On extremal ternary self-dual codes of length 36 and related symmetric 2-$(36, 15, 6)$ designs

joint work with Vladimir D. Tonchev, Michigan Technological University, Houghton, USA

Sanja Rukavina
sanjar@math.uniri.hr

Faculty of Mathematics
University of Rijeka, Croatia

ALCOCRYPT - ALgebraic and combinatorial methods for COding and CRYPTography

February 21, 2023, CIRM, Luminy

Extremal ternary self-dual codes and t-designs

- The minimum distance, or equivalently, the minimum weight d of a ternary self-dual code of length n divisible by 12 satisfies the upper bound $d \leq n/4 + 3$, and a self-dual ternary code with minimum distance $d = n/4 + 3$ is called *extremal*.
- An incidence structure $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$, with point set $\mathcal{P}$, block set $\mathcal{B}$ and incidence $\mathcal{I}$ is a t-(v, k, λ) design, if $|\mathcal{P}| = v$, every block $B \in \mathcal{B}$ is incident with precisely k points, and every t distinct points are together incident with precisely λ blocks. A design is called symmetric if it has same number of points and blocks.
- If C is an extremal ternary self-dual code of length $n \equiv 0 (mod 12)$, then the supports of all codewords of any nonzero weight $w < n$ are the blocks of a 5-design[1].

[1] E. F. Assmus, Jr., H. F. Mattson, Jr., New 5-designs, J. Combin. Theory, Ser. A 6 (1969), 122-151.

Known examples

Ternary extremal self-dual codes are known for the following lengths $n \equiv 0 (mod 12)$:

n	# of codes	
12	1	extended Golay code
24	2	extended QR code, Pless SC
36	≥ 1	Pless SC
48	≥ 2	extended QR code, Pless SC
60	≥ 3	extended QR code, Pless SC, code by Nebe and Villar

Pless, V.: On a new family of symmetry codes and related new five-designs. Bull. Amer. Math. Soc. **75**(6), 1339–1342 (1969)

Pless, V.: Symmetry codes over $GF(3)$ and new five-designs. J. Combin. Theory Ser. A **12**, 119–142 (1972)

Known examples

n	# of codes	.
12	1	extended Golay code
24	2	extended QR code, Pless SC
36	≥ 1	Pless SC
48	≥ 2	extended QR code, Pless SC
60	≥ 3	extended QR code, Pless SC, code by Nebe and Villar

Pless, V.: On a new family of symmetry codes and related new five-designs. Bull. Amer. Math. Soc. **75**(6), 1339–1342 (1969)

Pless, V.: Symmetry codes over $GF(3)$ and new five-designs. J. Combin. Theory Ser. A **12**, 119–142 (1972)

Seventh International Workshop on Optimal Codes and Related Topics
September 6-12, 2013, Albena, Bulgaria *pp. 158-163*

An analogue of the Pless symmetry codes

Gabriele Nebe nebe@math.rwth-aachen.de
Darwin Villar darwin.villar@rwth-aachen.de
Lehrstuhl D für Mathematik, RWTH Aachen University
52056 Aachen, Germany

Dedicated to the memory of Professor Stefan Dodunekov

Abstract. A series of monomial representations of $SL_2(p)$ is used to construct a new series of self-dual ternary codes of length $2(p+1)$ for all primes $p \equiv 5 \pmod 8$. In particular we find a new extremal self-dual ternary code of length 60.

1 Introduction

In 1969 Vera Pless [6] discovered a family of self-dual ternary codes $\mathcal{P}(p)$ of length $2(p+1)$ for primes p with $p \equiv -1 \pmod 6$. Together with the extended quadratic residue codes $XQR(q)$ of length $q+1$ (q prime, $q \equiv \pm 1 \pmod{12}$) they define a series of self-dual ternary codes of high minimum distance (see [3, Chapter 16, §8]). For $p = 5$, the Pless code $\mathcal{P}(5)$ coincides with the Golay code $\mathfrak{g}_{12}$ which is also the extended quadratic residue code $XQR(11)$ of length 12.

