

New Results on Binary Codes Obtained by Doubling Construction

Alexander A. Davydov¹, Stefano Marcugini², Fernanda Pambianco²

¹Kharkevich Institute for Information Transmission Problems, Russian Academy of Sciences, Bol'shoi Karetnyi pereulok 19, Moscow 127051, Russian Federation

²Dipartimento di Matematica e Informatica, Università degli Studi di Perugia, Via Vanvitelli 1, Perugia 06123, Italy

E-mails: adav@iitp.ru stefano.marcugini@unipg.it fernanda.pambianco@unipg.it

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 $\text{Aut}(C)$ of codes obtained by doubling construction is studied. A subgroup of $\text{Aut}(C)$ is described and it is proved that the subgroup coincides with $\text{Aut}(C)$ 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.

Keywords: Linear binary codes, doubling construction, quasi-perfect codes, automorphism group of a code, proper and t -proper codes.

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 $\text{PG}(r - 1, 2)$ of dimension $r - 1$. A cap in $\text{PG}(N, 2)$ is a set of points no three of which are collinear. A cap is complete if no point can be added to it.

Observation 1. An arbitrary $[n, n - r, 4]$ code is either a quasi-perfect code or the 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, 6, 7, 15] draws attention as in it the number of weight 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).

Observation 2 [6]. All quasi-perfect $[n, n - r, 4]$ codes of length $n \geq 2^{r-2} + 2$ can be described by doubling construction (see Equation (1) below).

So, it is appropriate to study quasi-perfect $[n, n - r, 4]$ codes from the point of view of doubling construction. Such researches were done, for instance, in [1, 2, 6, 7]. In **this work** we continue investigations of codes created by doubling construction, including quasi-perfect ones.

In Section 2, we describe doubling construction and, basing on the results of [6], give a general description of a parity check matrix for a whole class of quasi-perfect binary codes with distance 4. Also, we classify all quasi-perfect $[17, 17 - 6, 4]$ codes and thereby all quasi-perfect $[n_r, n_r - r, 4]$ codes with $n_r = 17 \cdot 2^{r-6}$, $r \geq 6$.

In Section 3, we prove a general theorem on weight spectrum of the code dual to quasi-perfect one and obtain all these spectra for quasi-perfect $[n_r, n_r - r, 4]$ codes with $n_r = 2^{r-2} + 2^{r-2-g}$, $g = 2, 3, 4$, $r \geq g + 2$.

In Section 4, the Automorphism group $\text{Aut}(C)$ of codes obtained by doubling construction is investigated. We describe a subgroup G of $\text{Aut}(C)$ and prove that if the starting matrix of doubling construction has an odd number of columns then $G = \text{Aut}(C)$. It happens for all quasi-perfect codes with $d = 4$ except for Hamming one.

In Section 5, the properness and t -properness for error detection of codes, obtained by doubling construction, is considered. We use the results of this work and papers [3, 8–11].

Some results of this work were briefly presented in [5].

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:

$$(1) \quad H_r = \left[\begin{array}{c|c} 0 \dots 0 & 1 \dots 1 \\ \hline - & - \\ H_{r-1} & H_{r-1} \end{array} \right].$$

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 [6] and the references therein.

Let us define matrices M , S , and Ω as

$$(2) \quad M = \begin{bmatrix} 01 \\ 11 \end{bmatrix}, \quad S = \begin{bmatrix} 10001 \\ 01001 \\ 00101 \\ 00011 \end{bmatrix}, \quad \Omega = \begin{bmatrix} 00000 & 1111 \\ 10001 & 0000 \\ 01001 & 1001 \\ 00101 & 0101 \\ 00011 & 0011 \end{bmatrix}.$$

The matrix S (respectively Ω) can be treated as a parity check matrix of the $[2^2+1, 1, 5]$ perfect repetition code (resp. $[2^3+1, 4, 4]$ quasi-perfect code). By [6, Lemma 10], there exists only one (up to equivalence) $[2^3+1, 4, 4]$ quasi-perfect code; moreover, the parity check matrix of this code can be presented in the form Ω .

From the results of the paper [6], we have a general description of a parity check matrix for a whole class of quasi-perfect codes with distance 4.

Theorem 1 [6]. (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

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

Moreover, n_r may not take any other value that is not listed in (3). 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

$$(4) \quad H_r = \begin{bmatrix} B_{r-g-2}^{(0)} & | & B_{r-g-2}^{(1)} & | & & | & B_{r-g-2}^{(D)} \\ \hline \text{---} & | & \text{---} & | & \dots & | & \text{---} \\ \hline H_{g+2}^* & | & H_{g+2}^* & | & & | & H_{g+2}^* \end{bmatrix},$$

where $D = 2^{r-g-2} - 1$, $B_{r-g-2}^{(j)} = [b_{r-g-2}^{(j)} \dots b_{r-g-2}^{(j)}]$ is the $(r-g-2) \times (2^g + 1)$ matrix of identical columns $b_{r-g-2}^{(j)}$ every of which is the $(r-g-2)$ -positional binary representation of the integer j (with the most significant bit at the top position), $H_{0+2}^* = M$, $H_{2+2}^* = S$, $H_{3+2}^* = \Omega$, H_{g+2}^* is a parity check matrix of a quasi-perfect $[2^g + 1, 2^g + 1 - (g+2), 4]$ code if $g \geq 4$.

