Pless symmetry codes, ternary QR codes, and related Hadamard matrices and designs

Vladimir D. Tonchev

Michigan Technological University

Vera Pless (1931–2020)

Bull. Amer. Math. Soc. 75, No. 6 (1969), 1339-1342.

ON A NEW FAMILY OF SYMMETRY CODES AND RELATED NEW FIVE-DESIGNS

BY VERA PLESS

Communicated by Wallace Givens, May 15, 1969

For every prime $p \equiv -1$ (3) we define a self-orthogonal $(2p+2, p+1)$ code over GF (3). It can be shown that the group leaving a $(2p+2, p+1)$ code invariant is $\mathrm{PSL}_2(p)$. The minimum weights of the first five codes in the family are determined and lead to new 5-designs.

Let t, r, and n be integers with $t \leqq r \leqq n$. A λ; $t-r-n$ design D is a collection of subsets of the n integers, each subset containing r elements, such that any t-subset of the n integers is contained in the same number λ of subsets in D. Some designs, a 1; $5-6-12$, a 1; $5-8-24$, and a 48; $5-12-24$ associated with the Mathieu groups M_{12} and M_{24}, have been known for a long time. Recently, [1] and [5], 2; $5-6-12$ and 2; $5-8-24$ designs have been found. Using coding theory [2] other 5-designs were found for $n=24$ and $n=48$. We have found new 5-designs for $n=36$ and $n=60$ and a number of r's. Also we found new 5-designs for $n=24$ and $n=48$ which are not equivalent to the ones mentioned above. Two t-designs are called equivalent if there is a permutation of the n integers so that the subsets of D go onto subsets in D.

Let V_{2p+2} be a vector space over GF(3) with a fixed, orthonormal basis. We call a subspace of this space an error correcting code. We define a family of codes of $\dim(p+1)$ (referred to as $(2p+2, p+1)$ codes) by a basis (I, S_p) where S_p is given below.

$$S_p = \begin{array}{c|ccccc|}
 & \infty & 0 & 1 \cdots & j \cdots & (p-1) \\
\infty & 0 & 1 & 1 & 1 & 1 \\
0 & \chi(-1) & \chi(0) & \chi(1) & \chi(j) & \chi(p-1) \\
1 & \chi(-1) & & & & \\
\vdots & & & & & \\
i & \chi(-1) & & & \chi(j-i) & \\
\vdots & & & & & \\
(p-1) & \chi(-1) & & & &
\end{array}$$

where $\chi(0)=0$, χ(a square) $=1$, χ(a nonsquare) $=-1$. We refer to the code generated by (I, S_p) as $C(p)$.

JOURNAL OF COMBINATORIAL THEORY (A) 12, 119–142 (1972)

Symmetry Codes over GF(3) and New Five-Designs

VERA PLESS

Air Force Cambridge Research Laboratories, L. G. Hanscom Field, Bedford, Massachusetts

Communicated by Andrew Gleason

Received November 3, 1969

For every odd prime power q where $q \equiv -1(3)$ we define a $(2q+2, q+1)$ code over the field of three elements. It is shown that all the codes in this family are self orthogonal.

For $q = 5$, the (12, 6) code is equivalent to the extended Golay code. For $q = 11$, it can be shown that the minimum weight of the (24, 12) code is 9. For $q = 17, 23, 29$ it is shown, in part by computer, that the minimum weights of the (36, 18), (48, 24), and (60, 30) codes are 12, 15, and 18 respectively.

There are 5-designs associated with vectors of certain weights in the (12, 6), (24, 12), (36, 18), (48, 24), and (60, 30) codes. There are new 5-designs associated with the last four codes mentioned. The 5-designs related to the (36, 18) and (60, 30) codes are the first 5-designs found with their parameters.

For each q we construct a group P of $(2q+2) \times (2q+2)$ monomial matrices. We show that P leaves the $(2q+2, q+1)$ code in the family invariant, and that $P/\{I, -I\}$ is isomorphic to $PGL_2(q)$.