Using invariant theory of finite groups, A. Gleason [2] has shown that the minimum distance of a self-dual ternary code of length $4n$ cannot exceed $3\lfloor \frac{n}{12} \rfloor + 3$. Self-dual codes that achieve equality are called *extremal*. Both constructions, the Pless symmetry codes and the extended quadratic residue codes yield extremal ternary self-dual codes for small values of p.

$n = 36$

n	# of codes	·
12	1	extended Golay code
24	2	extended QR code, Pless SC
36	≥ 1	Pless symmetry code C(17)
48	≥ 2	extended QR code, Pless SC
60	≥ 3	extended QR code, Pless SC, code by Nebe and Villar

$n = 36$

n	# of codes	.
12	1	extended Golay code
24	2	extended QR code, Pless SC
36	≥ 1	Pless symmetry code C(17)
48	≥ 2	extended QR code, Pless SC
60	≥ 3	extended QR code, Pless SC, code by Nebe and Villar

It is known[2] that the Pless symmetry code $C(q)$ of length $n = 2q + 2$, where $q \equiv -1 \pmod 3$ is an odd prime power, contains a set of n codewords of weight n, which after replacing every entry equal to 2 by -1 form the rows of a Hadamard matrix equivalent to the Paley-Hadamard matrix of type II.

In particular, the Pless symmetry code $C(17)$ contains the rows of a Hadamard matrix P of Paley type II, having a full automorphism group of order $4 \cdot 17(17^2 - 1) = 19584$, and the rows of P span the code $C(17)$.

[2] V. Pless, Symmetry codes over $GF(3)$ and new five-designs, *J. Combin. Theory, Ser. A* **12** (1972), 119-142.

Recently, Tonchev showed[3] that the code $C(17)$ contains a second equivalence class of Hadamard matrices of order 36 having as rows codewords of $C(17)$.

- Any matrix H from the second equivalence class has a full automorphism group of order 72 and the rows of H span the code $C(17)$.
- In addition, H is monomially equivalent to a regular Hadamard matrix H', such that every row of H' has 15 entries equal to -1 and 21 entries equal to 1, thus H' has a constant row sum 6. The symmetric 2-$(36, 15, 6)$ design D with a $(0, 1)$-incidence obtained by replacing every entry 1 of H' with 0 and every entry -1 of H' with 1 has a trivial full automorphism group, and the row span of its incidence matrix over $GF(3)$ is equivalent to the Pless symmetry code $C(17)$.

$\Rightarrow$ Hadamard matrices derived from the symmetry code of length 36?

[3] V. D. Tonchev, On Pless symmetry codes, ternary QR codes, and related Hadamard matrices and designs, *Des. Codes Cryptogr.* 90 (2022) 2753-2762 doi.org/10.1007/s10623-021-00941-0.

- Huffman proved[4] that any extremal ternary self-dual code of length 36 that admits an automorphism of prime order $p > 3$ is monomially equivalent to the Pless symmetry code.
- More recently, Eisenbarth and Nebe extended Huffman's result[5] by proving that the Pless symmetry code is the unique (up to monomial equivalence) ternary extremal self-dual code of length 36 that admits an automorphism of order 3. In addition, it was proved in that if C is an extremal ternary self-dual code of length 36 then either C is equivalent to the Pless symmetry code or the full automorphism group of C is a subgroup of the cyclic group of order 8.

$\Rightarrow$ Symmetric 2-$(36, 15, 6)$ designs with an involution and their ternary codes?

[4] W. C. Huffman, On extremal self-dual ternary codes of lengths 28 to 40, *IEEE Trans. Info. Theory* **38** No. 4 (1992), 1395-1400.

[5] S. Eisenbarth, G. Nebe, Self-dual codes over chain rings, *Math. Comput. Sci.* **14** (2020), 443 - 456.

Journal of Algebraic Combinatorics
https://doi.org/10.1007/s10801-022-01206-2

Extremal ternary self-dual codes of length 36 and symmetric 2-(36, 15, 6) designs with an automorphism of order 2

Sanja Rukavina[1] · Vladimir D. Tonchev[2]

- Hadamard matrices[6] derived from the symmetry code of length 36
- Symmetric 2-$(36, 15, 6)$ designs with an involution and their ternary codes

[6] A Hadamard matrix of order n is an $n \times n$ matrix H of 1's and -1's such that $HH^T = nI_n$, where I_n is the identity matrix of order n. It follows that $n = 1, 2$, or $n = 4t$ for some integer $t \geq 1$.

