Ternary self-dual codes, Hadamard matrices and related designs

Vladimir D. Tonchev

Michigan Technological University

Joint work with Sanja Rukavina, University of Rijeka, Croatia

Linear codes

A *linear* $[n, k]$ code C over $GF(q)$ is a k-subspace of $GF(q)^n$.

The *support* $Sup(x)$ of a vector x is the set of indices of its nonzero components.

The Hamming *weight* of $x \in GF(q)^n$ is $w(x) = |Sup(x)|$.

An $[n, k, d]$ code C is an $[n, k]$ code with minimum weight d.

The *dual* code $C^\perp$ is an $[n, n-k]$ code being the orthogonal complement of C.

An $[n, k]$ code is *self-orthogonal* if $C \subseteq C^\perp$, and *self-dual* if $C = C^\perp$.

Combinatorial designs

A t-(v, k, λ) design D with a *point* set $X = \{x_i\}_{i=1}^{v}$ is a collection of k-subsets $\mathcal{B}$=$\{B_j\}_{j=1}^{b}$ called *blocks*, such that every t-subset of X is contained in exactly λ blocks.

The **incidence matrix** of D is a $b \times v$ $(0, 1)$-matrix $A = (a_{i,j})$, where $a_{i,j} = 1$ if $x_j \in B_i$ and $a_{i,j} = 0$ otherwise.

If $t = 2$ and $v > k > 0$ then $b \geq v$ (Fisher inequality).

A 2-(v, k, λ) design is **symmetric** if $b = v$, or equivalently, every two blocks share exactly λ points.

Ternary extremal self-dual codes

An upper bound (Mallows and Sloane 1973)

If C is a self-dual $[n, n/2, d]$ ternary code then

$$d \leq 3[\frac{n}{12}] + 3.$$

Definition

A ternary self-dual code of length n is **extremal** if it meets the upper bound: $d = 3[\frac{n}{12}] + 3$.

Theorem (Assmus and Mattson 1969)

If C is an extremal ternary self-dual code of length $n \equiv 0 \pmod{12}$ then the supports of all codewords of any nonzero weight $w < n$ are the blocks of a 5-design.

Extended QR codes and Pless symmetry codes

Theorem (Assmus and Mattson 1969)

The ternary extended quadratic residue codes $QR(n-1)^*$ of length $n = 12, 24, 48$ and 60 are extremal and support 5-designs.

Pless Symmetry Codes (Pless 1969)

- For every odd prime power $q \equiv -1 \pmod 3$ there is a ternary self-dual $[2q+2, q+1]$ code $C(q)$.
- The symmetry codes of length $n = 12, 24, 36, 48, 60$ $(q = 5, 11, 17, 23, 29)$ are extremal and support 5-designs.

Note

The 5-designs obtained from the extremal codes of length 24, 36, 48 and 60, were the only known 5-designs at that time, other than the 5-designs arising from the 5-transitive Mathieu groups M_{12} and M_{24}, which were known since the 1930's.

The known extremal ternary self-dual codes of length $n \equiv 0 \pmod{12}$

- $n = 12$: QR^*_{11} and $C(5)$ are equivalent to the Golay code G_{12}.
- $n = 24$: Extended $QR(23)^*$ code, Pless symmetry code $C(11)$.
- $n = 36$: Pless symmetry code $C(17)$.
- $n = 48$: QR^*_{47}, $C(23)$.
- $n = 60$: QR^*_{59}, $C(29)$, NV.

The code NV is a group theoretical analogue of the Pless symmetry code $C(29)$, found by G. Nebe and D. Villar in 2013.

Theorem

- Up to equivalence, G_{12} there is only extremal ternary self-dual code of length 12 (Pless 1968).
- There are exactly two inequivalent codes of length 24 (Leon, Pless, and Sloane 1981).

Hadamard matrices and designs

A **Hadamard matrix** of order n is an $n \times n$ matrix H of 1's and -1's such that $HH^T = nI$, where I is the identity matrix.
A *necessary* condition: if $n > 2$ then $n = 4t$ for some integer $t \geq 1$.

Theorem

If H is a Hadamard matrix of order $n = 4t$ being a multiple of a prime $p > 2$ then the row space of H is a self-orthogonal code over $GF(p)$.

An **automorphism** of a Hadamard matrix H is a pair of $\{0, 1, -1\}$-monomial matrices L, R such that $LHR = H$.

Two Hadamard matrices H_1, H_2 of the same order are **equivalent** if there are monomial matrices L, R such that $LH_1R = H_2$.