We can form a Hadamard matrix by considering the rows of this matrix as certain maximal weight vectors contained in this code. This Hadamard matrix is left invariant by the group P described above.

I. INTRODUCTION

In this paper we define a family of codes over GF(3), where each code is associated with q, a power of an odd prime, such that $q \equiv -1(3)$. The first code in the family is the well known Golay (12, 6) code. The next four codes have high minimum weights and new 5-designs are associated with them. We also describe a group which leaves each code invariant.

In Section II we define each code in terms of a basis $[I, S_q]$ where S_q is given in terms of the residues and non-residues in GF(q). The matrix S_q figures prominently [5, pp. 209, 210] in the construction of Hadamard matrices. In Section II these codes are shown to be self orthogonal. Also it is shown that, for $q \equiv 1(4)$, $[-S_q, I]$ is also a basis of its code, and, for $q \equiv 3(4)$, $[S_q, I]$ is again a basis of its code.

In Section III, using this and other properties, we determine the

JOURNAL OF COMBINATORIAL THEORY 6, 122–151 (1969)

New 5-Designs*

E. F. ASSMUS, JR.† AND H. F. MATTSON, JR.

Applied Research Laboratory, Sylvania Electronic Systems, Waltham, Massachusetts 02154

Communicated by A. M. Gleason

Received April 4, 1968

ABSTRACT

A t-design on a point-set S is a collection $\mathscr{D}$ of subsets of S, all of the same cardinality, with the property that every t-subset of S is contained in precisely λ elements of $\mathscr{D}$, λ a fixed integer parameter of the design. Via the theory of error-correcting codes, we construct here several new 5-designs on 24 and 48 points as well as the two classic 5-designs on 12 and 24 points associated with the Mathieu groups M_{12} and M_{24}. We are able, in many cases, to say what the automorphism groups of the new 5-designs are.

1. INTRODUCTION

Tactical configurations and Hadamard matrices, studied for many years by combinatorialists, and the newer subject called error-correcting codes, studied for less than twenty years, have some interesting interconnections. The purpose of this report is to establish a number of new results arising therefrom.

Our main result is the construction (via Theorem 4.2) of several new 5-designs on 24 and 48 points and the determination (Section 5) of their automorphism groups as $\mathrm{PSL}_2(23)$ and $\mathrm{PSL}_2(47)$, respectively. A secondary result (Section 5) is that $\mathrm{PSL}_2(l)$ is the automorphism group of certain quadratic-residue codes of length $l + 1$ for all primes l having $(l - 1)/2$ prime and satisfying $23 \leqslant l \leqslant 4{,}079$. (For $l = 23$ we use [15] and a new 5-design on 24 points; the other cases are an immediate consequence of the Parker and Nikolai search [22].) We have derived elsewhere [7] the consequence that for $l \equiv -1 \pmod{12}$, the Paley-Hadamard matrix of order $l + 1$ has $\mathrm{PSL}_2(l)$ as automorphism group for l as above.

---

* The research reported in this paper was sponsored by the Air Force Cambridge Research Laboratories, Office of Aerospace Research, under contract AF19(628)-5998.

† Lehigh University and Sylvania.

Let A and B be linear orthogonal (n, k) and $(n, n-k)$ codes over GF(q) with minimum weights d and e. Let t be an integer less than d. Let v_0 be the largest integer satisfying

$$v_0 - \left[\frac{v_0 + (q-2)}{q-1}\right] < d,$$

and w_0 the largest integer satisfying

$$w_0 - \left[\frac{w_0 + (q-2)}{q-1}\right] < e,$$

where, if $q = 2$, we take $v_0 = w_0 = n$. Then two vectors of A with weight at most v_0 having their non-0 coordinates in the same places must be scalar multiples of each other, and the same for B. This property is essential to our method of proof of our main result,

