Self-Dual Codes over Small Prime Fields from Combinatorial Designs

Dimitris E. Simos[1] Christos Koukouvinos[1]

[1]Department of Mathematics
National Technical University of Athens, Greece

3rd International Conference in Algebraic Informatics (CAI2009)
May 22, Thessaloniki, Greece
Dedicated to the retirement of Prof Dr Werner Kuich

Outline of the Talk

Outline of the Talk

Outline of the Talk

Linear Codes

Definition

A linear $[n, k]$ code C over $GF(p)$ is a k-dimensional vector subspace of $GF(p)^n$, where $GF(p)$ is the Galois field with p elements.

Linear Codes

Definition

A linear $[n, k]$ code C over $GF(p)$ is a k-dimensional vector subspace of $GF(p)^n$, where $GF(p)$ is the Galois field with p elements.

- We consider the case where p is a prime.

Linear Codes

Definition

A linear $[n, k]$ code C over $GF(p)$ is a k-dimensional vector subspace of $GF(p)^n$, where $GF(p)$ is the Galois field with p elements.

- We consider the case where p is a prime.
- The elements of C are called codewords and the (Hamming) weight $wt(x)$ of a codeword x is the number of non-zero coordinates in x.

Linear Codes

Definition

A linear $[n, k]$ code C over $GF(p)$ is a k-dimensional vector subspace of $GF(p)^n$, where $GF(p)$ is the Galois field with p elements.

- We consider the case where p is a prime.
- The elements of C are called codewords and the (Hamming) weight $wt(x)$ of a codeword x is the number of non-zero coordinates in x.

Definition

- The minimum weight of C is defined as $\min\{wt(x) \mid 0 \neq x \in C\}$.
- An $[n, k, d]$ code is an $[n, k]$ code with minimum weight d.

Linear Codes

Definition

A linear $[n, k]$ code C over $GF(p)$ is a k-dimensional vector subspace of $GF(p)^n$, where $GF(p)$ is the Galois field with p elements.

- We consider the case where p is a prime.
- The elements of C are called codewords and the (Hamming) weight $wt(x)$ of a codeword x is the number of non-zero coordinates in x.

Definition

- The minimum weight of C is defined as $\min\{wt(x) \mid 0 \neq x \in C\}$.
- An $[n, k, d]$ code is an $[n, k]$ code with minimum weight d.

- A matrix whose rows are linearly independent and generate the code C is called a generator matrix of C.

Self-Dual Codes

Definition

The dual code $C^{\perp}$ of C is defined as
$C^{\perp} = \{x \in \mathrm{GF}(p)^n | \; x \cdot y = 0 \text{ for all } y \in C\}$. C is self-dual if $C = C^{\perp}$.

Self-Dual Codes

Definition

The dual code $C^{\perp}$ of C is defined as $C^{\perp} = \{x \in \mathrm{GF}(p)^n | \; x \cdot y = 0 \text{ for all } y \in C\}$. C is self-dual if $C = C^{\perp}$.

- Existence of self-dual codes (MacWilliams and Sloane, 1977):
  1. $p \equiv 1 (\mathrm{mod}\ 4)$: A self-dual $[n, n/2]$ code over $GF(p)$ exists if and only if n is even.
  2. $p \equiv 3 (\mathrm{mod}\ 4)$: A self-dual $[n, n/2]$ code over $GF(p)$ exists if and only if $n \equiv 0 (\mathrm{mod}\ 4)$.

Self-Dual Codes

Definition

The dual code $C^{\perp}$ of C is defined as $C^{\perp} = \{x \in \mathrm{GF}(p)^n | \; x \cdot y = 0 \text{ for all } y \in C\}$. C is self-dual if $C = C^{\perp}$.

- Existence of self-dual codes (MacWilliams and Sloane, 1977):
  1. $p \equiv 1 (\mathrm{mod}\ 4)$: A self-dual $[n, n/2]$ code over $GF(p)$ exists if and only if n is even.
  2. $p \equiv 3 (\mathrm{mod}\ 4)$: A self-dual $[n, n/2]$ code over $GF(p)$ exists if and only if $n \equiv 0 (\mathrm{mod}\ 4)$.
- Self-dual codes with the largest minimum weight among self-dual codes of that length are called optimal.

Self-Dual Codes

Definition

The dual code $C^{\perp}$ of C is defined as $C^{\perp} = \{x \in \mathrm{GF}(p)^n | \; x \cdot y = 0 \text{ for all } y \in C\}$. C is self-dual if $C = C^{\perp}$.

- Existence of self-dual codes (MacWilliams and Sloane, 1977):
  1. $p \equiv 1 (\mathrm{mod}\ 4)$: A self-dual $[n, n/2]$ code over $GF(p)$ exists if and only if n is even.
  2. $p \equiv 3 (\mathrm{mod}\ 4)$: A self-dual $[n, n/2]$ code over $GF(p)$ exists if and only if $n \equiv 0 (\mathrm{mod}\ 4)$.
- Self-dual codes with the largest minimum weight among self-dual codes of that length are called optimal.