Hadamard matrices derived from the symmetry code of length 36

- The code $C(17)$ contains exactly 888 codewords of weight 36. In what follows, we denote by U the set of all 888 codewords in $C(17)$ of full weight. The 3-rank (that is, the rank over the finite field of order 3, $GF(3)$) of the matrix having as rows the codewords from U is 18, hence U spans $C(17)$. In the context of Hadamard matrices, we view the codewords from U as vectors with components ± 1.
- We consider Hadamard matrices of order 36 whose rows are obtained from codewords of full weight 36 in the ternary Pless symmetry code $C(17)$ after replacing all codeword entries that are equal to 2 with -1.

Lemma

A set S of 36 codewords from U is the row set of a Hadamard matrix of order 36 if and only if the Hamming distance between every two codewords from S is 18.

Lemma

If H is a Hadamard matrix whose rows are codewords from U then the row set of any normalized Hadamard matrix obtained from H belongs to a code which is monomially equivalent to $C(17)$.

The set U of the Pless symmetry code $C(17)$[7,8], does not contain the all-one codeword $\bar{1} = (1, \ldots, 1)$, while it contains a codeword v with one entry equal to -1, located in the code coordinate labeled by ∞, and 35 entries equal to 1.

[7] V. Pless, On a new family of symmetry codes and related new five-designs, *Bull. Amer. Math. Soc.* **75**, No. 6 (1969), 1339-1342.

[8] V. Pless, Symmetry codes over $GF(3)$ and new five-designs, *J. Combin. Theory, Ser. A* **12** (1972), 119-142.

Negating (that is, multiplying by 2 (mod 3)) the code coordinate of $C(17)$ labeled by ∞ transforms the symmetry code $C(17)$ into a monomially equivalent code $L(17)$ which does contain the all-one vector $\bar{1}$ [9].

$\#x$	$(w_1(x), w_2(x))$
1	(0,36)
408	(15,21)
70	(18,18)
408	(21,15)
1	(36,0)

If $x \in L(17)$ is a codeword of full weight 36, we denote by $w_i(x)$ the number of entries of x that are equal to i $(i = 1, 2)$.

[9] V. D. Tonchev, On Pless symmetry codes, ternary QR codes, and related Hadamard matrices and designs, *Des. Codes Cryptogr.* 90 (2022) 2753-2762 doi.org/10.1007/s10623-021-00941-0.

All inequivalent Hadamard matrices of order 36 whose rows are obtained from codewords in $L(17)$ of weight 36 can be enumerated as follows.

- We consider W as an 888×36 matrix, and for every integer i, $1 \leq i \leq 888$, we define a matrix W_i, being the matrix obtained by negating all columns of W which have entry -1 in row i. Thus, the ith row of W_i is the all-one vector $\bar{1}$, and this row must be a row of every normalized Hadamard matrix consisting of rows of W_i. We refer to W_i as a matrix obtained by switching of W with respect to row i.
- To reduce the search further, we consider only normalized Hadamard matrices with first column being the all-one column.

- We define a graph Γ_i having as vertices all rows of W_i with first entry 1 and exactly 18 entries equal to 1, where two vertices are adjacent in Γ_i if and only if the Hamming distance between the corresponding rows of W_i is 18.

Lemma

(a) Any set of 35 rows of W_i that corresponds to a clique of size 35 in Γ_i, together with the all-one row $\bar{1}$, is the set of rows of a normalized Hadamard matrix.
(b) The maximum clique size in Γ_i is 35.

One can compute representatives of the equivalence classes of Hadamard matrices by an examination of the 35-cliques in the graphs Γ_i, $1 \leq i \leq 888$. Since every codeword $x \in W$ with weight structure $(w_1(x), w_2(x)) = (21, 15)$ is the negative of the codeword $2x \in W$ with weight structure $(15, 21)$, it is sufficient to examine the graphs Γ_i such that the weight structure of the ith row of W is $(15, 21)$ or $(18, 18)$.