THEOREM 4.2. *Suppose that the number of non-0 weights of B which are less than or equal to $n - t$ is itself less than or equal to $d - t$. Then, for each weight v with $d \leqslant v \leqslant v_0$, the vectors of weight v in A yield a t-design, and for each weight w with $e \leqslant w \leqslant \min\{n - t, w_0\}$, the vectors of weight w in B yield a t-design.*

Before proving the above result we remark that for B we will in fact show that for each weight w, with $e \leqslant w \leqslant \min\{n - t, w_0\}$, the vectors of weight w yield blocks the complements of which form a t-design. We will need the following combinatorial

LEMMA. *Suppose $(S, \mathscr{D})$ is a t-design. Then, if T and T' are two t-subsets of S, and k an integer satisfying $0 \leqslant k \leqslant t$, we see that*

$$|\{D \in \mathscr{D};\ |D \cap T| = k\}| = |\{D \in \mathscr{D};\ |D \cap T'| = k\}|.$$

That is, the number of subsets in $\mathscr{D}$ intersecting a given t-subset in precisely k points is independent of the chosen t-subset.

PROOF: For $k = t$ the assertion is simply the condition that $(S, \mathscr{D})$ is a t-design. Now we use induction downward observing that for $K \subseteq T$, $|K| = k$, we see that

$$|\{D \in \mathscr{D}; K \subseteq D\}| = \frac{\lambda \binom{n-k}{t-k}}{\binom{d-k}{t-k}} = \lambda_k,$$

Summary

- A code $L(q)$, monomially equivalent to the Pless symmetry code $C(q)$ of length $2q+2$, contains the (0,1)-incidence matrix of a **Hadamard 3-**$(2q+2, q+1, (q-1)/2)$ **design** $D(q)$ associated with a **Paley-Hadamard matrix of type II**.
- The ternary extended QR code of length $n \equiv 0 \pmod{12}$ contains a **Hadamard 3-design** associated with a **Paley-Hadamard matrix of type I**.
- If $q = 5, 11, 17, 23$, the full **permutation** automorphism group of $L(q)$ coincides with the **full** automorphism group of $D(q)$.
- A similar result holds for the ternary extended QR codes of lengths 24 and 48.
- All Hadamard matrices of order 36 formed by codewords of the Pless symmetry code $C(17)$ are classified up to equivalence:
  (1) the **Paley-Hadamard matrix** H **of type II**, with a full automorphism group of order 19584;
  (2) a **regular Hadamard matrix** H' such that the related symmetric 2-$(36, 15, 6)$ design has **trivial** automorphism group.

MacWilliams Identity and Gleason's Theorem

MacWilliams Identity

If $A(x) = \sum_{i=0}^{n} A_i x^i$ and $B(x) = \sum_{i=0}^{n} B_i x^i$ are the weight enumerators of a linear $[n, k]_q$ code C and its dual code $C^{\perp}$, then

$$q^k B(x) = (1 + (q-1)x)^n A(\frac{1-x}{1+(q-1)x}).$$

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

The Assmus-Mattson Theorem

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.

Theorem (Assmus and Mattson 1969)

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

Note

The code QR^*_{11} is equivalent to the extended ternary Golay code G_{12}.

Pless Symmetry Codes

Theorem (V. Pless 1969)

Let $q \equiv -1 \pmod 3$ be an odd prime power, and let

$$S_p = \begin{pmatrix} 0 & 1 & 1 & \cdots & 1 & \cdots & 1 \\ \chi(-1) & \chi(0) & \chi(1) & \cdots & \chi(\beta) & \cdots & \chi(-1) \\ \cdots & & & & & & \\ \chi(-1) & & & \cdots & \chi(\beta-\alpha) & \cdots & \\ \cdots & & & & & & \\ \chi(-1) & & & & & & \end{pmatrix},$$

where $\chi(0) = 0$, $\chi(a) = 1$ if $a \neq 0$ is a square in $GF(q)$, and $\chi(a) = -1$ if $a \neq 0$ is not a square in $GF(q)$.

