MATHEMATICAL COMMUNICATIONS
Math. Commun. **18**(2013), 297–308

Binary doubly-even self-dual codes of length 72 with large automorphism groups*

Dean Crnković[1,†], Sanja Rukavina[1] and Loredana Simčić[2]

[1] *Department of Mathematics, University of Rijeka, Radmile Matejčić 2, HR-51 000 Rijeka, Croatia*
[2] *Faculty of Engineering, University of Rijeka, Vukovarska 58, HR-51 000 Rijeka, Croatia*

Received February 2, 2013; accepted April 12, 2013

Abstract. We study binary linear codes constructed from fifty-four Hadamard 2-$(71,35,17)$ designs. The constructed codes are self-dual, doubly-even and self-complementary. Since most of these codes have large automorphism groups, they are suitable for permutation decoding. Therefore we study PD-sets of the obtained codes. We also discuss the error-correcting capability of the obtained codes by majority logic decoding. Further, we describe a construction of a 3-$(72,12,11)$ design and a 3-$(72,16,2010)$ design from a binary $[72,16,12]$ code, and a construction of a strongly regular graph with parameters $(126,25,8,4)$ from a binary $[35,8,4]$ code related to a derived 2-$(35,17,16)$ design.

AMS subject classifications: 94B05, 05B20, 05B05, 05E30

Key words: self-dual code, Hadamard matrix, strongly regular graph

1. Introduction

Error-correcting codes that have large automorphism groups can be useful in applications as the group can be useful in decoding algorithms; see [9, Part 2, Chapter 17] and [22] for a discussion of possibilities. Especially, codes with large automorphism groups are suitable for permutation decoding, since permutation decoding can be used when a code has a sufficiently large automorphism group to ensure the existence of a set of automorphisms, called a PD-set, that has some specific properties (see [11, 12, 13, 16]). In this paper we study doubly-even self-dual binary linear codes of length 72, constructed from Hadamard designs with parameters 2-$(71,35,17)$. The obtained codes have large automorphism groups, hence they are possibly suitable for permutation decoding. Moreover, the constructed codes are self-dual. The class of self-dual codes is important in coding theory from both theoretical and practical reasons. Self-dual codes are in particular of interest because many of the best codes known are of this type. For example, self-dual ternary codes include among others the ternary Golay code of length 12, the quadratic residue codes and the symmetry codes. A comprehensive study of self-dual codes can be found in [18].

*This work was supported by the Ministry of Science, Education and Sports, Republic of Croatia, grant 319-0000000-3037.
†Corresponding author. *Email addresses:* `deanc@math.uniri.hr` (D. Crnković), `sanjar@math.uniri.hr` (S. Rukavina), `lsimcic@riteh.hr` (L. Simčić)

A code C of length n over an alphabet $\mathbf{F}_q$ of size q is a subset $C \subseteq \mathbf{F}_q^n$. A code is binary if $q = 2$. Elements of a code are called codewords. For $x = (x_1, \dots, x_n)$, $y = (y_1, \dots, y_n) \in \mathbf{F}_q^n$, the number $d(x, y) = |\{i \,|1 \leq i \leq n,\, x_i \neq y_i\}|$ is called a Hamming distance. A minimum distance of a code C is a number $d = min\{d(x, y) \,|x, y \in C, x \neq y\}$.

Two codes are equivalent if one of the codes can be obtained from the other by permuting the coordinates in all codewords, and permuting the symbols within one or more coordinate positions. Two codes are isomorphic if one can be obtained from the other by permuting the coordinates only. An automorphism of a code C is an isomorphism from C to C.

For $x \in \mathbf{F}_q^n$ we define the weight $\omega(x)$ of x by $\omega(x) = d(x, 0)$. The weight enumerator of a code C is the polynomial $A(x) = \sum_{i=0}^{n} A_i x^i$, where A_i is the number of codewords of weight i. A code is even if all weights are even, and doubly-even if all weights are divisible by 4.

Let q be a prime power and $\mathbf{F}_q$ the finite field of order q. A linear code of length n is a linear subspace of the vector space $\mathbf{F}_q^n$. A k-dimensional subspace of $\mathbf{F}_q^n$ is called a linear $[n, k]$ code over $\mathbf{F}_q$. For a linear code C its minimum distance is equal to its minimum weight $min\{\omega(x) \,|x \in C, x \neq 0\}$. A linear $[n, k, d]$ code is a linear $[n, k]$ code with minimum distance (or weight) d.

An $[n, k, d]$ linear code can correct up to $\left\lfloor \frac{d-1}{2} \right\rfloor$ errors.

An information set for $[n, k, d]$ code C is a set of k coordinate positions such that the corresponding columns of the generator matrix are linearly independent.

