrm{Aut}(\mathcal{C})$ as the stabilizer group of the columns of its parity check matrix H_r treated as points of $\mathrm{PG}(r-1, 2)$. We will denote $\mathrm{Aut}(\mathcal{C})$ also as $\mathrm{Aut}(H_r)$.

We consider the matrices H_r obtained from a starting matrix H_s applying double construction $r-s$ times.

Lemma 1. *The columns of H_r are $[b_i|h_j]^T$, where h_j is any column of H_s and b_i is the binary representation of any integer in the interval* $[0, \dots, 2^{r-s}-1]$.

Proof. By induction on $r-s$. $\square$

Now we describe a *subgroup* of $\mathrm{Aut}(\mathcal{C})$. Let $Z_{\ell,m}$ be the $\ell \times m$ matrix with all entries equal to 0 and let $T_{\ell,m}$ be any binary $\ell \times m$ matrix. We denote by Γ_r the set of matrices $\left\{ \left[\begin{array}{c|c} K_{r-s} & T_{r-s,s} \\ \hline Z_{s,r-s} & A_s \end{array} \right] : K_{r-s} \in \mathrm{GL}(r-s, 2), T_{r-s,s} \text{ is any binary } (r-s) \times s \text{ matrix}, A_s \in \mathrm{Aut}(H_s) \right\}$.

Remark 1. $|\Gamma_r| = (2^{r-s}-1)(2^{r-s}-2)\dots(2^{r-s}-2^{r-s-1})|\mathrm{Aut}(H_s)|2^{(r-s)s}$.

Theorem 5. Γ_r *is a subgroup of* $\mathrm{Aut}(H_r)$.

Proof. Let $[b_{r-s}|h_s]^T \in H_r$ and let $M_r = \left[\begin{array}{c|c} K_{r-s} & T_{r-s,s} \\ \hline Z_{s,r-s} & A_s \end{array} \right] \in \Gamma_r$. Then

$$\left[\begin{array}{c|c} K_{r-s} & T_{r-s,s} \\ \hline Z_{s,r-s} & A_s \end{array} \right] \left[\begin{array}{c} b_{r-s} \\ \hline h_s \end{array} \right] = \left[\begin{array}{c} K_{r-s}b_{r-s} + T_{r-s,s}h_s \\ \hline A_s h_s \end{array} \right] \in H_r.$$

Moreover, $\mathrm{Det}(M_r) = \mathrm{Det}(K_{r-s}) \cdot \mathrm{Det}(A_s) \neq 0$, so $\Gamma_r \subset \mathrm{Aut}(H_r)$. Finally,

$$\left[\begin{array}{c|c} K'_{r-s} & T'_{r-s,s} \\ \hline Z_{s,r-s} & A'_s \end{array} \right] \left[\begin{array}{c|c} K''_{r-s} & T''_{r-s,s} \\ \hline Z_{s,r-s} & A''_s \end{array} \right] =$$

$$\begin{bmatrix} K'_{r-s}K''_{r-s} & K'_{r-s}T''_{r-s,s} + K''_{r-s}T'_{r-s,s} \\ \hline Z_{s,r-s} & A'_sA''_s \end{bmatrix} \in \Gamma_r. \qquad \square$$

In general, $\Gamma_r \neq \mathrm{Aut}(H_r)$. For example, if we apply repeatedly doubling construction starting from matrix M (so, $s = 2$), the columns of H_r form a cap of $\mathrm{PG}(r-1,2)$ that is the complement of a hyperplane; its stabilizer group is $\mathrm{AGL}(r-1,2)$ and $|\mathrm{AGL}(r-1,2)| = (2^r - 2)\dots(2^r - 2^{r-1})$.

On the other hand, there exist codes of redundancy r obtained by doubling construction whose automorphism group is Γ_r.

Theorem 6. *Let $\mathcal{C}_s$ be an $[n, n-s]$ code having a parity check matrix H_s without zero columns and without rows of weight $n/2$. Then for the codes $\mathcal{C}_r$ obtained applying doubling construction r-s times starting from H_s, it holds that* $\mathrm{Aut}(\mathcal{C}_r) = \Gamma_r$.

Proof. By induction on $r-s$. Let $r = s+1$. Let $H_{s+1} = \begin{bmatrix} 0\dots0 & 1\dots1 \\ \hline h_1\dots h_{n_s} & h_1\dots h_{n_s} \end{bmatrix}$ be a parity check matrix of $\mathcal{C}_{s+1}$ and $M_{s+1} = \begin{bmatrix} x_{1,1} & t_1 \\ \hline x_{2,1} & a_1 \\ \vdots & \vdots \\ x_{s+1,1} & a_s \end{bmatrix} \in \mathrm{Aut}(\mathcal{C}_{s+1})$.