- The ternary code $C(q)$ generated by (I_{q+1}, S_q) is self-dual.
- The codes $C(q)$ for $q = 5, 11, 17, 23, 29$ ($n = 12, 24, 36, 48, 60$) are extremal and support 5-designs.

Note. The symmetry code $C(5)$ is equivalent to the Golay code G_{12}.

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

- $n = 12$: $G_{12} = QR^*_{11} = C(5)$.
- $n = 24$: QR^*_{23}, $C(11)$.
- $n = 36$: $C(17)$.
- $n = 48$: QR^*_{47}, $C(23)$.
- $n = 60$: QR^*_{59}, $C(29)$, NV.

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

Theorem

Up to equivalence, there is only one extremal ternary self-dual code of length 12 (G_{12}), and two inequivalent codes of length 24 (QR^*_{23} and $C(11)$).

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 $\mathrm{SL}_2(p)$ 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 $\mathrm{XQR}(q)$ 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 $\mathrm{XQR}(11)$ 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.

This short note gives an interpretation of the Pless codes using monomial representations of the group $\mathrm{SL}_2(p)$. This construction allows to read off a large subgroup of the automorphism group of the Pless codes (which was already described in [6]). A different but related series of monomial representations of $\mathrm{SL}_2(p)$ is investigated to construct a new series of self-dual ternary codes $\mathcal{V}(p)$ of length $2(p+1)$ for all primes $p \equiv 5 \pmod 8$. The automorphism group of $\mathcal{V}(p)$ contains the group $\mathrm{SL}_2(p)$. For $p = 5$ we again find $\mathcal{V}(5) \cong \mathfrak{g}_{12}$ the Golay code of length 12, but for larger primes these codes are new. In particular the code $\mathcal{V}(29)$ is an extremal ternary code of length 60, so we now know three extremal ternary codes of length 60: $\mathrm{XQR}(59)$, $\mathcal{P}(29)$ and $\mathcal{V}(29)$.

2 Codes and monomial groups

Let K be a field, $n \in \mathbb{N}$. Then the **monomial group** $\mathrm{Mon}_n(K^*) \leq \mathrm{GL}_n(K)$ is the group of monomial $n \times n$-matrices over K, where a matrix is called

Classification of ternary self-dual codes

- The largest length $n \equiv 0 \pmod 4$ for which **all** ternary self-dual codes have been classified up to equivalence, is $\mathbf{n = 24}$ (Harada and Munemasa 2009).
- The largest length $n \equiv 0 \pmod 4$ for which all **extremal** ternary self-dual codes have been classified up to equivalence, is $\mathbf{n = 28}$ (Harada, Munemasa and Venkov 2009).
- A partial classification of **extremal** ternary self-dual codes of length $\mathbf{n \leq 40}$ admitting automorphisms of **prime** order $\mathbf{p \geq 5}$ was given by C. W. Huffman (1992).
- G. Nebe (2012) proved that, up to equivalence, the only **extremal** ternary self-dual codes of length 48 that admit an automorphism of a **prime** order $\mathbf{p \geq 5}$, are the Pless symmetry code and the extended QR code.
- Extremal ternary self-dual codes of length $n \equiv 0 \pmod{12}$ **do not exist** for $n = 72, 96, 120$, and all $n \geq 144$, because the weight enumerator contains a negative coefficient.

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.
It follows that $n = 1, 2$, or $n = 4t$ for some integer $t \geq 1$.