Let C be a t-error-correcting code with information set $\mathcal{I}$. A PD-set for C is a set $\mathcal{S}$ of automorphisms of C which is such that every t-set of coordinate positions is moved by at least one member of $\mathcal{S}$ out of the information set $\mathcal{I}$.

A minimum size a PD-set can have is given by the following theorem by Gordon (see [8]).

Theorem 1. *If $\mathcal{S}$ is a PD-set for a t-error correcting $[n, k, d]$ code C, and $r = n-k$, then*

$$|\mathcal{S}| \geq \left\lceil \frac{n}{r} \left\lceil \frac{n-1}{r-1} \left\lceil \cdots \left\lceil \frac{n-t+1}{r-t+1} \right\rceil \cdots \right\rceil \right\rceil \right\rceil .$$

PD-sets are used for permutation decoding, an algorithm for decoding linear codes. The algorithm was introduced by MacWilliams in 1964 and it can be found in [15] and [16].

A non-zero codeword is called normalized if the leftmost non-zero component is 1. In a binary code, every codeword is normalized. The support of a nonzero vector $x = (x_1 \dots, x_n) \in F_q^n$ is the set of indices of its nonzero coordinates, i.e. $supp(x) = \{i \,|x_i \neq 0\}$. A nonzero codeword c of a binary linear code C is called minimal in C if $supp(c)$ does not cover the support of another nonzero codeword.

Minimal codewords are important from a cryptographic point of view, since these words are used in particular secret sharing schemes (see [17]).

Let G be a generator matrix of a linear code C. Given a codeword $c \in C$, let G_c denote the submatrix consisting of the columns of G corresponding to the components of c that have value 0, and let ρ_c denote the rank of G_c.

The following statement can be found in [14, Theorem 2]:

Theorem 2. *A codeword c is minimal if and only if c is normalized and $\rho_c = k-1$.*

The dual code $C^{\perp}$ of a code C is its orthogonal space with respect to the usual dot product in $\mathbf{F}_q^n$. The dual code of an $[n,k]$ code is an $[n,n-k]$ code. An $[n,k]$ code is called self-orthogonal if $C \subset C^{\perp}$, and self-dual if $C = C^{\perp}$. The length of a self-dual code is even and $n = 2k$. A binary code is called self-complementary if it contains the all-one vector.

A t-(v,k,λ) design is a finite incidence structure $(\mathcal{P},\mathcal{B},\mathcal{I})$ satisfying the following requirements:

1. $|\mathcal{P}| = v$,
2. every element of $\mathcal{B}$ is incident with exactly k elements of $\mathcal{P}$,
3. every t elements of $\mathcal{P}$ are incident with exactly λ elements of $\mathcal{B}$.

The elements of a set $\mathcal{P}$ are called points and the elements of a set $\mathcal{B}$ are called blocks. A 2-(v,k,λ) design is called a block design. If $|\mathcal{P}| = |\mathcal{B}| = v$ and $2 \leq k \leq v-2$, then a 2-(v,k,λ) design is called a symmetric design. Given two designs $\mathcal{D}_1 = (\mathcal{P}_1,\mathcal{B}_1,\mathcal{I}_1)$ and $\mathcal{D}_2 = (\mathcal{P}_2,\mathcal{B}_2,\mathcal{I}_2)$, an isomorphism from $\mathcal{D}_1$ onto $\mathcal{D}_2$ is a bijection which maps points onto points and blocks onto blocks preserving the incidence relation. An isomorphism from a symmetric design $\mathcal{D}$ onto itself is called an automorphism of $\mathcal{D}$. The set of all automorphisms of $\mathcal{D}$ forms its full automorphism group denoted by $\mathrm{Aut}(\mathcal{D})$.

Let $\mathcal{D} = (\mathcal{P},\mathcal{B},\mathcal{I})$ be a symmetric 2-(v,k,λ) design. Excluding from $\mathcal{D}$ a block x and all points that are not incident with that block, one obtains its derived design $\mathcal{D}_x$ with parameters $2-(k,\lambda,\lambda-1)$, provided that $\lambda \geq 2$. Further, excluding from the design $\mathcal{D}$ a block x and all points incident with that block, provided that $k \geq \lambda+2$, one obtains its residual design $\mathcal{D}^x$ with parameters $2-(v-k,k-\lambda,\lambda)$.

