Further results on binary codes obtained by doubling construction

Alexander A. Davydov[@] Stefano Marcugini[*] Fernanda Pambianco[*]

@ Institute for Information Transmission Problems (Kharkevich Institute), Russian Academy of Science, Moscow, Russia
* Department of Mathematics and Informatics, Perugia University, Perugia, Italy

Eighth International Workshop on Optimal Codes and Related Topic, Sofia, Bulgaria, July 10–14, 2017

INTRODUCTION

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 **stabilizer group** $\mathrm{Aut}(H_r)$ of parity check matrix of codes obtained by doubling construction is studied.

The **properness** and t-properness for error detection of codes obtained by doubling construction are considered.

NOTATION. Connection with PROJECTIVE GEOMETRIES

$[n, n-r, d]$ **code** $\leftrightarrow$ linear binary code of length n, redundancy r, and minimum distance d.

A code with $d = 4$ is **quasi-perfect** if it has covering radius 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 $r-1$. We use this for stabilizer group of the matrix.

All our results can be treated in geometrical language.

TWO VERY IMPORTANT properties of quasi-perfect codes

1. 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 $r \rightarrow$

We should investigate namely quasi-perfect codes

2. All quasi-perfect $[n, n-r, 4]$ codes with $n \geq 2^{r-2} + 2$ can be described by **doubling construction**

[4] A.A. Davydov, L.M. Tombak, ACCT1988 and PrInfTransm 1989

It is appropriate to study quasi-perfect $[n, n-r, 4]$ codes from the point of view of doubling construction.

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

$$H_r = \left[\begin{array}{c|c} 0\ldots0 & 1\ldots1 \\ ----- & --- \\ H_{r-1} & H_{r-1} \end{array}\right].$$

$n_r = 2n_{r-1}$.

$$d_{r-1} = 3 \rightarrow d_r = 3.$$
$$d_{r-1} \geq 4 \rightarrow d_r = 4$$

USEFUL MATRICES for DOUBLING CONSTRUCTION

$B^{(r)}_{j,g} = [b_j \dots b_j] \leftrightarrow (r-g-2) \times (2^g+1)$ matrix of **identical columns** b_j

$r \leftrightarrow$ code redundancy; $b_j \leftrightarrow$ binary presentation of j

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

Hamming code M *Panchenko code* Π_r *code* $\mathcal{W}_r$

Panchenko code has the minimal possible number of codewords of weight 4

Quasi-perfect codes with $d = 4$. Length. Construction

THEOREM 1. [Davydov, Tombak 1988, 1989]

$n_r \geq 2^{r-2} + 2$. $[n_r, n_r - r, 4]$ quasi-perfect code

(i) $n_r = (2^g + 1)2^{r-2-g}, \quad g = 0, 2, 3, 4, \ldots, r-3$

The such and only such lengths are possible.

(ii) Parity check matrix H_r **always** can be transformed to form

$$H_r = \left[\begin{array}{c|c|c|c} B_{0,g}^{(r)} & B_{1,g}^{(r)} & \ldots & B_{D,g}^{(r)} \\ \hline H_{g+2} & H_{g+2} & & H_{g+2} \end{array}\right], \quad (3)$$

$D = 2^{r-g-2} - 1$, $H_{0+2} = M$, $H_{2+2} = S$, $H_{3+2} = \Omega$smallskip

H_{g+2} = PCM of QP $[2^g + 1, 2^g + 1 - (g+2), 4]$ code, $g \geq 4$

(3) is the result of $r - g - 2$ applying of doubling construction

MAIN TOOL for NEW RESULTS

We obtain properties of resultant codes of doubling construction on the base of the corresponding properties of the starting code: classification, dual weight spectrum, stabilizer group of parity check matrix, properness for error detection,...

For every property, connections between starting and resultant codes are investigated in special manner. Our contributions are to explain these connections.