Let r_j be the j-th row of $M_{s+1}H_{s+1}$, $j = 2, \dots, s+1$. Then $r_j = [a_{j-1}\cdot h_1^T \dots a_{j-1}\cdot h_{n_s}^T | \, x_{j,1} + a_{j-1}\cdot h_1^T \dots x_{j,1} + a_{j-1}\cdot h_{n_s}^T]$. As $M_{s+1} \in \mathrm{Aut}(\mathcal{C}_{s+1})$, it induces a permutation on the coordinates of the codewords, so $\mathrm{weight}(r_j) = 2\ \mathrm{weight}(p_{j-1})$, where p_j is the j-th row of H_s. On the other hand, consider the elements of r_j of position i and $i + n_s, i = 1, \dots, n_s$; they are $a_{j-1}\cdot h_i^T$ and $x_{j,1} + a_{j-1}\cdot h_i^T$. If $x_{j,1} = 1$, exactly one of these elements is equal to 1, so $\mathrm{weight}(r_j) = n_s$. This is not possible by hypothesis. Moreover $x_{2,1} = \dots = x_{s+1,1} = 0$ implies $x_{1,1} = 1$, otherwise $\mathrm{Det}(M_{s+1}) = 0$. Finally, the sub-matrix $A_s = \begin{bmatrix} a_1 \\ \vdots \\ a_s \end{bmatrix}$ permutes the columns of H_s, so it belongs to $\mathrm{Aut}(\mathcal{C}_s)$. In fact, let $[b|h_i]^T$ be a column of H_{s+1}. Then $M_{s+1}\begin{bmatrix} b \\ - \\ h_j \end{bmatrix} = \begin{bmatrix} y \\ - \\ A_sh_j \end{bmatrix}$ is a column of H_{s+1} if and only if A_sh_j is a column of H_s. Moreover, if $A_sh_i = A_sh_j, i \neq j$, then two of the columns $[0|h_i]^T$, $[0|h_j]^T$, $[1|h_j]^T$ have the same image under M_{s+1}. The proof of the general case, i.e, $r - s > 1$, is similar. $\square$

Corollary 2. *Let $\mathcal{C}_s$ be an $[n, n-s]$ code having a parity check matrix H_s without zero columns. If n is odd then for the codes $\mathcal{C}_r$ obtained applying doubling construction r-s times starting from H_s, it holds that* $\mathrm{Aut}(\mathcal{C}_r) = \Gamma_r$

Remark 2. $|\mathrm{Aut}(S)| = 120$, $|\mathrm{Aut}(\Omega)| = 336$, $|\mathrm{Aut}(\Phi_1)| = 40320$, $|\mathrm{Aut}(\Phi_2)| = 576$, $|\mathrm{Aut}(\Phi_3)| = 384$, $|\mathrm{Aut}(\Phi_4)| = 720$, $|\mathrm{Aut}(\Phi_5)| = 11520$.

Corollary 3. $|\mathrm{Aut}(\Pi_r)| = 120(2^{r-4} - 1)(2^{r-4} - 2)\dots(2^{r-4} - 2^{r-3})2^{4(r-4)}$.
$|\mathrm{Aut}(\mathcal{W}_r)| = 336(2^{r-5} - 1)(2^{r-5} - 2)\dots(2^{r-5} - 2^{r-4})2^{5(r-5)}$.

4 Properness and t-properness for error detection of codes obtained by doubling construction

Problems connected with error detection are considered, e.g., in [3,6,7], see also the references therein. Here we consider the *binary symmetric channel*.

Let p be the error probability by symbol in the channel.

Let $P_{ue}(C, p)$ be the undetected error probability for the code C under condition that the code is used only for error detection;

Let $P_{ue}^{(t)}(C, p)$ be the undetected error probability for the code C under condition that $d \geq 2t + 1$ and the code is used for correction of $\leq t$ errors.

Definition 3. (i) *A binary code C is* proper (*resp.* t-proper) *if $P_{ue}(C, p)$ (resp. $P_{ue}^{(t)}(C, p)$) is an increasing function of p in the interval $[0, \frac{1}{2}]$.*

(ii) *Let $a \geq 0$ and $b \leq \frac{1}{2}$ be real values. A binary code C is* proper (*resp.* t-proper) *in the interval $[a, b]$ if $P_{ue}(C, p)$ (resp. $P_{ue}^{(t)}(C, p)$) is an increasing function of p in $[a, b]$.*

Using the results of this work, in particular Theorem 3 and Proposition 1, and papers [2, 3, 6, 7], we proved a number of results on the properness and t-properness of codes obtained by doubling construction.