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

If H is a Hadamard matrix of order $n = 4t$ normalized with respect to row i and column j, deleting the jth column of H and the jth column of $-H$ from the matrix $(H, -H)$ gives the point-by-block (± 1)-incidence matrix of a Hadamard 3-$(\mathbf{4t}, \mathbf{2t}, \mathbf{t-1})$ design D^***.**

A Hadamard matrix H of order $n = 4t$ is **regular** if all rows of H contain the same number **k** of -1's**.**
Then $t = m^2$ for some integer m, $k = 2m^2 \pm m$, and replacing all -1's with zeros gives the $(0, 1)$-incidence matrix of a symmetric 2-$(\mathbf{4m^2}, \mathbf{2m^2} \pm \mathbf{t}, \mathbf{m^2} \pm \mathbf{m})$ design (called sometimes a **Menon** design)**.**

Symmetry codes and Hadamard matrices

Let q be an odd prime power such that $q \equiv -1 \pmod 3$.

Theorem (Pless 1972)

- if $q \equiv 1 \pmod 4$, the matrix

$$H_1(q) = \begin{pmatrix} I + S_q & -I + S_q \\ -I + S_q & -I - S_q \end{pmatrix} \tag{1}$$

  is a Hadamard matrix whose rows are codewords from $C(q)$.
- If $q \equiv 3 \pmod 4$, the matrix

$$H_3(q) = \begin{pmatrix} I + S_q & I + S_q \\ I - S_q & -I + S_q \end{pmatrix} \tag{2}$$

  is a Hadamard matrix whose rows are codewords from $C(q)$.

The Hadamard matrices (1), (2) are equivalent to **Paley-Hadamard matrices of type II**.

The automorphism group of $C(q)$

Theorem (Pless 1972)

The symmetry code $C(q)$ is invariant under a group of order $\mathbf{q(q^2-1)}$ isomorphic to $PGL(2,q)$.

If $q = 5$, 11, or 23, the rows of the Hadamard matrix $H_1(q)$ from (1) (resp. $H_3(q)$ from (2)) and $-H_1(q)$ (resp. $-H_3(q)$) exhaust all codewords of full weight, and span the code.

Theorem (Pless 1972)

If $q = 5$, 11, or 23, the full monomial automorphism group of $C(q)$ coincides with the full automorphism group of $H_1(q)$ (resp. $H_3(q)$).

Note. The full automorphism group of a Paley-Hadamard matrix of type II for $q > 5$ was determined by de Launey and Stafford in 2008, and is of order $\mathbf{4fq(q^2-1)}$ if $q = p^f$, where p is prime.

Note. The symmetry code C(17) of length 36 contains 888 codewords of weight 36, while the number of codewords of weight 60 in $C(29)$ is 41184.

The code $L(q)$: a monomial equivalent of $C(q)$

The sum of all rows of the generator matrix of the symmetry code $C(q)$ is a vector v of full Hamming weight $2q+2$, with all components equal to 1 if -1 is not a square in $GF(q)$, and v has $2q+1$ components equal to 1, and the position labeled by ∞ is equal to -1 whenever -1 is a square in $GF(q)$.

Next, we consider a code $L(q)$ which is monomially equivalent to the Pless symmetry code $C(q)$ and always contains the all-one vector, namely the code with a generator matrix G' given by

$$G' = (I_{q+1}, U_q), \tag{3}$$

where U_q is a $(q+1) \times (q+1)$ matrix obtained from S_q by replacing every nonzero entry in the first column with -1. A parity check matrix of $L(q)$ is given by

$$P = (-U_q^T, I_{q+1}). \tag{4}$$

Symmetry codes and Hadamard 3-designs

Theorem

The matrix H given by

$$H = \begin{pmatrix} G' + P \\ G' - P \end{pmatrix} = \begin{pmatrix} I_{q+1} - U_q^T & U_q + I_{q+1} \\ I_{q+1} + U_q^T & U_q - I_{q+1} \end{pmatrix} \quad (5)$$

is a Hadamard matrix with rows being full weight codewords of $L(q)$.