A Hadamard matrix H of order $n = 4t$ is **normalized** with respect to its ith row and jth column if all entries in row i and column j are equal to 1. Deleting the all-one ith row and jth column and replacing all -1's with 0's gives the incidence matrix of a symmetric 2-$(\mathbf{4t-1, 2t-1, t-1})$ design D called a **Hadamard 2-design.**
If H is a Hadamard matrix of order $n = 4t$ normalized with respect to a row, deleting the all-one row of H and the all -1-row of $-H$ in

$$\begin{pmatrix} H \\ -H \end{pmatrix}$$

and replacing all -1's with 0's gives the incidence matrix of a **Hadamard 3**-$(\mathbf{4t, 2t, t-1})$ design D^*.

A Hadamard matrix H of order $n = 4t$ is **regular** of degree $\underline{k}$ if every row of H contains exactly $\mathbf{k}$ $+1$'s.
Then necessarily $t = m^2$ for some integer m, $k = 2m^2 \pm m$, and replacing all -1's with zeros gives the incidence matrix of a symmetric 2-$(\mathbf{4m^2, 2m^2 \pm t, m^2 \pm m})$ design (called a **Menon** design).

Hadamard matrices of Paley type

Let $q = p^r$, where p is an odd prime, and let $Q = \{q_{i,j}\}$ be the $q \times q$ matrix with rows and columns labeled by the elements of $GF(q)$ and defined as follows:
$q_{ij} = 0$ if $i = j$, $q_{ij} = +1$ if $i - j$ is a nonzero square in $GF(q)$, and $q_{ij} = -1$ if $i - j$ is not a square in $GF(q)$.
Let $\bar{1} = (1, \ldots, 1)$ be the constant all-one vector with q components.
Let S be the $(q+1) \times (q+1)$ matrix defined by

$$S = \begin{bmatrix} 0 & \bar{1} \\ -\bar{1}^T & Q \end{bmatrix}.$$

The matrix S satisfies the equation

$$SS^T = qI_{q+1}.$$

A square $n \times n$ $\{0, 1, -1\}$-matrix with zero diagonal that satisfies the equation $SS^T = (n-1)I$ is called a **conference** matrix.

Theorem (Paley 1933)

1. If $q \equiv 3 \pmod 4$ then $H = I + S$ a Hadamard matrix of order $n = q + 1$.
2. If $q \equiv 1 \pmod 4$ then

$$H = \begin{bmatrix} S + I & S - I \\ S - I & -S - I \end{bmatrix}$$

is a Hadamard matrix of order $n = 2q + 2$.

These matrices are known as **Paley-Hadamard** matrices of **type I** and **type II** respectively.

Hadamard matrices in ternary QR codes

Theorem

- If $q \equiv 3 \pmod 4$ is a prime power, a quadratic residue (QR) code of length q is a code spanned by the incidence matrix A of a symmetric Hadamard 2-$(q, (q-1)/2, (q-3)/4)$ design associated with a **Paley-Hadamard matrix of type I.**
- The extended code is spanned by a matrix obtained by bordering A with the all-one column.
- If, in addition, $q \equiv -1 \pmod 3$, that is, $q = 12s + 11$, the ternary extended QR code is self-dual that contains a **Hadamard matrix** having as rows codewords of weight $q + 1$, equivalent to a **Paley-Hadamard matrix of type I.**

Symmetry codes and Hadamard matrices

Let q be an odd prime power such that $q \equiv -1 \pmod 3$.
The Pless **symmetry code** $C(q)$ is defined as a ternary self-dual code of length $n = 2q + 2$ with a generator matrix $G = (I, S)$.

Theorem (Pless 1972)

- The symmetry code $C(q)$ contains a **Hadamard matrix** H of order $n = 2q + 2$ whose rows are codewords of full weight $2q + 2$, after any entry equal to 2 is replaced by -1.
- H is equivalent to a **Paley Hadamard matrix of type II**.

The matrix H is normalized with respect to a row if if -1 is not a square in $GF(q)$, and contains a row R with $n - 1$ entries equal to 1 and one entry equal to -1 whenever -1 is a square in $GF(q)$. In the latter case, negating the column of H with entry -1 in row R gives a **normalized Hadamard matrix** with respect to row R, whose row space is a code $\mathbf{L}(\mathbf{q})$ which is equivalent to $\mathbf{C}(\mathbf{q})$ and contains the all-one vector.

The code $L(q)$

Theorem

- The code $L(q)$ contains the all-one vector $\bar{1} = (1, \ldots, 1)$.
- The code $L(q)$ contains a set of $4q + 2$ (0,1)-codewords of weight $q + 1$ that form the incidence matrix of a Hadamard 3-$(2q + 2, q + 1, (q - 1)/2)$ design $D(q)$.
- If $q = 5, 11, 17, 23$, the code $L(q)$ contains **exactly** $4q + 2$ (0,1)-codewords of weight $q + 1$, and every such codeword is the incidence vector of a block of the Hadamard 3-design $D(q)$.
- The code $L(q)$ is spanned by the incidence matrix of $D(q)$.