Quasi-perfect codes with $d = 4$. CLASSIFICATION

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

THEOREM 2. Φ_j is a parity check matrix of $[17, 11, 4]$ code. 5 codes with the parity check matrices $\Phi_1, \ldots, \Phi_5$ are all distinct $[2^4 + 1, 2^4 + 1 - (4 + 2), 4]$ quasi-perfect codes.

matrices Φ_j are given in Proceedings

Quasi-perfect codes with $d = 4$. DUAL weight spectrum

THEOREM 3. Let $\{A^{\perp}_w(\mathcal{T}_{g+2}),\ w = 0, 1, \ldots, 2^g + 1\}$ be 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 (3).
Then 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

$$A^{\perp}_{w2^{r-2-g}}(\mathcal{C}_r) = A^{\perp}_w(\mathcal{T}_{g+2}),\ w = 0, 1, \ldots, 2^g + 1;$$
$$A^{\perp}_{(2^g+1)2^{r-3-g}}(\mathcal{C}_r) = 2^r - 2^{g+2}$$

Doubling construction. STABILIZER GROUP

$\mathcal{C} \rightarrow [n, n-r]$ **binary** code with parity check matrix H

$\mathrm{Aut}(H) \leftrightarrow$ stabilizer group of columns of H treated as points of $\mathrm{PG}(r-1, 2)$

We obtain stabilizer group of resultant matrix of doubling construction from stabilizer group of starting matrix

Doubling construction. STABILIZER GROUP

$\Gamma_r \leftrightarrow$ set of matrices

H_s – starting matrix of doubling construction

$GL(n,2) \leftrightarrow$ general linear group ($n \times n$ invertible matrices)

$$\Gamma_r := \left\{ \left[\begin{array}{c|c} K_{r-s} & T_{r-s,s} \\ \hline Z_{s,r-s} = \mathbf{0} & A_s \end{array} \right] : K_{r-s} \in \mathrm{GL}(r-s,2) \right\}$$

$T_{r-s,s}$ is **any** binary $(r-s) \times s$ matrix, $\quad A_s \in \mathrm{Aut}(H_s)$.

$$|\Gamma_r| = |\mathrm{GL}(r-s,2)| \cdot |\mathrm{Aut}(H_s)| \cdot 2^{(r-s)s}$$

$$|\mathrm{GL}(r-s,2)| = (2^{r-s}-1)(2^{r-s}-2)\ldots(2^{r-s}-2^{r-s-1})$$

Doubling construction. STABILIZER GROUP

H_r – resultant matrix of doubling construction ($r - s$ times)

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

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 $n/2$ (in particular with n **odd**).

Then for matrix H_r obtained applying doubling construction r-s times starting from H_s, we have $\mathrm{Aut}(H_r) = \Gamma_r$.

.....

All quasi-perfect $[n, n-r, 4]$ codes (except for Hamming code) have starting matrix H_{g+2} with the **odd** number of columns $2^{g+1} + 1$

Properness and t-properness. Literatura

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

R. Dodunekova, Extended Binomial Moments of a Linear Code and the Undetected Error Probability, *Problems Inform. Transm.*, **39**, 255–26, 2003.

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

T. Kløve, *Codes for Error Detection*, World Scientific, 2007.

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

Properness and t-properness. Definitions

p – the error probability by symbol in the channel.
$P_{ue}(C, p)$ – the undetected error probability for the code C under condition that the code is used only for error detection;
$P_{ue}^{(t)}(C, p)$ – the undetected error probability for the code C under condition that the code is used for correction of $\leq t$ errors.

Definition

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

Lemma 2. In doubling construction, 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 $\left\lceil \frac{1}{3} n_{r-1} \right\rceil \leq d^{\perp}_{r-1} \leq \frac{1}{2} n_{r-1}$. Then the resultant $[n_r, n_r - r, d_r]$ code given by the parity check matrix H_r has dual distance in $\left\lceil \frac{1}{3} n_r \right\rceil \leq d^{\perp}_{r} \leq \frac{1}{2} n_r$.

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 $\mathcal{V}_{r,5}$.

Properness and t-properness. Doubling construction

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. Starting codes with parity check matrices S and Ω are proper and 1-proper.

Codes Π_r (with starting matrix S) are proper for $r = 5$–9 and 1-proper for $r =$5–7.

Codes $\mathcal{W}_r$ (with starting matrix Ω) are proper and 1-proper for $r = 6$.

However, codes Π_r are not proper for $r = 10$–20.

Thank you Spasibo

Premnogo blagodarya

Mille grazie

!‘Muchas gracias

Toda raba

Merci beaucoup

Dankeschön

Dank u wel

Domo arigato