Theorem

- The code $L(q)$ contains a set of $4q + 2$ (0,1)-codewords of weight $q + 1$ that form the block-by-point incidence matrix of a Hadamard 3-$(2q + 2, q + 1, (q - 1)/2)$ design $D(q)$ associated with a Paley-Hadamard matrix of type II.
- 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 permutation automorphism group of $L(q)$

Theorem

If $q = 5, 11, 17, 23$, the full **permutation** automorphism group of $L(q)$ coincides with the full automorphism group of the Hadamard 3-design $D(q)$, being of order $q(q-1)$.

Note. The code $L(29)$ contains 19606 (0,1)-codewords of weight 30. It is an open question whether this set contains the incidence matrices of any Hadamard 3-$(60, 30, 14)$ designs that are not isomorphic to $D(29)$.

Note. The number of codewords of weight 60 in $L(29)$ is 41184. It seems likely that there may be Hadamard matrices of order 60 formed by codewords of weight 60 that are not equivalent to the Paley-Hadamard matrix of type II.

The code $L(17)$

The set of all 888 codewords of $L(17)$ of full weight 36 comprises of the following disjoint subsets:

- the 36 rows of the Hadamard matrix H (5) normalized with respect to a row $\bar{1}$;
- the 36 rows of $2H$ that include a constant row $\bar{2}$;
- 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 3-design $D(17)$.

Hadamard matrices of order 36 contained in $L(17)$

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 $\mathbf{H}'$, 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.

Some Hadamard matrices of order 36 and their codes

- Up to equivalence, there are exactly 11 Hadamard matrices of order 36 with automorphism groups of order divisible by 17 (Tonchev 1986). Each of these matrices spans a ternary self-dual code of length 36, but only one, namely the Paley-Hadamard matrix of type II, spans an extremal code, equivalent to the Pless symmetry code $C(17)$.
- Up to equivalence, there exists exactly one Hadamard matrix of order 36 with a doubly-transitive automorphism group, isomorphic to $SP(6,2) \times Z_2$ (N. Ito and J. Leon, 1980). This matrix spans a ternary self-orthogonal code of minimum distance 12 and dimension 14.

Hadamard matrices and ternary QR codes

Theorem.

- The symmetry codes $C(11)$, $C(23)$, and $C(29)$ have siblings with the same parameters and weight distribution, being ternary extended quadratic-residue codes.
- If $q \equiv 3 \pmod 4$ is a prime power, a quadratic residue (QR) code of length q is a code spanned by the (0,1)-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.

Theorem

Let $q = 12s + 11$ be a prime power, and let QR_q be the ternary extended QR code of length $q + 1$.

1. QR_q contains a **Paley-Hadamard matrix of type I** having as rows codewords of weight $q + 1$.
2. QR_q contains a set of $2q$ (0,1)-codewords of weight $(q + 1)/2$ that form the incidence matrix of a **Hadamard 3-design** associated with the Paley-Hadamard matrix of type I of order $q + 1$.
3. If $q = 11, 23$ or 47, QR_q contains **exactly** $2q$ (0,1)-codewords of weight $(q + 1)/2$, and the permutation automorphism group of the code coincides with the full automorphism group of the Hadamard 3-design from part (2).

Note. The number of codewords of full weight 60 in QR_{59} is 41184. It is an interesting open question whether there are any Hadamard matrices of order 60 formed by codewords of weight 60 that are not equivalent to the Paley-Hadamard matrix of type I.

Hadamard designs and self-dual codes

Hadamard matrices and designs have been used for the construction of self-orthogonal and self-dual codes over other finite fields.

- The extended binary Golay code is generated by a bordered incidence matrix of a symmetric Hadamard 2-$(23, 11, 5)$ design associated with a Paley-Hadamard matrix of type I.
- Hadamard matrices of order 28 with an automorphism of order 7 were used for the classification of self-orthogonal codes over $GF(7)$:

V. Pless and V. D. Tonchev, Self-dual codes over $GF(7)$, *IEEE Trans. Info. Theory*, **33** (1987) 723-727.

V. D. Tonchev, Hadamard matrices of order 28 with an automorphism of order 7, *J. Combin. Theory* Set A **40** (1985) 62-81.