A Hadamard matrix of order m is an $m \times m$ matrix $H = (h_{i,j})$, $h_{i,j} \in \{-1,1\}$, satisfying $HH^{\top} = H^{\top}H = mI_m$, where I_m is an $m \times m$ identity matrix. Two Hadamard matrices are equivalent if one can be transformed into the other by a series of row or column permutations and negations. From each Hadamard matrix of order m one can obtain a symmetric $(m-1, \frac{1}{2}m-1, \frac{1}{4}m-1)$ design. Also, from any symmetric $(m-1, \frac{1}{2}m-1, \frac{1}{4}m-1)$ design we can recover a Hadamard matrix. Symmetric designs with parameters $(m-1, \frac{1}{2}m-1, \frac{1}{4}m-1)$ are called Hadamard designs. Let $(\mathcal{P},\mathcal{B},\mathcal{I})$ be a Hadamard $(m-1, \frac{1}{2}m-1, \frac{1}{4}m-1)$ design and let ∞ be a new symbol. We construct a new design $\mathcal{D}^*$ with the point set $\mathcal{P}^* = \mathcal{P} \cup \{\infty\}$ and a block set defined as follows: for the blocks containing ∞ we take all the blocks of $\mathcal{B}$ with ∞ adjoined; for the blocks not containing ∞ we take the complements (in $\mathcal{P}$) of the blocks of $\mathcal{B}$. Then $\mathcal{D}^*$ is a 3-$(m, \frac{1}{2}m, \frac{1}{4}m-1)$ design. Any design with parameters $(m, \frac{1}{2}m, \frac{1}{4}m-1)$ is called a Hadamard 3-design.

Definition 1. *Let $\mathcal{S} = (\mathcal{P},\mathcal{B},\mathcal{I})$ be an incidence structure. The code of $\mathcal{S}$ over the field F is the subspace $C_F(S)$ of $F^{\mathcal{P}}$ spanned by the vectors corresponding to the characteristic functions of the blocks of $\mathcal{S}$.*

The following statement can be found in [1, Corollary 7.4.1]:

Theorem 3. *For any prime p and any equivalence class of Hadamard matrices, there is, up to code equivalence, only one p-ary code associated with the 3-design from the equivalence class.*

Definition 2. *If H is a Hadamard matrix, then the p-ary code of H, denoted by $C_p(H)$, is a p-ary code associated with any 3-design defined by H.*

In this article we study 12 binary linear codes spanned by rows of block-by-point incidence matrices of the symmetric $(71, 35, 17)$ designs constructed in [6] and [7], and the Hadamard design obtained via a cyclic difference set described in [10]. As far as we know these are the only Hadamard 2-$(71, 35, 17)$ designs explicitly constructed up to now. The constructed codes are self-dual, doubly-even and self-complementary. Self-dual doubly-even binary codes of length 72 have been extensively studied (see [2, 3, 19]), since 72 is the smallest length of the code for which it is not known if there is an extremal doubly-even self-dual code. Nevertheless, as far as we know, this is the first study of PD-sets in these codes. We have also determined the number of minimal words of constructed codes of weight up to 16. Further, we discuss the error-correcting capability of the obtained codes by majority logic decoding. In addition, we describe a construction of a 3-$(72, 12, 11)$ design and a 3-$(72, 16, 2010)$ design from one of the constructed $[72, 36, 12]$ codes, and a construction of a strongly regular graph with parameters $(126, 25, 8, 4)$ from a binary $[35, 8, 4]$ code related to a 2-$(35, 17, 16)$ design, a derived design of a symmetric $(71, 35, 17)$ design.

2. Codes constructed from Hadamard matrices of order 72

The following statements can be found in [23, Theorem 1.98]:

Theorem 4. *Assume that $\mathcal{D}$ is a 2-(v, k, λ) design with block intersection numbers $s_1, s_2, \ldots, s_m$. Denote by C the binary code spanned by the block-by-point incidence matrix of $\mathcal{D}$. Then the following properties hold:*

1. *If $k, s_1, s_2, \ldots, s_m$ are all even, then C is self-orthogonal.*
2. *If $v, k, s_1, s_2, \ldots, s_m$ are all even, then C is contained in a length v self-dual code.*
3. *If $v \equiv 0 \pmod 8$, $k \equiv 0 \pmod 4$, and $s_1, s_2, \ldots, s_m$ are all even, then C is contained in a doubly-even self-dual code of length v.*
4. *The dual code $C^\perp$ has minimum distance $d^\perp \geq \dfrac{r + \lambda}{\lambda}$.*

Lemma 1. *Let C be the binary code of a Hadamard matrix of order 72. Then C is a self-orthogonal doubly-even code. Moreover, C is a self-complementary code.*

Proof. Two blocks of a 3-$(72, 36, 17)$ design intersect in 18 or 0 points. Properties from Theorem 4 hold for every code of a Hadamard matrix of order 72, so these codes are self-orthogonal linear codes. Further, for each block of a Hadamard 3-design its complement is also a block of a design, hence the binary code of a Hadamard matrix is self-complementary. □

Remark 1. *All of the codes obtained in this article are* $[72, 36]$ *linear codes. Since they are self-orthogonal, they are self-dual.*