Bounds on the Minimum distance of linear codes

`www.codetables.de` maintained by Marcus Grassl.

Weight Enumerators of Self-Dual Codes

MacWilliams, Mallows and Sloane, 1972

The weight enumerator of a self-dual code over $GF(p)$ is an element of

$$\mathbb{C}[(x+(\sqrt{p}-1)y)^2, y(x-y)].$$

Weight Enumerators of Self-Dual Codes

MacWilliams, Mallows and Sloane, 1972

The weight enumerator of a self-dual code over $GF(p)$ is an element of

$$\mathbb{C}[(x+(\sqrt{p}-1)y)^2, y(x-y)].$$

An Important Property

The weight enumerator $W_p(n)$ of a self-dual $[n, n/2, n/2+1]$ code over $GF(p)$ is uniquely determined.

What is Combinatorial Design Theory?

Question

Is it possible to arrange elements of a finite set into subsets so that certain properties are satisfied?

What is Combinatorial Design Theory?

Question

Is it possible to arrange elements of a finite set into subsets so that certain properties are satisfied?

Answer

Combinatorial Design Theory is the field of combinatorial mathematics that deals with the existence and construction of systems of finite sets whose intersections have specified numerical properties.

What is Combinatorial Design Theory?

Question

Is it possible to arrange elements of a finite set into subsets so that certain properties are satisfied?

Answer

Combinatorial Design Theory is the field of combinatorial mathematics that deals with the existence and construction of systems of finite sets whose intersections have specified numerical properties.

Example

Hadamard matrices, skew-Hadamard matrices, weighing matrices, orthogonal designs etc.

Why Interested in Self-Dual Codes?

- Their classes include some of the best-known error-correcting codes (i.e. Reed Muller). A Hadamard code (equivalent to a first-order Reed Muller code) was used during the 1971 Mariner 9 mission to correct the error in picture transmission.

Why Interested in Self-Dual Codes?

- Their classes include some of the best-known error-correcting codes (i.e. Reed Muller). A Hadamard code (equivalent to a first-order Reed Muller code) was used during the 1971 Mariner 9 mission to correct the error in picture transmission.

Self-dual codes have strong connections with,

- Combinatorics

Why Interested in Self-Dual Codes?

- Their classes include some of the best-known error-correcting codes (i.e. Reed Muller). A Hadamard code (equivalent to a first-order Reed Muller code) was used during the 1971 Mariner 9 mission to correct the error in picture transmission.

Self-dual codes have strong connections with,

- Combinatorics
- Group Theory and Lattices

Why Interested in Self-Dual Codes?

- Their classes include some of the best-known error-correcting codes (i.e. Reed Muller). A Hadamard code (equivalent to a first-order Reed Muller code) was used during the 1971 Mariner 9 mission to correct the error in picture transmission.

Self-dual codes have strong connections with,

- Combinatorics
- Group Theory and Lattices

while some of their applications can be found in:

- Communications

Why Interested in Self-Dual Codes?

- Their classes include some of the best-known error-correcting codes (i.e. Reed Muller). A Hadamard code (equivalent to a first-order Reed Muller code) was used during the 1971 Mariner 9 mission to correct the error in picture transmission.

Self-dual codes have strong connections with,

- Combinatorics
- Group Theory and Lattices

while some of their applications can be found in:

- Communications
- Number and Design Theory

Our Results on Self-Dual Codes

Our Goal

We are interested in the construction of extremal self-dual codes for large lengths over $GF(3)$ and/or new self-dual codes over $GF(5)$.

Our Results on Self-Dual Codes

Our Goal

We are interested in the construction of extremal self-dual codes for large lengths over $GF(3)$ and/or new self-dual codes over $GF(5)$.

- We constructed some new extremal ternary self-dual codes from skew-Hadamard matrices for:
  1. Length $2n = 16$ from skew-Hadamard matrices of order $n = 8$
  2. Length $2n = 24$ from skew-Hadamard matrices of order $n = 12$
  3. Length $2n = 40$ from skew-Hadamard matrices of order $n = 20$
  4. Length $2n = 48$ from skew-Hadamard matrices of order $n = 24$

Our Results on Self-Dual Codes

Our Goal

We are interested in the construction of extremal self-dual codes for large lengths over $GF(3)$ and/or new self-dual codes over $GF(5)$.

- We constructed some new extremal ternary self-dual codes from skew-Hadamard matrices for:
  1. Length $2n = 16$ from skew-Hadamard matrices of order $n = 8$
  2. Length $2n = 24$ from skew-Hadamard matrices of order $n = 12$
  3. Length $2n = 40$ from skew-Hadamard matrices of order $n = 20$
  4. Length $2n = 48$ from skew-Hadamard matrices of order $n = 24$
- We constructed a new self-dual code of length 72 and dimension 36 whose minimum weight is 16 over $GF(5)$, for the first time.