The incidence structure with $(0,1)$-incidence matrix obtained from W by replacing all entries that are equal to 2 with zero, has full automorphism group G of order 272. The group G partitions the set of 408 rows of W with weight structure $(15,21)$ into four orbits of lengths 68, 68, 136, 136, and the set of 70 rows with weight structure $(18,18)$ into four orbits of lengths 2, 17, 17, 34. Therefore, it is sufficient to examine eight switchings of W, one for each orbit, all together.

$\#x$	$(w_1(x), w_2(x))$
1	(0,36)
93	(12,24)
36	(15,21)
628	(18,18)
36	(21,15)
93	(24,12)
1	(36,0)

An examination of the matrices W_i obtained by switching of W with respect to any of the 408 rows having weight structure $(15,21)$ shows that any such matrix has a complete weight distribution given in the table for W_{408}, where W_{408} is obtained by the switching of W with respect to row no. 408.

$\#x$	$(w_1(x), w_2(x))$
1	(0,36)
93	(12,24)
36	(15,21)
628	(18,18)
36	(21,15)
93	(24,12)
1	(36,0)

Theorem

(a) The 36 codewords of W_{408} with weight structure $(15, 21)$ form a regular Hadamard matrix H which is monomially equivalent to the Paley-Hadamard matrix of type II.
(b) The symmetric 2-$(36, 15, 6)$ design D associated with H has a full automorphism group of order 24.
(c) The incidence matrix of D has 3-rank 18, and its linear span over $GF(3)$ is a code equivalent to the Pless symmetry code $C(17)$.

Every row of the regular Hadamard matrix H from Theorem contains 15 entries equal to 1 and 21 entries equal to -1. A $(0, 1)$-incidence matrix A of the associated symmetric 2-$(36, 15, 6)$ design D is obtained by adding the all-one codeword $\bar{1}$ to every row of H, followed by a multiplication of all rows by 2 (mod 3). Hence, the ternary code spanned by the rows of H contains also the rows of A.

Symmetric 2-$(36, 15, 6)$ designs with an involution and their ternary codes

- Huffman proved[10] that any extremal ternary self-dual code of length 36 that admits an automorphism of prime order $p > 3$ is monomially equivalent to the Pless symmetry code.
- More recently, Eisenbarth and Nebe extended Huffman's result[11] by proving that the Pless symmetry code is the unique (up to monomial equivalence) ternary extremal self-dual code of length 36 that admits an automorphism of order 3. In addition, it was proved in that if C is an extremal ternary self-dual code of length 36 then either C is equivalent to the Pless symmetry code or the full automorphism group of C is a subgroup of the cyclic group of order 8.

$\Rightarrow$ Symmetric 2-$(36, 15, 6)$ designs with an involution and their ternary codes?

[10] W. C. Huffman, On extremal self-dual ternary codes of lengths 28 to 40, *IEEE Trans. Info. Theory* **38** No. 4 (1992), 1395-1400.

[11] S. Eisenbarth, G. Nebe, Self-dual codes over chain rings, *Math. Comput. Sci.* **14** (2020), 443 - 456.

- It is known that every finite group of order 2^n contains a subgroup of order 2^i for every i in the range $1 \leq i \leq n$. By this property, finding all nonisomorphic 2-$(36, 15, 6)$ designs which are invariant under an involution and whose incidence matrix spans a ternary extremal self-dual code, will also give the enumeration of all nonisomorphic 2-$(36, 15, 6)$ designs invariant under a nontrivial subgroup of the cyclic group of order 8 with this property.
- For the construction of 2-$(36, 15, 6)$ designs we use the method for constructing orbit matrices with presumed action of an automorphism group, which are then indexed to construct designs. After constructing 2-$(36, 15, 6)$ designs, we check the 3-rank of their incidence matrices, and if it is equal to 18 we determine the minimum weight of the corresponding ternary code.