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 [15], see also [1, 2, 6, 7]. The parity check matrix of Π_r is the matrix H_r of (4) with $g = 2$, $D = 2^{r-4} - 1$, $H_{g+2}^* = S$. We denote by W_r the $[9 \cdot 2^{r-5}, 9 \cdot 2^{r-5} - r, 4]$ code (with starting matrix Ω).

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.

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.

In order to classify $[2^4 + 1, 2^4 + 1 - (4 + 2), 4]$ codes, we (similarly to [6, Equation (18)]) introduce a $(g + 2) \times (2^g + 1)$ matrix

$$(5) \quad H_{g+2}^*(a_1, \dots, a_v; x) = \begin{bmatrix} 0 \dots 0 & | & 1 & | & 1 & | & \dots & | & 1 \\ \hline \text{-----} & | & - & | & - & | & - & | & - \\ H_{g+1}^{\text{Ham}} \setminus \{a_1, \dots, a_v\} & | & x & | & x \oplus a_1 & | & \dots & | & x \oplus a_v \end{bmatrix},$$

where a_i and x are $(g + 1)$ -positional distinct columns; the entry $H_{g+1}^{\text{Ham}} \setminus \{a_1, \dots, a_v\}$ notes the $(g + 1) \times (2^g - v)$ matrix obtained by removing of the columns a_1, \dots, a_v from the parity check matrix of the $[2^g, 2^g - (g + 1), 4]$ extended Hamming code; \oplus means the bit-by-bit sum of binary columns modulo two; v is a parameter.

Conjecture 1 [6, Remark 5].

(i) There exist exactly 5 distinct (up to equivalence) quasi-perfect $[2^4 + 1, 2^4 + 1 - (4 + 2), 4]$ codes.

(ii) Parity check matrices of these codes can be presented in the form

$$H_{4+2}^*(a_1, a_2, \dots, a_v; x) \text{ with } v = 1, 3, 4, 5, 6,$$

where 5-positional columns a_1, a_2, \dots, a_v are linearly independent for $v \leq 5$, columns a_1, a_2, a_3, a_4, a_5 are linear independent for $v = 6$.

Note that the order of columns a_1, a_2, \dots, a_v does not influence the properties of the matrix $H_{4+2}^*(a_1, a_2, \dots, a_v; x)$. Therefore, for $v = 6$ any quintuplet of columns from the set $\{a_1, a_2, a_3, a_4, a_5, a_6\}$ must be linearly independent. It is possible, for instance, if the columns a_1, a_2, a_3, a_4, a_5 are linearly independent and also $a_6 = a_1 \oplus a_2 \oplus a_3 \oplus a_4 \oplus a_5$.

Conjecture 1(i) is proved in [4, 12] by exhaustive computer search.

Proposition 1 [4, 12]. There exist exactly 5 distinct (up to equivalence) quasi-perfect $[17, 11, 4]$ codes.

In this work, we prove Conjecture 1(ii) for specified columns a_i and x . We put

$$(6) \quad \begin{aligned} a_1 &= (10000)^T, a_2 = (10001)^T, a_3 = (10010)^T, a_4 = (10100)^T, \\ a_5 &= (11000)^T, x = (11111)^T, a_6 = a_1 \oplus a_2 \oplus a_3 \oplus a_4 \oplus a_5 = (11111)^T, x' = (11110)^T. \end{aligned}$$

Note that, in (6), the columns a_1, a_2, a_3, a_4, a_5 are linearly independent.

Let us define the matrices Φ_1, \dots, Φ_5 as follows:

$$(7) \quad \begin{aligned} \Phi_1 &= H_{4+2}^*(a_1; x), \Phi_2 = H_{4+2}^*(a_1, a_2, a_3; x), \Phi_3 = H_{4+2}^*(a_1, a_2, a_3, a_4; x), \\ \Phi_4 &= H_{4+2}^*(a_1, a_2, a_3, a_4, a_5; x), \Phi_5 = H_{4+2}^*(a_1, a_2, a_3, a_4, a_5, a_6; x'), \end{aligned}$$

where a_i, x , and x' are taken from (6).

By (5)-(7), we have

$$(8) \quad \Phi_1 = \begin{bmatrix} 0000000 & 00000000 & 11 \\ 1111111 & 11111111 & 10 \\ 0000000 & 11111111 & 11 \\ 0001111 & 00001111 & 11 \\ 0110011 & 00110011 & 11 \\ 1010101 & 01010101 & 11 \end{bmatrix}, \quad \Phi_2 = \begin{bmatrix} 00000 & 00000000 & 1111 \\ 11111 & 11111111 & 1000 \\ 00000 & 11111111 & 1111 \\ 01111 & 00001111 & 1111 \\ 10011 & 00110011 & 1110 \\ 10101 & 01010101 & 1101 \end{bmatrix},$$

$$(9) \quad \Phi_3 = \begin{bmatrix} 0000 & 00000000 & 11111 \\ 1111 & 11111111 & 10000 \\ 0000 & 11111111 & 11111 \\ 0111 & 00001111 & 11110 \\ 1011 & 00110011 & 11101 \\ 1101 & 01010101 & 11011 \end{bmatrix}, \quad \Phi_4 = \begin{bmatrix} 0000 & 00000000 & 1111111 \\ 1111 & 11111111 & 1000000 \\ 0000 & 11111111 & 1111110 \\ 0111 & 00011111 & 1111101 \\ 1011 & 01100111 & 1110111 \\ 1101 & 10101011 & 1101111 \end{bmatrix},$$

$$(10) \quad \Phi_5 = \begin{bmatrix} 0000 & 000000 & 1111111 \\ 1111 & 111111 & 1000000 \\ 0000 & 111111 & 1111100 \\ 0111 & 000111 & 1111010 \\ 1011 & 011001 & 1110110 \\ 1101 & 101010 & 0010001 \end{bmatrix}.$$

Proposition 2. All matrices Φ_1, \dots, Φ_5 are non equivalent to each other and every matrix is a parity check matrix of a $[17, 11, 4]$ quasi-perfect code.