Hadamard designs $\mathcal{D}_1, \ldots, \mathcal{D}_{45}$ described in [7], Hadamard designs described in [6], which will be denoted by $\mathcal{D}_{46}, \ldots, \mathcal{D}_{53}$ and Hadamard design obtained via a cyclic difference set described in [10], which will be denoted by $\mathcal{D}_{54}$, give rise to 24 inequivalent Hadamard matrices, that produce 12 inequivalent binary codes denoted by $C_1, \ldots, C_{12}$:

- C_1 constructed from $\mathcal{D}_1, \mathcal{D}_2$, $\mathcal{D}_3, \mathcal{D}_4$, $\mathcal{D}_5, \mathcal{D}_6$, $\mathcal{D}_9, \mathcal{D}_{10}$, $\mathcal{D}_{31}, \mathcal{D}_{32}$, $\mathcal{D}_{33}$, $\mathcal{D}_{34}$, $\mathcal{D}_{35}$, $\mathcal{D}_{36}$, $\mathcal{D}_{37}$ and $\mathcal{D}_{38}$,
- C_2 constructed from $\mathcal{D}_7, \mathcal{D}_8, \mathcal{D}_{11}, \mathcal{D}_{13}, \mathcal{D}_{39}, \mathcal{D}_{40}, \mathcal{D}_{41}$ and $\mathcal{D}_{42}$,
- C_3 constructed from $\mathcal{D}_{12}, \mathcal{D}_{43}, \mathcal{D}_{46}, \mathcal{D}_{47}, \mathcal{D}_{48}$ and $\mathcal{D}_{49}$,
- C_4 constructed from $\mathcal{D}_{14}, \mathcal{D}_{15}, \mathcal{D}_{44}$ and $\mathcal{D}_{45}$,
- C_5 constructed from $\mathcal{D}_{16}, \mathcal{D}_{17}, \mathcal{D}_{18}, \mathcal{D}_{19}, \mathcal{D}_{20}, \mathcal{D}_{21}, \mathcal{D}_{22}$ and $\mathcal{D}_{23}$,
- C_6 constructed from $\mathcal{D}_{24}, \mathcal{D}_{25}, \mathcal{D}_{26}$ and $\mathcal{D}_{27}$,
- C_7 constructed from $\mathcal{D}_{28}$,
- C_8 constructed from $\mathcal{D}_{29}$ and $\mathcal{D}_{30}$,
- C_9 constructed from $\mathcal{D}_{50}$ and $\mathcal{D}_{51}$,
- C_{10} constructed from $\mathcal{D}_{52}$,
- C_{11} constructed from $\mathcal{D}_{53}$,
- C_{12} constructed from $\mathcal{D}_{54}$.

In Table 1, we give parameters of the codes $C_1,\ldots,C_{12}$, and their weight enumerators written in the form

$$\begin{aligned} A(x) = x^0 &+ \alpha_1 x^4 + \alpha_2 x^8 + \alpha_3 x^{12} + \alpha_4 x^{16} + \alpha_5 x^{20} + \alpha_6 x^{24} + \alpha_7 x^{28} + \alpha_8 x^{32} + \alpha_9 x^{36} \\ &+ \alpha_8 x^{40} + \alpha_7 x^{44} + \alpha_6 x^{48} + \alpha_5 x^{52} + \alpha_4 x^{56} + \alpha_3 x^{60} + \alpha_2 x^{64} + \alpha_1 x^{68} + x^{72}. \end{aligned}$$

Using Theorem 2, for these codes we found the number of minimal words of weight 8, 12 and 16. These numbers are listed in Table 2.

In Table 3, orders of automorphism groups are listed for codes $C_1, \ldots, C_{12}$, and information about the structure of the automorphism group is given for codes C_4, C_{10}, C_{11} and C_{12}. For other codes we were not able to establish the structure of their automorphism groups, due to the size of groups.

Automorphism groups of codes C_1 and C_2 are mutually isomorphic, and so are automorphism groups of C_5 and C_6. In the structure of the automorphism group of the code C_4, H_2 is a Sylow 2-subgroup of the full automorphism group.

We found PD-sets for codes C_1, C_2, C_3, C_4, C_5, C_6, C_7, C_8, C_9, C_{10} and C_{12}. In Table 4, we list Gordon bounds for PD-sets for these codes and sizes of PD-sets found in these codes.