Hadamard matrices in ternary linear codes

Lemma 1

A set M of n codewords of weight n in a ternary linear self-orthogonal code of length $n \equiv 0 \pmod{12}$ is the set of rows of a Hadamard matrix of order n if and only if the Hamming distance between every two codewords from M is equal to $n/2$.

Corollary

if H is a Hadamard matrix of order n having as rows codewords in a ternary linear code C, the code contains at least 2^n distinct Hadamard matrices that are equivalent to H.

Lemma 2

If H is a Hadamard matrix whose rows are codewords in a ternary linear code C, then the set rows of any **normalized** Hadamard matrix obtained from H belongs to a code which is monomially equivalent to C.

Codewords of weight 36 in the code $L(17)$

The symmetry code $C(17)$ and its equivalent code $L(17)$ each contains exactly 888 codewords of weight 36.
The set W of all 888 codewords of $L(17)$ of weight 36 spans the code and comprises of the following disjoint subsets:

- 36 rows of a Hadamard matrix H which is normalized with respect to a row $\bar{1}$ and equivalent to a Paley-Hadamard matrix of type II;
- 36 rows of $2H$ (or $-H$) that include a constant row $\bar{2} = (2, \ldots, 2)$;
- a set T of 408 codewords having 15 components equal to 1 and 21 components equal to 2;
- a set $2T$ of 408 codewords obtained by multiplying every codeword from T by 2.

Note. Adding $\bar{2}$ to any $(0,1)$-codeword of weight 18 gives a codeword of weight 36 with 18 1's and 18 2's; hence the code $L(17)$ contains exactly 70 $(0,1)$-codewords of weight 18 obtained by adding the codeword $\bar{2}$ to the rows of H and $2H$, and these 70 $(0,1)$-codewords form the incidence matrix of the Hadamard 3-$(36, 18, 8)$ design $D(17)$.

Enumeration of Hadamard matrices in $L(17)$

We can enumerate all **normalized Hadamard matrices** of order 36 with rows from the set W of codewords of full weight in $L(17)$ by the following simple algorithm that employs Lemma 1 and Lemma 2:

1. Choose a codeword $x \in W$. If $x = \bar{1}$ then go to Step 2, else go to Step 4.
2. Define a graph Γ with vertices the codewords $y \in W$ such that $y = (y_1, \ldots, y_{36})$ contains exactly 18 components equal to 1, and $y_1 = 1$. Two vertices u, z of Γ are adjacent if they differ in 18 positions.
3. Enumerate and record all cliques of size 35 in Γ. Every such clique together with $\bar{1}$ forms a normalized Hadamard matrix.
4. For $i = 1$ to 36 do if $x_i = -1$ then negate the ith column of W.
5. Go to Step 2.

We can enumerate the **regular Hadamard matrices** arising from $L(17)$ as cliques of size 36 in a graph with vertices being the codewords in W containing exactly 15 entries equal to $+1$.

Inequivalent normalizations of W

The set W of all codewords of weight 36 can be **normalized** with respect to every of the 888 codewords by negating columns of W.

An examination of the matrices W_i obtained by normalizing W with respect to a row i having weight structure $(18, 18)$ shows that any such matrix has the same complete weight distribution as W and is given in Table 1.

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

Table 1: The complete weight distribution of W

Theorem

1. The code $L(17)$ contains **two** equivalence classes of Hadamard matrices of order 36:
   - a Hadamard matrix **H** equivalent to a Paley-Hadamard matrix of type II, with full automorphism group of order $\mathbf{19584 = 2^7 3^2 17}$;
   - a second Hadamard matrix $\mathbf{H}'$ with full automorphism group of order **72**, being a **regular** Hadamard matrix such that the associated **symmetric 2-**$(36, 15, 6)$ **design** D' has a **trivial** automorphism group.
2. The ternary code spanned by the incidence matrix of the 2-$(36, 15, 6)$ design D' is an extremal ternary $[36, 18, 12]$ code equivalent to the symmetry code $C(17)$.
3. The automorphism group of $L(17)$ partitions the set of codewords of weight 36 into two orbits of length 72 and 816 respectively, the orbit of length 72 consisting of rows of H and $-H$.
4. The full automorphism group of the code $L(17)$ coincides with the full automorphism group H.

An examination of the matrices W_i obtained by normalizing 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 Table 2, where W_{408} is obtained by normalizing 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)

Table 2: The complete weight distribution of W_{408}

A second regular Hadamard matrix associated with the Pless symmetry code

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 $C(17)$.

Note.
Every row of the regular Hadamard matrix H from part (b) of the 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 $2 \pmod 3$. Hence, the ternary code spanned by the rows of H contains also the rows of A.