Proof: We checked the assertion by computer.

By Propositions 1 and 2, the following theorem is proved. \square

Theorem 2. The five codes with the parity check matrices Φ_1, \dots, Φ_5 give the whole list of all distinct, up to equivalence, $[2^4 + 1, 2^4 + 1 - (4 + 2), 4]$ quasi-perfect codes.

Now, by Corollary 1, we can say that all quasi-perfect $[n_r, n_r - r, 4]$ codes with $n_r = 17 \cdot 2^{r-6}$, $r \geq 6$, are classified.

3. Dual weight spectrum of codes obtained by doubling construction

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

Theorem 3. Let $g \geq 2$ and let $\{A_w^\perp(T_{g+2}), w = 0, 1, \dots, 2^g + 1\}$ be the weight spectrum of the code dual to the starting $[2^g + 1, 2^g + 1 - (g + 2), d]$ code T_{g+2} with the parity check matrix H_{g+2}^* of the construction (4). 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 C_r with the parity check matrix H_r of (4) is as follows:

$$(11) \quad A_{w2^{r-2-g}}^\perp(C_r) = A_w^\perp(T_{g+2}), w = 0, 1, \dots, 2^g + 1,$$

$$A_{(2^g+1)2^{r-3-g}}^\perp(C_r) = 2^r - 2^{g+2},$$

$$A_u^\perp(C_r) = 0, u \notin \{0 \cdot 2^{r-2-g}, 1 \cdot 2^{r-2-g}, \dots, (2^g + 1)2^{r-2-g}\} \cup \{(2^g + 1)2^{r-3-g}\}.$$

Proof. We consider the matrix H_r of (4) as a generator matrix of the dual code. If a codeword of the dual code is created without the inclusion of the top $r-g-2$ rows

(i.e., without matrices $B_r^{(j)}$), then its weight is equal to the weight of the corresponding word formed from rows of matrix H_{g+2}^* multiplied by $D + 1 = 2^{r-g-2}$. This explains the term $A_{w2^{r-2-g}}^\perp(C_r) = A_w^\perp(T_{g+2})$. If at least one of the top $r - g - 2$ rows of H_r in (4) is used for creating a word of the dual code, then the weight of this word is equal to $(2^g + 1)2^{r-3-g}$. The number of such words is $2^r - 2^{g+2}$. \square

Let $V_{r,j}$ be the $[17 \cdot 2^{r-6}, 17 \cdot 2^{r-6} - r, 4]$ code with the parity check matrix H_r of (4)

where $g = 4$, $H_{g+2}^* = H_{4+2}^* = \Phi_j$, $D = 2^{r-6} - 1$, $j = 1, \dots, 5$.

Proposition 3. For the $[n_r, n_r - r, 4]$ quasi-perfect codes Π_r , W_r , and $V_{r,1}, \dots, V_{r,5}$, the weight spectrum of the nonzero weights of the dual codes is as follows:

$$\Pi_r, n_r = 5 \cdot 2^{r-4}: A_{2 \cdot 2^{r-4}}^\perp = 10, A_{5 \cdot 2^{r-5}}^\perp = 2^r - 2^4, A_{4 \cdot 2^{r-4}}^\perp = 5,$$

$$W_r, n_r = 9 \cdot 2^{r-5}: A_{2 \cdot 2^{r-5}}^\perp = 1, A_{4 \cdot 2^{r-5}}^\perp = 21, A_{9 \cdot 2^{r-6}}^\perp = 2^r - 2^5,$$

$$A_{6 \cdot 2^{r-5}}^\perp = 7, A_{8 \cdot 2^{r-5}}^\perp = 2,$$

$$V_{r,1}, n_r = 17 \cdot 2^{r-6}: A_{2 \cdot 2^{r-6}}^\perp = 1, A_{8 \cdot 2^{r-6}}^\perp = 45, A_{17 \cdot 2^{r-7}}^\perp = 2^r - 2^6,$$

$$A_{10 \cdot 2^{r-6}}^\perp = 15, A_{16 \cdot 2^{r-6}}^\perp = 2,$$

$$V_{r,2}, n_r = 17 \cdot 2^{r-6}: A_{4 \cdot 2^{r-6}}^\perp = 1, A_{6 \cdot 2^{r-6}}^\perp = 3, A_{8 \cdot 2^{r-6}}^\perp = 42, A_{17 \cdot 2^{r-7}}^\perp = 2^r - 2^6,$$

$$A_{10 \cdot 2^{r-6}}^\perp = 12, A_{12 \cdot 2^{r-6}}^\perp = 3, A_{14 \cdot 2^{r-6}}^\perp = 1, A_{16 \cdot 2^{r-6}}^\perp = 1,$$