Binary extremal self-dual codes derived from Hadamard matrices and designs

- The Paley-Hadamard matrix of type II of order 28 is the only Hadamard matrix of this order that admits an automorphism of order 13 and yields an extremal binary self-dual code of length 56:

V. D. Tonchev, Hadamard matrices of order 28 with an automorphism of order 13, *J. Combin. Theory* Set A **35** (1983), 43-57.

V. D. Tonchev, Self-orthogonal designs and extremal dobly-even codes, *J. Combin. Theory* Set A **52** (1989), 197-205.

- Many more extremal doubly-even binary self-dual codes derived from Hadamard matrices of order 28 were found in

F. C. Bussemaker and V. D. Tonchev, New extremal doubly-even codes of length 56 derived from Hadamard matrices of order 28, *Discrete Math.* **76** (1989), 45-49.

Open Questions

A general open question is whether there are more, yet unknown, extremal ternary self-dual codes of length $n \equiv 0 \pmod{12}$.

Specifically,

1. Is the symmetry code $C(17)$ the only extremal code of length 36?
2. Are QR_{47}^* and $C(23)$ the only extremal codes of length 48?
3. Are QR_{59}^*, $C(29)$, and NV the only extremal codes of length 60?
4. Is there a Hadamard matrix of non-Paley type that spans QR_{59}^* or $C(29)$?
5. Is the Nebe-Villar code the row space of a Hadamard matrix of order 60?
6. Is there an extremal ternary self-dual code of length 84, 108, or 132?

Open Questions

A general open question is whether there are more, yet unknown, extremal ternary self-dual codes of length $n \equiv 0 \pmod{12}$. Specifically,

1. Is the symmetry code $C(17)$ the only extremal code of length 36?
2. Are QR^*_{47} and $C(23)$ the only extremal codes of length 48?
3. Are QR^*_{59}, $C(29)$, and NV the only extremal codes of length 60?
4. Is there a Hadamard matrix of non-Paley type that spans QR^*_{59} or $C(29)$?
5. Is the Nebe-Villar code the row space of a Hadamard matrix of order 60?
6. Is there an extremal ternary self-dual code of length 84, 108, or 132?

Open Questions

A general open question is whether there are more, yet unknown, extremal ternary self-dual codes of length $n \equiv 0 \pmod{12}$. Specifically,

1. Is the symmetry code $C(17)$ the only extremal code of length 36?
2. Are QR^*_{47} and $C(23)$ the only extremal codes of length 48?
3. Are QR^*_{59}, $C(29)$, and NV the only extremal codes of length 60?
4. Is there a Hadamard matrix of non-Paley type that spans QR^*_{59} or $C(29)$?
5. Is the Nebe-Villar code the row space of a Hadamard matrix of order 60?
6. Is there an extremal ternary self-dual code of length 84, 108, or 132?

Open Questions

A general open question is whether there are more, yet unknown, extremal ternary self-dual codes of length $n \equiv 0 \pmod{12}$. Specifically,

1. Is the symmetry code $C(17)$ the only extremal code of length 36?
2. Are QR_{47}^{*} and $C(23)$ the only extremal codes of length 48?
3. Are QR_{59}^{*}, $C(29)$, and NV the only extremal codes of length 60?
4. Is there a Hadamard matrix of non-Paley type that spans QR_{59}^{*} or $C(29)$?
5. Is the Nebe-Villar code the row space of a Hadamard matrix of order 60?
6. Is there an extremal ternary self-dual code of length 84, 108, or 132?