	Parameters	α_1	α_2	α_3	α_4
C_1	$[72, 36, 4]$	18	425	13328	745892
C_2	$[72, 36, 4]$	18	153	10608	590580
C_3	$[72, 36, 4]$	630	58905	1947792	30260340
C_4	$[72, 36, 4]$	18	153	13872	551412
C_5	$[72, 36, 8]$	0	289	6256	374476
C_6	$[72, 36, 8]$	0	153	4896	296820
C_7	$[72, 36, 4]$	306	29529	973488	15131700
C_8	$[72, 36, 8]$	0	153	6528	277236
C_9	$[72, 36, 4]$	42	777	29904	1273284
C_{10}	$[72, 36, 8]$	0	28	1078	256261
C_{11}	$[72, 36, 12]$	0	0	462	244305
C_{12}	$[72, 36, 12]$	0	0	2982	214065

	α_5	α_6	α_7	α_8	α_9
C_1	25862712	495169812	4324680048	16466504606	26093523052
C_2	26505720	495846276	4315865616	16489380078	26063078636
C_3	254186856	1251677700	3796297200	7307872110	43434873668
C_4	26721144	495128196	4317481296	16486794990	26066094572
C_5	17645664	461503692	4408373904	16575744838	25792178496
C_6	17967168	461841924	4403966688	16587182574	25776956288
C_7	131807736	839757636	4144182480	11996428590	34462853804
C_8	18074880	461482884	4404774528	16585890030	25778464256
C_9	36774360	538436724	4221311664	16302189246	26519444732
C_{10}	18093180	462717759	4398644778	16599729055	25760592456
C_{11}	18137196	462861315	4397571090	16602349995	25757148008
C_{12}	18303516	462306915	4398818490	16600354155	25759476488

Table 1: *Parameters and weight enumerators of codes* $C_1, \ldots, C_{12}$

	8	12	16
C_1	272	8704	596224
C_2	0	9792	470016
C_3	0	0	0
C_4	0	13056	391680
C_5	289	6256	353600
C_6	153	4896	293760
C_7	0	0	0
C_8	153	6528	274176
C_9	224	17472	740352
C_{10}	28	1078	255967
C_{11}	0	462	244305
C_{12}	0	2982	214065

Table 2: *The number of minimal words of weights 8, 12 and 16 in codes* $C_1, \ldots, C_{12}$

Code	Automorphism group	Order of the automorphism group
C_1		$17 \cdot 2^{38}$
C_2		$17 \cdot 2^{38}$
C_3		$31 \cdot 29 \cdot 23 \cdot 19 \cdot 17^2 \cdot 13^2 \cdot 11^3 \cdot 7^5 \cdot 5^8 \cdot 3^{17} \cdot 2^{69}$
C_4	$\mathbb{Z}_{17} \times \mathbb{Z}_9 \times H_2$	$17 \cdot 3^2 \cdot 2^{41}$
C_5		$17 \cdot 2^{20}$
C_6		$17 \cdot 2^{20}$
C_7		$17^2 \cdot 13^2 \cdot 11^2 \cdot 7^4 \cdot 5^6 \cdot 3^{16} \cdot 2^{67}$
C_8		$17 \cdot 3^2 \cdot 2^{23}$
C_9		$7^2 \cdot 5 \cdot 3^3 \cdot 2^{46}$
C_{10}	$Frob_{21} : (\mathbb{Z}_4 : \mathbb{Z}_2)$	168
C_{11}	$\mathbb{Z}_{35} : (\mathbb{Z}_6 \times \mathbb{Z}_4)$	840
C_{12}	$L(2, 71)$	$71 \cdot 7 \cdot 5 \cdot 3^2 \cdot 2^3$

Table 3: *Automorphism groups for codes $C_1, \ldots, C_{12}$*

Code	Gordon bound	Size of the found PD-set
C_1	2	3
C_2	2	3
C_3	2	3
C_4	2	3
C_5	14	42
C_6	14	41
C_7	2	3
C_8	14	38
C_9	2	2
C_{10}	14	54
C_{12}	62	402

Table 4: *Sizes of found PD-sets for codes C_1, C_2, C_3, C_4, C_5, C_6, C_7, C_8, C_9, C_{10} and C_{12}*

Remark 2. *The most interesting codes described in this paper are the* $[72, 36, 12]$ *codes C_{11} and C_{12}, especially the code C_{12} that admits a simple automorphism group $L(2, 71)$. Binary doubly-even self-dual* $[72, 36, 12]$ *codes have been studied in [2]. In that paper, Bouyukliev, Fack and Winne described* $[72, 36, 12]$ *codes constructed from 7238 Hadamard matrices of order 36. They obtained 522 inequivalent doubly-even self-dual* $[72, 36, 12]$ *codes and listed their weight distributions. Comparing the weight distributions of codes C_{11} and C_{12} with weight distributions listed in [2] we conclude that C_{11} and C_{12} are not equivalent to the* $[72, 36, 12]$ *codes studied by Bouyukliev, Fack and Winne. In Section 5, we describe a construction of 3-designs from the code C_{12}.*

In the next section, we discuss decoding of codes $C_1, \ldots, C_{12}$ by another decoding algorithm, majority logic decoding, which is suitable for decoding linear codes whose dual codes support the blocks of a t-design.