$$V_{r,3}, n_r = 17 \cdot 2^{r-6}: A_{5 \cdot 2^{r-6}}^\perp = 2, A_{7 \cdot 2^{r-6}}^\perp = 8, A_{8 \cdot 2^{r-6}}^\perp = 30, A_{17 \cdot 2^{r-7}}^\perp = 2^r - 2^6,$$

$$A_{9 \cdot 2^{r-6}}^\perp = 12, A_{11 \cdot 2^{r-6}}^\perp = 8, A_{13 \cdot 2^{r-6}}^\perp = 2, A_{16 \cdot 2^{r-6}}^\perp = 1;$$

$$V_{r,4}, n_r = 17 \cdot 2^{r-6}: A_{6 \cdot 2^{r-6}}^\perp = 6, A_{8 \cdot 2^{r-6}}^\perp = 40, A_{17 \cdot 2^{r-7}}^\perp = 2^r - 2^6,$$

$$A_{10 \cdot 2^{r-6}}^\perp = 10, A_{12 \cdot 2^{r-6}}^\perp = 6, A_{16 \cdot 2^{r-6}}^\perp = 1;$$

$$V_{r,5}, n_r = 17 \cdot 2^{r-6}: A_{7 \cdot 2^{r-6}}^\perp = 16, A_{8 \cdot 2^{r-6}}^\perp = 30, A_{17 \cdot 2^{r-7}}^\perp = 2^r - 2^6,$$

$$A_{11 \cdot 2^{r-6}}^\perp = 16, A_{16 \cdot 2^{r-6}}^\perp = 1.$$

Proof: By computer search, we obtained the following dual weight spectra of the nonzero weights of the starting $[n_{g+2}, n_{g+2} - (g + 2), 4]$ quasi-perfect codes with the parity check matrices $S, \Omega, \Phi_1, \dots, \Phi_5$:

$$S, n_{g+2} = 5: A_2^\perp = 10, A_4^\perp = 5;$$

$$\Omega, n_{g+2} = 9: A_2^\perp = 1, A_4^\perp = 21, A_6^\perp = 7, A_8^\perp = 2,$$

$$\Phi_1, n_{g+2} = 17: A_2^\perp = 1, A_8^\perp = 45, A_{10}^\perp = 15, A_{16}^\perp = 2,$$

$$\Phi_2, n_{g+2} = 17: A_4^\perp = 1, A_6^\perp = 3, A_8^\perp = 42, A_{10}^\perp = 12, A_{12}^\perp = 3, A_{14}^\perp = 1, A_{16}^\perp = 1,$$

$$\Phi_3, n_{g+2} = 17: A_5^\perp = 2, A_7^\perp = 8, A_8^\perp = 30, A_9^\perp = 12, A_{11}^\perp = 8, A_{13}^\perp = 2, A_{16}^\perp = 1,$$

$$\Phi_4, n_{g+2} = 17: A_6^\perp = 6, A_8^\perp = 40, A_{10}^\perp = 10, A_{12}^\perp = 6, A_{16}^\perp = 1,$$

$$\Phi_5, n_{g+2} = 17: A_7^\perp = 16, A_8^\perp = 30, A_{11}^\perp = 16, A_{16}^\perp = 1.$$

Now we use Theorem 3. \square

4. 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 C into itself form the code automorphism group of C , denoted by $\text{Aut}(C)$.

A code and its dual have the same automorphism group.

Theorem 4 [14, Chapter 8, Problem 29]. $\text{Aut}(C) = \text{Aut}(C^\perp)$.

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

On the other hand, we can consider the columns c_j of G as points of the projective space $\text{PG}(n-r-1, 2)$. Let $K \in \text{GL}(n-r, 2) = \text{PGL}(n-r, 2)$ 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 places and therefore preserves the weight of each codeword. Then, by [14, Chapter 8, Problem 33], if no coordinate of C is always zero, K corresponds to a permutation $\pi \in \text{Aut}(C)$.

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

Lemma 1. The $r \times 2^{r-s}n_s$ matrix H_r , obtained from a starting $s \times n_s$ matrix H_s applying doubling construction $r-s$ times, has the form

$$(12) \quad H_r = \begin{bmatrix} b_{r-s}^{(0)} \dots b_{r-s}^{(0)} & | & b_{r-s}^{(1)} \dots b_{r-s}^{(1)} & | & b_{r-s}^{(2^\ell-1)} \dots b_{r-s}^{(2^\ell-1)} \\ \text{-----} & | & \text{-----} & | & \text{-----} \\ h_1 \dots h_{n_s} & | & h_1 \dots h_{n_s} & | & h_1 \dots h_{n_s} \end{bmatrix},$$

where $\ell = r-s$, h_j is the j -th s -positional column of H_s , and $b_{r-s}^{(i)}$ is the $(r-s)$ -positional binary representation of the integer i .

Proof: By induction on $r-s$. □

Now we describe a *subgroup* of $\text{Aut}(C)$. Let $Z_{\ell, m}$ be the $\ell \times m$ matrix with all entries equal to 0 and let $T_{\ell, m}$ be any $\ell \times m$ binary matrix. We denote by Γ_r the following set of matrices:

$$(13) \quad \Gamma_r = \left\{ \begin{bmatrix} K_{r-s} & | & T_{r-s, s} \\ \text{---} & | & \text{---} \\ Z_{s, r-s} & | & A_s \end{bmatrix} : K_{r-s} \in \text{GL}(r-s, 2), A_s \in \text{Aut}(H_s) \right\}.$$

Proposition 4. It holds that

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

Proof: Note that $|\text{GL}(n, 2)| = (2^n - 1)(2^n - 2) \dots (2^n - 2^{n-1})$. Also, there are $2^{\ell m}$ distinct matrices $T_{\ell, m}$. □

Theorem 5. The matrix set Γ_r is a subgroup of $\text{Aut}(H_r)$.