Open Questions

A general open question is whether there are more, yet unknown, extremal ternary self-dual codes of length $n \equiv 0 \pmod{12}$. Specifically,

1. Is the symmetry code $C(17)$ the only extremal code of length 36?
2. Are QR^*_{47} and $C(23)$ the only extremal codes of length 48?
3. Are QR^*_{59}, $C(29)$, and NV the only extremal codes of length 60?
4. Is there a Hadamard matrix of non-Paley type that spans QR^*_{59} or $C(29)$?
5. Is the Nebe-Villar code the row space of a Hadamard matrix of order 60?
6. Is there an extremal ternary self-dual code of length 84, 108, or 132?

Open Questions

A general open question is whether there are more, yet unknown, extremal ternary self-dual codes of length $n \equiv 0 \pmod{12}$. Specifically,

1. Is the symmetry code $C(17)$ the only extremal code of length 36?
2. Are QR^*_{47} and $C(23)$ the only extremal codes of length 48?
3. Are QR^*_{59}, $C(29)$, and NV the only extremal codes of length 60?
4. Is there a Hadamard matrix of non-Paley type that spans QR^*_{59} or $C(29)$?
5. Is the Nebe-Villar code the row space of a Hadamard matrix of order 60?
6. Is there an extremal ternary self-dual code of length 84, 108, or 132?

Open Questions

A general open question is whether there are more, yet unknown, extremal ternary self-dual codes of length $n \equiv 0 \pmod{12}$. Specifically,

1. Is the symmetry code $C(17)$ the only extremal code of length 36?
2. Are QR^*_{47} and $C(23)$ the only extremal codes of length 48?
3. Are QR^*_{59}, $C(29)$, and NV the only extremal codes of length 60?
4. Is there a Hadamard matrix of non-Paley type that spans QR^*_{59} or $C(29)$?
5. Is the Nebe-Villar code the row space of a Hadamard matrix of order 60?
6. Is there an extremal ternary self-dual code of length 84, 108, or 132?

Thank You!

Bibliography

- E. F. Assmus, Jr. and H. F. Mattson, Jr., New 5-designs, *J. Combin. Theory, Ser. A* **6** (1969), 122-151.
- W. Cary Huffman, On extremal self-dual ternary codes of lengths 28 to 40, *IEEE Trans. Info. Theory* **38** No. 4 (1992), 1395-1400.
- W. de Launey, R. M. Stafford, On the automorphisms of Palye's type II Hadamard matrix, *Discrete Math.* **308** (2008), 2910-2924.
- C. L. Mallows and N. J. A. Sloane, An upper bound for self-dual codes, *Information and Control* 22 (1973), 188-200.
- G. Nebe, D. Villar, An analogue of the Pless symmetry codes, *Seventh International Workshop on Optimal Codes and Related Topics*, September 6 - 12, 2013, Albena, Bulgaria, pp. 158-163.
- R. E. A. C. Paley, On orthogonal matrices, *J. Math. Phys.* **12** (1933) 311-320.
- 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, *J. Combin. Theory, Ser. A* **12** (1972), 119-142.
- V. Pless and V. D. Tonchev, Self-dual codes over *GF*(7), *IEEE Trans. Info. Theory*, **33** (1987) 723-727.
- V. D. Tonchev, On Pless symmetry codes, ternary QR codes, and related Hadamard matrices and designs, *Designs, Codes and Cryprography*, to appear.
- V. D. Tonchev, Hadamard matrices of order 28 with an automorphism of order 13, *J. Combin. Theory* Set A **35** (1983), 43-57.
- V. D. Tonchev, Hadamard matrices of order 28 with an automorphism of order 7, *J. Combin. Theory* Set A **40** (1985) 62-81.
- V. D. Tonchev, Self-orthogonal designs and extremal dobly-even codes, *J. Combin. Theory* Set A **52** (1989), 197-205.
- V. D. Tonchev, Codes and Designs, Chapter 15 in: *Handbook of Coding Theory*, Vol. II, pages 1229-1268, V. S. Pless and W. C.