3. Majority logic decoding

A linear code whose dual code supports the blocks of a t-design admits one of the simplest decoding algorithms, majority logic decoding (see [21] and [23]). If a codeword $x = (x_1, \dots, x_n) \in C$ is sent over a communication channel and a vector $y = (y_1, \dots, y_n)$ is received, for each symbol y_i a set of values $y_i^{(1)}, \dots, y_i^{(r_i)}$ of r_i linear functions defined by the blocks of the design are computed, and y_i is decoded as the most frequent among the values $y_i^{(1)}, \dots, y_i^{(r_i)}$. The following result has been obtained by Rudolph [21].

Theorem 5. *If C is a linear $[n, k]$ code such that $C^{\perp}$ contains a set S of vectors of weight w whose supports are the blocks of a 2-(n, w, λ) design, the code C can correct up to*

$$e = \left\lfloor \frac{r + \lambda - 1}{2\lambda} \right\rfloor$$

errors by majority logic decoding, where $r = \lambda \dfrac{n-1}{w-1}$.

Rahman and Blake [20] improved the Rudolph's bound in the case when $C^{\perp}$ supports a t-design with $t \geq 2$.

Theorem 6. *Assume that the dual code of a linear code C supports a t-(n, w, λ) design $\mathcal{D}$, where $t \geq 2$. Let*

$$A_l = \sum_{j=0}^{l-1} (-1)^j \binom{l-1}{j} \lambda_{j+2},$$

where

$$\lambda_i = \lambda \binom{n-i}{t-i} / \binom{w-i}{t-i}, \quad (0 \leq i \leq t),$$

is the number of blocks of $\mathcal{D}$ containing a set of i fixed points. Define further

$$A'_l = \begin{cases} A_l, & \text{if } l \leq t-1, \\ A_{t-1}, & \text{if } l > t-1. \end{cases}$$

Then C can correct up to l errors by majority logic decoding, where l is the largest integer that satisfies the inequality

$$\sum_{i=1}^{l} A'_i \leq \lfloor (\lambda_1 + A'_l - 1)/2 \rfloor.$$

An easy way to construct a p-ary code whose dual code supports a design is to start with a t-design $\mathcal{D}$, and consider the dual code of the code spanned by the block-by-point incidence matrix of $\mathcal{D}$. We are interested in finding the error-correcting capability of codes $C_1, \dots, C_{12}$ by majority logic decoding.

Theorem 7. *Let H be a Hadamard matrix of order m, where $m \geq 4$, and $C_p(H)$ be the p-ary code of the matrix H. Then $C_p(H)^{\perp}$, the dual code of $C_p(H)$, can correct up to one error by majority logic decoding.*

Proof. $C_p(H)$ is the p-ary code associated with a 3-$(m, \frac{1}{2}m, \frac{1}{4}m-1)$ design defined by H. This 3-design is also a 2-$(m, \frac{1}{2}m, \frac{1}{2}m-1)$ design with $r = \lambda_1 = m-1$. One can easily verify that

$$e = \lfloor (r + \lambda_2 - 1)/2\lambda_2 \rfloor = 1.$$

By Theorem 5 the code $C_p(H)^{\perp}$ can correct up to one error by majority logic decoding. □

The following statement is a direct consequence of Theorem 7.

Corollary 1. *Let H be a Hadamard matrix of order m, where $m \geq 4$, and $C_p(H)$ the p-ary code of the matrix H. If $C_p(H)$ is self-dual, then it can correct up to one error by majority logic decoding.*

We conclude that codes $C_1, \ldots, C_{12}$ can correct one error by majority logic decoding. Note that this is the full error-correcting capability of the codes C_1, C_2, C_3, C_4, C_7 and C_9, while the codes C_5, C_6, C_8, C_{10}, C_{11} and C_{12} can correct up to three or five errors.

4. Construction of strongly regular graphs

In this section we describe a construction of some strongly regular graphs from codes that are related to Hadamard $(71, 35, 17)$ designs and their derived and residual designs. From the 54 Hadamard $(71, 35, 17)$ designs we obtain up to isomorphism 261 derived designs with parameters 2-$(35, 17, 16)$, and 302 residual 2-$(36, 18, 17)$ designs.

The derived designs produce 26 linear codes with parameters

$[35, 35, 1], [35, 33, 1], [35, 31, 1], [35, 27, 1], [35, 19, 1], [35, 30, 1], [35, 25, 1]$ and $[35, 26, 1]$,

and their dual codes with parameters

$[35, 0, 5], [35, 2, 8], [35, 4, 4], [35, 2, 4], [35, 8, 4], [35, 16, 4], [35, 8, 12], [35, 2, 16], [35, 5, 4],$
$[35, 1, 12], [35, 2, 8], [35, 1, 16], [35, 1, 8], [35, 10, 4], [35, 9, 4], [35, 2, 12], [35, 4, 8],$
$[35, 4, 12]$ and $[35, 5, 12]$.