Proof: Let $\begin{bmatrix} b_{r-s}^{(u)} \\ \text{---} \\ h_j \end{bmatrix}$, $u \in \{0, \dots, 2^{r-s} - 1\}, j \in \{1, \dots, n_s\}$, be a column of H_r of

$$(12). \text{ Let } M_r = \left[\begin{array}{c|c} K_{r-s} & T_{r-s,s} \\ \text{---} & \text{---} \\ Z_{s,r-s} & A_s \end{array} \right] \in \Gamma_r. \text{ Then}$$

$$\left[\begin{array}{c|c} K_{r-s} & T_{r-s,s} \\ \text{---} & \text{---} \\ Z_{s,r-s} & A_s \end{array} \right] \begin{bmatrix} b_{r-s}^{(u)} \\ \text{---} \\ h_j \end{bmatrix} = \begin{bmatrix} K_{r-s} b_{r-s}^{(u)} + T_{r-s,s} h_j \\ \text{---} \\ A_s h_j \end{bmatrix} \in H_r.$$

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

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

□

In general, $\Gamma_r \neq \text{Aut}(H_r)$. For example, if we apply repeatedly doubling construction starting from matrix M (so, $s = 2$), the columns of H_r form a 2^{r-1} -cap of $\text{PG}(r-1, 2)$ that is the complement of a hyperplane; its stabilizer group is $\text{AGL}(r-1, 2)$ and $|\text{AGL}(r-1, 2)| = (2^r - 2) \dots (2^r - 2^{r-1})$. Note that the mentioned cap corresponds to the $[2^{r-1}, 2^{r-1} - r, 4]$ extended Hamming code.

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

Lemma 2. Let $X = \{x_1, \dots, x_n\}$ be a set of n boolean values. Let Σ_n be the multiset of all possible 2^n sums of elements of X (counting also the sum without addends and attributing the value 0 to it). If at least one of the elements of X is equal to 1 then Σ_n contains 2^{n-1} zeros and 2^{n-1} ones.

Proof: By induction on n . The case $n = 1$ is trivial. In the general case consider the 2^{n-1} sums that do not contain x_n . If an index i , $1 \leq i \leq n-1$, exists such that $x_i = 1$, then by the inductive hypothesis 2^{n-2} sums are equal to 0 and 2^{n-2} sums are equal to 1. Adding x_n we obtain other 2^{n-2} sums equal to 0 and 2^{n-2} sums equal to 1 whether $x_n = 0$ or $x_n = 1$. If $x_i = 0$, $i = 1, \dots, n-1$, then the 2^{n-1} sums not containing x_n are equal to 0, $x_n = 1$ and the 2^{n-1} sums containing x_n are equal to 1. □

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

Proof: Let $\ell = r - s$. Let $H_s = [h_1 \dots h_{n_s}]$ where h_i is an s -positional column. By Lemma 1, H_r of the form (12) is a parity check matrix of the code C_r . Let

$$(14) \quad M_r = \left[\begin{array}{ccc|ccc} & & & t_1 & & \\ & & & \vdots & & \\ & K_\ell & & & & \\ & & & t_\ell & & \\ \hline & & & & & \\ & & & & & \\ x_{\ell+1,1} \dots x_{\ell+1,\ell} & & & a_1 & & \\ \vdots & & & \vdots & & \\ x_{r,1} \dots x_{r,\ell} & & & a_s & & \end{array} \right] \in \text{Aut}(C_r),$$

where K_ℓ is an $\ell \times \ell$ matrix, t_i and a_j are s -positional rows, and $x_{i,j} \in \{0, 1\}$. Let r_j be the j -th row of $M_r H_r$, $j = \ell + 1, \dots, r$. Then

$$r_j = \left[a_{j-\ell} h_1^T \dots a_{j-\ell} h_{n_s}^T \mid x_{j,1} + a_{j-\ell} h_1^T \dots x_{j,1} + a_{j-\ell} h_{n_s}^T \mid x_{j,2} + a_{j-\ell} h_1^T \dots x_{j,2} + a_{j-\ell} h_{n_s}^T \mid \dots \right. \\ \left. \dots \mid x_{j,1} + \dots + x_{j,\ell} + a_{j-1} h_1^T \dots x_{j,1} + \dots + x_{j,\ell} + a_{j-\ell} h_{n_s}^T \right].$$