Automorphisms of ternary self-dual $[36, 18, 12]$ codes

Theorem (Huffman 1992; Eisenbarth and Nebe 2020)

- Up to equivalence, the only ternary self-dual [36,18,12] code with an automorphism of an **odd** prime order is the Pless symmetry code $C(17)$.
- A ternary self-dual $[36, 18, 12]$ code is either equivalent to the Pless symmetry code $C(17)$ or its full automorphism group is a subgroup of the cyclic group of order 8.

These results and the fact that the Pless symmetry code is spanned by the incidence matrices of symmetric 2-$(36, 15, 6)$ designs, including one having a trivial full automorphism group, motivated us to study symmetric 2-$(36, 15, 6)$ designs with an automorphism of order 2 (or an **involution**) and the related ternary codes.

2-(36,15,6) designs with an involution

The first step in the process of constructing a design with a prescribed automorphism group is to find all admissible orbit **orbit matrices.**
Let $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ be a 2-(v, k, λ) design and $G \leq \mathrm{Aut}(\mathcal{D})$.
We denote by $\mathcal{P}_1, \ldots, \mathcal{P}_m$ the G-orbits of points, and by $\mathcal{B}_1, \ldots, \mathcal{B}_n$ the G-orbits of blocks. Let $|\mathcal{P}_i| = \nu_i$, $|\mathcal{B}_j| = \beta_j$, $i = 1, \ldots, m$, $j = 1, \ldots, n$.

The matrix $M = \{m_{ij})$, where m_{ij} is the number of blocks from jth orbit of blocks that contain a point from the ith orbit of points, is called an **orbit matrix** of $\mathcal{D}$ with respect to the group G. The entries of M satisfy the following equations:

$$\sum_{j=1}^{n} m_{ij} = r, \ \sum_{j=1}^{n} \frac{\nu_t}{\beta_j} m_{sj} m_{tj} = \lambda \nu_t + \delta_{st}(r - \lambda). \qquad (1)$$

After finding all matrices that satisfy the equations (1),
the next step of the construction process involves the expansion of every admissible orbit matrix to an incidence matrix of a 2-(v, k, λ) design.

In order to determine the possible orbit lengths distribution, we use the following upper and lower bounds on the number of fixed points.

Theorem (Lander 1983)

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

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

  Equality holds if σ is an involution and every non-fixed block contains exactly λ fixed points.

- If σ is an involution fixing $f \neq 0$ points then

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

It follows that if σ is an involution of a symmetric 2-$(36, 15, 6)$ then either $f = 0$ or $4 \leq f \leq 18$. Our computations show that there are no orbit matrices for $f \in \{6, 14, 18\}$.

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

# fixed pts	# orbit matrices	# designs	self-dual codes	max d
0	119,907	13,869	none	-
4	12,991	884,139	+	12
8	670	498,592	none	-
10	56	186,369	none	-
12	311	3,719,232	+	9
16	83	209,160	none	-

2-(36,15,6) designs with an involution and extremal self-dual codes

The classification of 2-(36,15,6) designs with an involution and 3-rank 18 implies the following.

Theorem

1. 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.
2. The full automorphism group G of D is of order 24, and G is isomorphic to the symmetric group S_4.
3. The regular Hadamard matrix associated with D is equivalent to the Paley-Hadamard matrix of type II.
4. The ternary code spanned by the incidence matrix of D is equivalent to the Pless symmetry code.

Thank You!

Bibliography

- E. F. Assmus, Jr. and H. F. Mattson, Jr., New 5-designs, *JCTA* **6** (1969), 122-151.
- S. Eisenbarth, G. Nebe, Self-dual codes over chain rings, *Math. Comp. Sci.* **14** (2020), 443 - 456.
- G. Nebe, D. Villar, An analogue of the Pless symmetry codes, *7th Int. Workshop "Optimal Codes and Related Topics"*, Sep. 6 - 12, 2013, Albena, Bulgaria, pp. 158-163.
- V. Pless, On a new family of symmetry codes and related new five-designs, *Bull. Amer. Math. Soc.* **75**, No. 6 (1969), 1339-1342.
- V. Pless, Symmetry codes over $GF(3)$ and new five-designs, *JCTA* **12** (1972), 119-142.
- S. Rukavina and V. D. Tonchev, Extremal ternary self-dual codes of length 36 and symmetric 2-(36,15,6) designs with an automorphism of order 2, *J. Alg. Combinatorics*, doi.org/10.1007/s10801-022-01206-2, 29 Dec. 2022.
- V. D. Tonchev, On Pless symmetry codes, ternary QR codes, and related Hadamard matrices and designs, *DCC* **90**, No. 11 (2022), 2753-2762.