The residual designs generate 23 linear codes with parameters

$[36, 35, 2], [36, 33, 2], [36, 31, 2], [36, 27, 2], [36, 19, 2], [36, 30, 2], [36, 34, 2], [36, 25, 2]$
and $[36, 26, 2]$,

and their dual codes with parameters

$[36, 1, 36], [36, 3, 4], [36, 5, 4], [36, 9, 4], [36, 17, 4], [36, 9, 12], [36, 3, 4], [36, 6, 4], [36, 2, 8],$
$[36, 3, 8], [36, 2, 16], [36, 2, 12], [36, 11, 4], [36, 10, 4], [36, 3, 12], [36, 5, 12]$ and $[36, 6, 12]$.

The support design of a code of length n for a given nonzero weight ω is the design with points the n coordinate indices and blocks the supports of all codewords of weight ω.

Let K_1 be the linear code with parameters $[35, 8, 4]$ with weight distribution

$$A(x) = x^0 + 36x^4 + 126x^8 + 84x^{12} + 9x^{16}.$$

This code is the dual code of the $[35, 27, 1]$ linear code obtained from a derived design. Let $\mathcal{S}_1$ be the support design of the code K_1 for the weight 8. The design $\mathcal{S}_1$ has 72 points and 126 blocks, and any two blocks intersect in 0, 2, 4 or 6 points. Let us define the graph $\mathcal{G}_1$ whose vertices are blocks of the design $\mathcal{S}_1$, two vertices being adjacent if and only if corresponding blocks intersect in 0 or 6 points. The graph $\mathcal{G}_1$ is a strongly regular graph with parameters $(126, 25, 8, 4)$ having the symmetric group S_{10} as the full automorphism group. This strongly regular graph has been previously known (see [4]), and it can be constructed from Johnson scheme $J(9, 4)$, where two quadruples are adjacent if and only if they have either zero or three points in common.

Let K_2 be a linear code with parameters $[36, 9, 4]$ with weight distribution

$$A(x) = x^0 + 36x^4 + 126x^8 + 84x^{12} + 9x^{16} + 9x^{20} + 84x^{24} + 126x^{28} + 36x^{32} + x^{36}.$$

This code is a dual code of the $[36, 27, 2]$ linear code obtained from residual designs. Let $\mathcal{S}_2$ be the support design of the code K_2 for the weight 8. That design has 126 blocks, and any two blocks intersect in 0, 2, 4 or 6 points. Define the graph $\mathcal{G}_2$ with 126 vertices, two vertices being adjacent if and only if corresponding blocks intersect in 6 points, or if they are disjoint. That graph is isomorphic to the graph $\mathcal{G}_1$.

Beside the strongly regular graph with parameters $(126, 25, 8, 4)$, we have constructed several triangular graphs from the codes studied in this paper.

From the support design of the code C_2 for weight 8 we obtain a strongly regular graph with parameters $(153, 32, 16, 4)$, i.e. the triangular graph $\binom{18}{2}$. From the code C_3 for weight 4 we get a strongly regular graph with parameters $(630, 68, 34, 4)$, i.e. the triangular graph $\binom{36}{2}$.

Support designs of dual codes of codes obtained from derived and residual designs led us to strongly regular graphs with parameters $(136, 30, 15, 4)$, $(28, 12, 6, 4)$ and $(36, 14, 7, 4)$, i.e. triangular graphs $\binom{17}{2}$, $\binom{8}{2}$ and $\binom{9}{2}$.

5. Construction of 3-designs

We have already pointed out that the $[72, 36, 12]$ code C_{12} admitting the simple automorphism group $L(2, 71)$ is the most interesting of the twelve $[72, 36]$ codes described in this paper. This code possesses one more interesting property, its codewords of weight 12 and 16 support 3-designs. The support design of the code C_{12} for weight 12 is a 3-design with parameters 3-$(72, 12, 11)$, having the full automorphism group of order 178920, isomorphic to the linear group $L(2, 71)$. The support design of C_{12} for weight 16 is a 3-design with parameters 3-$(72, 16, 2010)$, having the full automorphism group isomorphic to $L(2, 71)$. Cameron, Maimani, Omidi and Tayfeh-Rezaie [5] determined all 3-designs admitting an automorphism group isomorphic to $L(2, q)$ with block size not congruent to 0 and 1 modulo p, where $q = p^n$ is a prime power congruent to 3 modulo 4. However, a construction of a 3-$(72, 12, 11)$ design and a 3-$(72, 16, 2010)$ design from a code have not been described so far.

Symmetric $(71, 35, 17)$ designs used for the construction of codes, as well as their derived and residual designs, can be found at

`http://www.math.uniri.hr/~sanjar/structures/`.