As $M_r \in \text{Aut}(C_r)$, it induces a permutation on the coordinates of the codewords, so

$$\text{weight}(r_j) = \text{weight}(q_j) = 2^\ell \cdot \text{weight}(p_{j-\ell}),$$

where q_j is the j -th row of H_r and p_i is the i -th row of H_s . On the other hand, fix a value i , $1 \leq i \leq n_s$, and consider the elements of r_j in positions $i + (k-1)n_s$, $k = 1, \dots, 2^\ell$, they are: $a_{j-\ell} h_i^T, x_{j,1} + a_{j-\ell} h_i^T, x_{j,2} + a_{j-\ell} h_i^T, \dots, x_{j,1} + x_{j,2} + a_{j-\ell} h_i^T, \dots, x_{j,1} + \dots + x_{j,\ell} + a_{j-\ell} h_i^T$. All possible sums of elements of the set $\{x_{j,1}, \dots, x_{j,\ell}\}$ appear as addends of $a_{j-\ell} h_i^T$. If at least one of the $x_{j,t}$ is equal to 1, then, by Lemma 2, exactly $2^{\ell-1}$ of these sums are equal to 1, and therefore exactly $2^{\ell-1}$ of these elements of r_j are equal to 1. It implies $\text{weight}(r_j) = n_s 2^{\ell-1}$ and $\text{weight}(p_{j-\ell}) = \text{weight}(r_j)/2^\ell = n_s/2$. This is not possible by hypothesis. Moreover, $x_{\ell+1,1} = \dots = x_{\ell+1,\ell} = \dots = x_{r,1} = \dots = x_{r,\ell} = 0$ implies $\text{Det}(K_\ell) \neq 0$, otherwise $\text{Det}(M_r) = 0$.

Finally, we show that the $s \times s$ submatrix

$$A_s = \begin{bmatrix} a_1 \\ \vdots \\ a_s \end{bmatrix}$$

permutes the columns of H_s , i.e., it belongs to $\text{Aut}(C_s)$. In fact, let $\begin{bmatrix} b_{r-s}^{(u)} \\ \vdots \\ h_j \end{bmatrix}$,

$u \in \{0, \dots, 2^{r-s} - 1\}$, $j \in \{1, \dots, n_s\}$, be a column of H_r of (12). Then, taking into account that $x_{i,j} = 0$ in M_r of (14), we have

$$M_r \begin{bmatrix} b_{r-s}^{(u)} \\ \vdots \\ h_j \end{bmatrix} = \begin{bmatrix} y \\ \vdots \\ A_s h_j \end{bmatrix},$$

where y is an $(r-s)$ -positional column. The column $\begin{bmatrix} y \\ - \\ A_s h_j \end{bmatrix}$ is a column of H_r if and

only if $A_s h_j$ is a column of H_s . Moreover, if $A_s h_i = A_s h_j$, $i \neq j$, then the $2^{\ell+1}$ columns

$$\begin{bmatrix} b_{r-s}^{(u)} \\ - \\ h_i \end{bmatrix}, \begin{bmatrix} b_{r-s}^{(u)} \\ - \\ h_j \end{bmatrix}, u = 0, \dots, 2^\ell - 1, \text{ can have only } 2^\ell \text{ different images under } M_r. \quad \square$$

Corollary 2. Let 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 code C_r obtained applying doubling construction $r-s$ times starting from H_s , it holds that $\text{Aut}(C_r) = \Gamma_r$.

By computer search, we obtained the following proposition.

Proposition 5. For the matrices of (2), (8)-(10), it holds that

$$|\text{Aut}(S)| = 120, |\text{Aut}(\Omega)| = 336, |\text{Aut}(\Phi_1)| = 40\,320, |\text{Aut}(\Phi_2)| = 576, |\text{Aut}(\Phi_3)| = 384, \\ |\text{Aut}(\Phi_4)| = 720, |\text{Aut}(\Phi_5)| = 11\,520.$$

Corollary 3. Let the value of $|\text{Aut}(\Phi_j)|$ be as in Proposition 5. It holds that

$$|\text{Aut}(\Pi_r)| = 120 \cdot 2^{4(r-4)} \prod_{i=0}^{r-3} (2^{r-4-i} - 2^i), \\ |\text{Aut}(W_r)| = 336 \cdot 2^{5(r-5)} \prod_{i=0}^{r-4} (2^{r-5-i} - 2^i), \\ |\text{Aut}(V_{r,j})| = |\text{Aut}(\Phi_j)| \cdot 2^{6(r-6)} \prod_{i=0}^{r-5} (2^{r-6-i} - 2^i), j = 1, \dots, 5.$$

Proof. Taking into account that all matrices of (2), (8)-(10), have an odd number of columns, the assertion follows from Proposition 4, Corollary 2, and Proposition 5. \square

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

Problems connected with error detection are considered, e.g., in [3, 8-11, 13], see also the references therein. Here we consider a *binary symmetric channel*.

Let p be the symbol error probability of the channel.

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

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

Definition 3 [8-11]. (i) A binary code C is proper (respectively t -proper) if $P_{ue}(C, p)$ (respectively $P_{ue}^{(t)}(C, p)$) 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 (respectively t -proper) in the interval $[a, b]$ if $P_{ue}(C, p)$ (respectively $P_{ue}^{(t)}(C, p)$) is an increasing function of p in $[a, b]$.

Using the results of this work, in particular Theorem 3 and Proposition 3, and papers [2, 3, 8-11], we proved a number of results on the properness and t -properness of codes obtained by doubling construction.