Let $\mathcal{D} = (\mathcal{P}, \mathcal{B}, I)$ be a 2-(v, k, λ) design and $G \leq \mathrm{Aut}(\mathcal{D})$. We denote the $G-$orbits of points by $\mathcal{P}_1, \ldots, \mathcal{P}_m$, $G-$orbits of blocks by $\mathcal{B}_1, \ldots, \mathcal{B}_n$, and put $|\mathcal{P}_i| = \nu_i$, $|\mathcal{B}_j| = \beta_j$, $i = 1, \ldots, m$, $j = 1, \ldots, n$.

Denote by a_{ij} the number of blocks of $\mathcal{B}_j$ which are incident with a representative of the point orbit $\mathcal{P}_i$. The number a_{ij} does not depend on the choice of a point $P \in \mathcal{P}_i$, and the following equalities hold:

$$\sum_{j=1}^{n} a_{ij} = r \,, \tag{1}$$

$$\sum_{j=1}^{n} \frac{\nu_t}{\beta_j} a_{sj} \; a_{tj} = \lambda \nu_t + \delta_{st}(r - \lambda) \,. \tag{2}$$

Definition

A $(m \times n)$-matrix $M = (a_{ij})$ with entries satisfying conditions (1) and (2) is called a point orbit matrix for the parameters $2 - (v, k, \lambda)$ and orbit lengths distributions $(\nu_1, \ldots, \nu_m)$ and $(\beta_1, \ldots, \beta_n)$.

Example

Incidence matrix for the symmetric (7,3,1) design

$$\left(\begin{array}{c|ccc|ccc} 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ \hline 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ \hline 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 \end{array}\right)$$

Corresponding orbit matrix for Z_3

	1	3	3
1	0	3	0
3	1	1	1
3	0	1	2

The first step in the construction is to determine possible orbit lengths distributions. For that we need the following facts

- Suppose that a nonidentity automorphism σ of a symmetric 2-(v, k, λ) design fixes f points. Then

$$f \leq v - 2(k-\lambda) \qquad \text{and} \qquad f \leq (\frac{\lambda}{k-\sqrt{k-\lambda}})v.$$

  Moreover, if equality holds in either inequality, σ must be an involution and every non-fixed blosk contains exactly λ fixed points.[12]

- Suppose that $\mathcal{D}$ is a nontrivial symmetric 2-(v, k, λ) design, with an involution σfixing f points and blocks. If $f \neq 0$, then[13]

$$f \geq \begin{cases} 1+\frac{k}{\lambda}, & \text{if } k \text{ and } \lambda \text{ are both even,} \\ 1+\frac{k-1}{\lambda}, & \text{otherwise.} \end{cases}$$

$\Rightarrow$ An involution acting on 2-$(36, 15, 6)$ design could have f fixed points, where $f \in \{4, 6, 8, 10, 12, 14, 16, 18\}$, or acts fixed points freely.

---

[12] E. Lander, *Symmetric Designs: An Algebraic Approach*, Cambridge University Press, 1983., [Corolarry 3.7]

[13] E. Lander, *Symmetric Designs: An Algebraic Approach*, Cambridge University Press, 1983.[Proposition 4.23]

- There are 119907 orbit matrices for an involution acting on 2-$(36, 15, 6)$ design without fixed points, but none of the corresponding designs yields no self-dual ternary code.
- Orbit matrices do not exist for $f \in \{6, 14, 18\}$.
- The results for the remaining cases are summarized in the following table

Number of fixed points	4	8	10	12	16
Number of orbit matrices	12991	670	56	311	83
Number of designs	884139	498592	186369	3719232	209160
max d in self-dual codes	12	$\times$	$\times$	9	$\times$

Theorem

(a) Up to isomorphism, there exists exactly one symmetric 2-$(36, 15, 6)$ design D that admits an automorphism of order 2 and its incidence matrix spans an extremal ternary self-dual code of length 36.
(b) The full automorphism group G of D is of order 24, and G is isomorphic to the symmetric group S_4.
(c) The regular Hadamard matrix associated with D is equivalent to the Paley-Hadamard matrix of type II.
(d) The ternary code spanned by D is equivalent to the Pless symmetry code.

THANK YOU!