Codes K_1 and K_2 are related to the symmetric $(71, 35, 17)$ design $\mathcal{D}_{43}$ from [7], that can also be found on the web site given above.

Acknowledgement

The authors would like to thank the referees for their helpful suggestions.

References

[1] E. F. Assmus Jnr, J. D. Key, *Designs and their codes*, Cambridge University Press, Cambridge, 1992.

[2] I. Bouyukliev, V. Fack, J. Winne, *Hadamard matrices of order 36 and double-even self-dual* $[72, 36, 12]$ *codes*, in: *Proceedings of EuroComb 2005*, Technische Universität Berlin, 2005, 93–98.

[3] S. Bouyuklieva, E. A. O'Brien, W. Willems, *The automorphism group of a self-dual doubly-even* $[72, 36, 16]$ *code is solvable*, IEEE Trans. Inform. Theory **52**(2006), 4244–4248.

[4] A. E. Brouwer, *Strongly Regular Graphs*, in: *Handbook of combinatorial designs, 2nd ed.*, (C. J. Colbourn and J. H. Dinitz, Eds.), Chapman and Hall/CRC, 2007, 852–868.

[5] P. J. Cameron, H. R. Maimani, G. R. Omidi, B. Tayfeh-Rezaie, *3-designs from* $PSL(2, q)$, Discrete Math. **306**(2006), 3063–3073.

[6] D. Crnković, D. Held, *Some Hadamard designs with parameters* $(71, 35, 17)$, J. Combin. Des. **10**(2001), 144–149.

[7] D. Crnković, S. Rukavina, *On symmetric* $(71, 35, 17)$ *designs*, Math. Maced. **2**(2004), 51–58.

[8] D. M. Gordon, *Minimal permutation sets for decoding the binary Golay codes*, IEEE Trans. Inform. Theory **28**(1982), 541–543.

[9] W. C. Huffman, *Codes and groups*, in: *Handbook of Coding Theory, Vol. 2*, (V. S. Pless and W. C. Huffman, Eds.), Elsevier, 1998, 1345–1440.

[10] D. Jungnickel, A. Pot, K. W. Smith, *Difference sets*, in: *Handbook of combinatorial designs, 2nd ed.*, (C. J. Colbourn and J. H. Dinitz, Eds.), Chapman and Hall/CRC, 2007, 419–435.

[11] J. D. Key, *Permutation decoding for codes from designs, finite geometries and graphs*, in: *Information Security, Coding Theory and Related Combinatorics*, (D. Crnković and V. Tonchev, Eds.), IOS Press, 2011, 172–201.

[12] J. D. Key, J. Moori, and B. G. Rodrigues, *Permutation decoding for binary codes from triangular graphs*, European J. Combin. **25** (2004), 113–123.

[13] H.-J. Kroll, R. Vincenti, *PD-sets for binary RM-codes and the codes related to the Klein quadric and to the Schubert variety of PG(5,2)*, Discrete Math. **308**(2008), 408–414.

[14] K. Lüders-Jensen, T. Jakobsen, *Bounds on minimal codewords in linear codes*, 1994, avaliable at `http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.55.2489)`.

[15] F. J. MacWilliams, *Permutation decoding of systematic codes*, Bell System Tech. J. **43**(1964), 485–505.

[16] F. J. MacWilliams, N. J. A. Sloane, *The theory of error-correcting codes*, North-Holland, Amsterdam, 1983.

[17] J. Massey, *Minimal codewords and secret sharing*, in: *Proceedings of the sixth joint Swedish-Russian workshop on information theory*, Molle, Sweden, 1993, 246–249.

[18] G. Nebe, E. M. Rains, N. J. A. Sloane, *Self-dual codes and invariant theory, Algorithms and Computation in Mathematics, Vol. 17*, Springer, Berlin, 2006.

[19] E. A. O'Brien, W. Willems, *On the automorphism group of a binary self-dual doubly-even [72,36,16] code*, IEEE Trans. Inform. Theory **57**(2011), 4445–4451.

[20] M. Rahman, I. F. Blake, *Majority logic decoding using combinatorial designs*, IEEE Trans. Inform. Theory **21**(1975), 585–587.

[21] L. D. Rudolph, *A class of majority logic decodable codes*, IEEE Trans. Inform. Theory **13**(1967), 305–307.

[22] L. M. G. M. Tolhuizen, W. J. van Gils, *A large automorphism group decreases the number of computations in the construction of an optimal encoder/decoder pair for a linear block code*, IEEE Trans. Inform. Theory **34**(1988), 333–338.

[23] V. D. Tonchev, *Codes*, in: *Handbook of combinatorial designs, 2nd ed.*, (C. J. Colbourn and J. H. Dinitz, Eds.), Chapman and Hall/CRC, 2007, 667–702.