Theorem 7 [11, Theorem 2]. Let a binary code of length n have dual distance d^\perp . If

$$\left\lceil \frac{n}{3} \right\rceil + 1 \leq d^\perp \leq \left\lfloor \frac{n}{2} \right\rfloor,$$

then the code is proper in the interval

$$\left[\frac{n+1-2d^\perp}{n-d^\perp}, \frac{1}{2} \right].$$

Lemma 3. 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 d_{r-1}^\perp in the region

$$(15) \quad \left\lceil \frac{n_{r-1}}{3} \right\rceil + 1 \leq d_{r-1}^\perp \leq \left\lfloor \frac{n_{r-1}}{2} \right\rfloor.$$

Then the resultant $[n_r, n_r - r, d_r]$ code, given by the parity check matrix H_r , has dual distance d_r^\perp in the region

$$(16) \quad \left\lceil \frac{n_r}{3} \right\rceil + 1 \leq d_r^\perp \leq \left\lfloor \frac{n_r}{2} \right\rfloor.$$

Proof: By (1) and (11), we has $n_r = 2n_{r-1}$ and $d_r^\perp = 2d_{r-1}^\perp$.

The right inequality of (15) corresponds to either $2d_{r-1}^\perp \leq n_{r-1}$ (if n_{r-1} is even), or $2d_{r-1}^\perp \leq n_{r-1} - 1$ (if n_{r-1} is odd). The right inequality of (16) always corresponds to $2d_{r-1}^\perp \leq n_{r-1}$. So, for all values of n_{r-1} , the right part of (16) follows from the right part of (15).

The left inequality of (15) (respectively of (16)) corresponds to one of three cases:

- $n_{r-1} + 3 \leq 3d_{r-1}^\perp$ (respectively $n_{r-1} + 1.5 \leq 3d_{r-1}^\perp$) if $n_{r-1} \equiv 0 \pmod{3}$;
- $n_{r-1} + 5 \leq 3d_{r-1}^\perp$ (respectively $n_{r-1} + 2 \leq 3d_{r-1}^\perp$) if $n_{r-1} \equiv 1 \pmod{3}$;
- $n_{r-1} + 4 \leq 3d_{r-1}^\perp$ (respectively $n_{r-1} + 2.5 \leq 3d_{r-1}^\perp$) if $n_{r-1} \equiv 2 \pmod{3}$.

So, for all values of n_{r-1} , the left part of (16) follows from the left part of (15). \square

Theorem 8. The codes Π_r , $V_{r,4}$, and $V_{r,5}$, are proper in intervals $[a, \frac{1}{2}]$, where

$$\Pi_r^\perp: a = \frac{1}{3} + \frac{1}{3 \cdot 2^{r-4}}, \quad r \geq 6; \quad V_{r,4}: a = \frac{5}{11} + \frac{1}{11 \cdot 2^{r-6}}, \quad r \geq 8;$$

$$V_{r,5}: a = \frac{3}{10} + \frac{1}{10 \cdot 2^{r-6}}, r \geq 6.$$

Proof. We use Proposition 3, Theorem 7, and Lemma 3. \square

Proposition 6 [11, Remark 1]. An $[n, n-r, d]$ code is proper in the interval $[0, \frac{d}{n}]$.

Proposition 7. The codes $\Pi_r^\perp, W_r^\perp, V_{r,j}^\perp$ dual to the codes $\Pi_r, W_r, V_{r,j}$, are proper in intervals $[0, b]$, where

$$b = \frac{2}{5} \text{ for } \Pi_r^\perp, b = \frac{2}{9} \text{ for } W_r^\perp, b = \frac{2}{17} \text{ for } V_{r,1}^\perp, b = \frac{4}{17} \text{ for } V_{r,2}^\perp, \\ b = \frac{5}{17} \text{ for } V_{r,3}^\perp, b = \frac{6}{17} \text{ for } V_{r,4}^\perp, b = \frac{7}{17} \text{ for } V_{r,5}^\perp.$$

Proof. We use Propositions 3 and 6. \square

Definition 4 [8-10].

- Let C be an $[n, n-r, d]$ code with dual weight spectrum $\{A_0^\perp, \dots, A_n^\perp\}$. Dual extended binomial moment B_ℓ^* is defined as follows:

$$B_\ell^* = \frac{1}{\binom{n}{\ell}} \sum_{i=1}^{\ell} \binom{n-i}{n-\ell} A_i^\perp, \ell = 1, \dots, n.$$

- Let C be an $[n, n-r, d]$ code. Let $Q_{h,i}$ be the number of vectors of weight i in the cosets of weight h , excluding the coset leaders. We define the following values:

$$(17) \quad A_{\ell,t}^* = \frac{1}{\binom{n}{\ell}} \sum_{i=t+1}^{\ell} \binom{n-i}{n-\ell} \sum_{h=0}^t Q_{h,i}, \ell = t+1, \dots, n.$$

Theorem 9 [8, Theorem 6]. Let C be an $[n, n-r, d]$ binary code with dual distance d^\perp and dual extended binomial moments $\{B_1^*, \dots, B_n^*\}$. Let $d + d^\perp \leq n$. If

$$B_{n-\ell}^* \leq B_{n-\ell+1}^* - 2^{r-\ell}, \ell = d+1, \dots, n-d^\perp+1,$$

then C is proper.

Proposition 8. The codes with the parity check matrices S and Ω are proper. The codes Π_r with $r = 5, 6, 7, 8, 9$ are proper. The code W_6 is proper.

Proof. We use Proposition 3 and Theorem 9. \square

Proposition 9. The codes Π_r with $10 \leq r \leq 20$ are not proper.