Lemma 2. *In doubling construction (1), let the starting $[n_{r-1}, n_{r-1} - (r - 1), d_{r-1}]$ code given by the parity check matrix H_{r-1} have dual distance in the region $\lceil \frac{n_{r-1}}{3} \rceil \leq d_{r-1}^{\perp} \leq \frac{n_{r-1}}{2}$. Then the resultant $[n_r, n_r - r, d_r]$ code given by the parity check matrix H_r has dual distance in the region $\lceil \frac{n_r}{3} \rceil \leq d_r^{\perp} \leq \frac{n_r}{2}$.*

Theorem 7. *The codes Π_r, $\mathcal{V}_{r,4}$, and $\mathcal{V}_{r,5}$, are proper in intervals $[a, \frac{1}{2}]$, where $a = \frac{1}{3} + \frac{1}{3 \cdot 2^{r-4}}$ for Π_r, $a = \frac{5}{11} + \frac{1}{11 \cdot 2^{r-6}}$ for $\mathcal{V}_{r,4}$, $a = \frac{3}{10} + \frac{1}{10 \cdot 2^{r-6}}$ for $\mathcal{V}_{r,5}$.*

Proposition 2. *The codes $\Pi_r^{\perp}$, $\mathcal{W}_r^{\perp}$, $\mathcal{V}_{r,j}^{\perp}$ dual to the codes Π_r, $\mathcal{W}_r$, $\mathcal{V}_{r,j}$, are proper in intervals $[0, b]$, where $b = \frac{2}{5}$ for $\Pi_r^{\perp}$, $b = \frac{2}{9}$ for $\mathcal{W}_r^{\perp}$, $b = \frac{2}{17}$ for $\mathcal{V}_{r,1}^{\perp}$, $b = \frac{4}{17}$ for $\mathcal{V}_{r,2}^{\perp}$, $b = \frac{5}{17}$ for $\mathcal{V}_{r,3}^{\perp}$, $b = \frac{6}{17}$ for $\mathcal{V}_{r,4}^{\perp}$, $b = \frac{7}{17}$ for $\mathcal{V}_{r,5}^{\perp}$.*

Proposition 3. *The codes with the parity check matrices S and Ω are proper and 1-proper. The codes Π_r are proper for $r = 5, 6, 7, 8, 9$ and 1-proper for $r = 5, 6, 7$. The codes $\mathcal{W}_r$ are proper and 1-proper for $r = 6$.*

Open Problem. Assume that in doubling construction (1), the starting code given by the parity check matrix H_{r-1} is proper (resp. 1-proper) for error detection. Is the resulting code with the the parity check matrix H_r proper (resp. 1-proper) too? (For example, see Construction * in [7, Section 2]; see also Proposition 3.)

References

[1] V. B. Afanassiev and A. A. Davydov, Weight Spectrum of Quasi-Perfect Binary Codes with Distance 4, in *Proc. IEEE Int. Symp. Inform. Theory (ISIT), Aachen, Germany, 2017*, to appear.

[2] V. B. Afanassiev, A. A. Davydov, and D. K. Zigangirov, Design and analysis of codes with distance 4 and 6 minimizing the probability of decoder error, *J. Communic. Technology Electronics*, **61**, 1440–1455, 2016.

[3] Ts. Baicheva, S. Dodunekov, and P. Kazakov, On the undetected error probability performance of cyclic redundancy-check codes of 16-bit redundancy, *IEEE Trans. Comm.* 147 (2000) 253–256.

[4] A. A. Davydov and L. M. Tombak, Quasiperfect Linear Binary Codes with Minimal Distance 4 and Complete Caps in Projective Geometry", *Problems of Inform. Transm.*, **25**, 265–275, 1989.

[5] A. A. Davydov and L. M. Tombak, An Alternative to the Hamming code in the Class of SEC-DED Codes in Semiconductor Memory, *IEEE Trans. Inform. Theory*, **IT-37**, 897–902, 1991.

[6] R. Dodunekova, S. M. Dodunekov, and E. Nikolova, A Survey on Proper Codes, *Discrete Appl. Math.*, **156**, 1499–1509, 2008.

[7] R. Dodunekova and E. Nikolova, Sufficient Conditions for Monotonicity of the Undetected Error Probability for Large Channel Error Probabilities, *Probl. Inform. Transm.*, **41**, 187–198, 2005.

[8] M. Khatirinejad and P. Lisonek, Classification and Constructions of Complete Caps in Binary Spaces, *Des. Codes Cryptogr.*, **39**, 17–31, 2006.

[9] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes,* North-Holland, Amsterdam, 1977.

[10] V. I. Panchenko, On optimization of linear code with distance 4, in *Proc. 8th All-Union Conf. on Coding Theory and Communications*, Kuibyshev, 1981, Part 2: Coding Theory (Moscow, 1981), pp. 132–134 [in Russian].