Proof. Using [9, Equation (2.2)] and Proposition 3, we obtain

$$P_{ue}(\Pi_r, p) = \frac{1}{2^r} (1 + 10(1-2p)^{2^{r-3}} + (2^r - 16)(1-2p)^{5 \cdot 2^{r-5}} + \\ + 5(1-2p)^{2^{r-2}}) - (1-p)^{5 \cdot 2^{r-4}}.$$

The corresponding derivative by p is

$$P'_{ue}(\Pi_r, p) = 5(-\frac{1}{2}(1-2p)^{2^{r-3}-1} - (2^{r-4}-1)(1-2p)^{5 \cdot 2^{r-5}-1} - \frac{1}{2}(1-2p)^{2^{r-2}-1} + \\ + 2^{r-4}(1-p)^{5 \cdot 2^{r-4}-1}).$$

Taking into account Theorem 8, we checked by computer that, for $10 \leq r \leq 20$, in the region $\left(0, \frac{1}{3} + \frac{1}{3 \cdot 2^{r-4}}\right)$ there exist values of p such that the derivative $P'_{ue}(\Pi_r, p)$ is negative. \square

Theorem 10 [10, Theorem 2]. Let C be an $[n, n-r, d]$ binary code with $A_{\ell,t}^*$ as in (17). If

$$A_{\ell,t}^* - 2A_{\ell-1,t}^* \geq 0, \ell = t+2, \dots, n,$$

then C is t -proper.

Proposition 10. The codes with the parity check matrices S and Ω are 1-proper. The codes Π_r with $r = 5, 6, 7$ are 1-proper. The code W_6 is 1-proper.

Proof: We use Theorem 10. In order to calculate the values of $A_{\ell,t}^*$, we take the parity check matrices of the corresponding codes. \square

Acknowledgements: 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). 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 Ga-lois e strutture di incidenza”) and by the Italian National Group for Algebraic and Geometric Structures and their Applications (GNSAGA-INDAM).

References

1. Afanasiev, V. B., A. A. Davydov. Weight Spectrum of Quasi-Perfect Binary Codes with Distance 4. – In: Proc. of IEEE Int. Symp. Inform. Theory (ISIT’17), Aachen, Germany, 2017, pp. 2193-2197.
<http://ieeexplore.ieee.org/document/8006918/>
2. Afanasiev, V. B., A. A. Davydov, D. K. Ziganigirov. Design and Analysis of Codes with Distance 4 and 6 Minimizing the Probability of Decoder Error. – J. Commun. Technology Electronics, Vol. **61**, 2016, No 12, pp. 1440-1455.
3. Baicheva, T., S. Dodunekov, P. Kazakov. On the Undetected Error Probability Performance of Cyclic Redundancy-Check Codes of 16-bit Redundancy. – IEEE Trans. Comm., Vol. **147**, 2000, No 5, pp. 253-256.
4. Bartoli, D., S. Marcugini, F. Pambianco. A Computer Based Classification of Caps in PG(5, 2). arXiv:1203.0994 [math.CO], 2012.
5. Davydov, A. A., S. Marcugini, F. Pambianco. Further Results on Binary Codes Obtained by Doubling Construction. – In: Proc. Eighth International Workshop on Optimal Codes and Related Topics, OC’17 (in Second International Conference “Mathematics Days in Sofia”), Sofia, Bulgaria, 2017, pp. 73-80.
6. Davydov, A. A., L. M. Tomba. Quasiperfect Linear Binary Codes with Minimal Distance 4 and Complete Caps in Projective Geometry. – Problems Inform. Transm., Vol. **25**, 1989, No 4, pp. 265-275.
7. Davydov, A. A., L. M. Tomba. An Alternative to the Hamming Code in the Class of SEC-DED Codes in Semiconductor Memory. – IEEE Trans. Inform. Theory, Vol. **IT-37**, 1991, No 3, pp. 897-902.

8. D o d u n e k o v a, R. Extended Binomial Moments of a Linear Code and the Undetected Error Probability. – Problems Inform. Transm., Vol. **39**, 2003, No 3, pp. 255-265.
9. D o d u n e k o v a, R., S. M. D o d u n e k o v, E. N i k o l o v a. A Survey on Proper Codes. – Discrete Appl. Math., Vol. **156**, 2008, No 9, pp. 1499-1509.
10. D o d u n e k o v a, R., S. M. D o d u n e k o v. t -Good and t -Proper Linear Error Correcting Codes. – Mathematica Balkanica. New Series, Vol. **17**, 2003, No 1-2, pp.147-154.
11. D o d u n e k o v a, R., E. N i k o l o v a. Sufficient Conditions for Monotonicity of the Undetected Error Probability for Large Channel Error Probabilities. – Probl. Inform. Transm., Vol. **41**, 2005, No 3, pp. 187-198.
12. K h a t i r i n e j a d, M., P. L i s o n e k. Classification and Constructions of Complete Caps in Binary Spaces. – Des. Codes Cryptogr., Vol. **39**, 2006, No 1, pp. 17-31.
13. K l ø v e, T. Codes for Error Detection. Singapore, World Scientific, 2007.
14. M a c W i l l i a m s, F. J., N. J. A. S l o a n e. The Theory of Error-Correcting Codes. North-Holland, Amsterdam, 1977.
15. P a n c h e n k o, V. I. On Optimization of Linear Code with Distance 4. – In: Proc. of 8th All-Union Conf. on Coding Theory and Communications, Kuibyshev, 1981, Part 2: Coding Theory, Moscow, 1981, pp. 132-134 (in Russian).

Received 30.09.2017; Accepted 08.12.2017