Hadamard Matrices

Definition

A square $n \times n$ matrix H with elements ± 1 that satisfies $HH^T = nI_n$ is called a Hadamard matrix of order n.

Hadamard Matrices

Definition

A square $n \times n$ matrix H with elements ± 1 that satisfies $HH^T = nI_n$ is called a Hadamard matrix of order n.

Necessary condition for the existence of a Hadamard matrix

The order of an Hadamard matrix is 1, 2, or $n \equiv (0 \mod 4)$.

Hadamard Matrices

Definition

A square $n \times n$ matrix H with elements ± 1 that satisfies $HH^T = nI_n$ is called a Hadamard matrix of order n.

Necessary condition for the existence of a Hadamard matrix

The order of an Hadamard matrix is 1, 2, or $n \equiv (0 \mod 4)$.

Equivalence of Hadamard Matrices

Two Hadamard matrices are equivalent if one can be transformed into the other by a series of row or column:

- permutations
- negations

Skew-Hadamard Matrices

Definition

A matrix H with entries from $\{1, -1\}$, for which

$$H = C + I_n$$

is said to be skew-Hadamard matrix of order n if $CC^T = (n-1)I_n$ and $C^T = -C$.

Skew-Hadamard Matrices

Definition

A matrix H with entries from $\{1, -1\}$, for which

$$H = C + I_n$$

is said to be skew-Hadamard matrix of order n if $CC^T = (n-1)I_n$ and $C^T = -C$.

- A readable reference is
  Geramita, A.V., Seberry, J.: Orthogonal Designs. Quadratic Forms and Hadamard Matrices. Lecture Notes in Pure and Applied Mathematics, 45. Marcel Dekker, Inc., New York (1979)

Construction of Self-Dual Codes over $GF(p)$

Construction Method over $GF(p)$ from Skew-Hadamard Matrices

Let H be a skew-Hadamard matrix of order n and suppose that there exist elements $a \neq 0$, $b \neq 0$, and $c \neq 0$ from $GF(p)$ such that

$$a^2 + (b-c)^2 + (n-1)c^2 \equiv 0 \pmod{p}.$$

Then the matrix

$$G = [aI_n \; cH - bI_n]$$

generates a self-dual code of length $2n$ and dimension n.

Bounds on the Largest Possible Minimum Weight

- A ternary self-dual code C which is optimal is called extremal, i.e. if it has the largest possible minimum weight.

Bounds on the Largest Possible Minimum Weight

- A ternary self-dual code C which is optimal is called extremal, i.e. if it has the largest possible minimum weight.
- The known bounds of d for $GF(3)$ are given by Tonchev (1996).

Bounds on the Largest Possible Minimum Weight

- A ternary self-dual code C which is optimal is called extremal, i.e. if it has the largest possible minimum weight.
- The known bounds of d for $GF(3)$ are given by Tonchev (1996).

Theorem

The minimum distance d of a ternary self-dual $[2n, n]$ code C satisfies

$$d \leq 3[n/6] + 3$$

where by $[x]$ we denote the nearest integer function of x.

Computation of Minimum Weight

- We computed the minimum weight of the self-dual codes derived by our construction for each possible solution of the diophantine equation,

$$a^2 + (b-c)^2 + (n-1)c^2 \equiv 0 \pmod 3$$

Computation of Minimum Weight

- We computed the minimum weight of the self-dual codes derived by our construction for each possible solution of the diophantine equation,

$$a^2 + (b-c)^2 + (n-1)c^2 \equiv 0 \pmod 3$$

- The diophantine equation has solutions for $n = 8, 12, 20, 24$ when $a \neq 0$, $b \neq 0$, $c \neq 0$ over $GF(3)$

Computation of Minimum Weight

- We computed the minimum weight of the self-dual codes derived by our construction for each possible solution of the diophantine equation,

$$a^2 + (b-c)^2 + (n-1)c^2 \equiv 0 \pmod 3$$

- The diophantine equation has solutions for $n = 8, 12, 20, 24$ when $a \neq 0$, $b \neq 0$, $c \neq 0$ over $GF(3)$
- We found extremal self-dual codes of lengths $2n = 16, 24, 40, 48$ derived from inequivalent skew-Hadamard matrices of orders $n = 8, 12, 20, 24$.

(Monomial) Equivalence of Linear Codes

Definition

Two linear codes C_1 and C_2 over $GF(p)$ are monomially equivalent if there is a monomial matrix M over $GF(p)$ such that $C_2 = C_1 M = \{cM \mid c \in C_1\}$.

- A monomial matrix over $GF(p)$ which maps C to itself is called an automorphism of C.

(Monomial) Equivalence of Linear Codes

Definition

Two linear codes C_1 and C_2 over $GF(p)$ are monomially equivalent if there is a monomial matrix M over $GF(p)$ such that $C_2 = C_1 M = \{cM \mid c \in C_1\}$.

- A monomial matrix over $GF(p)$ which maps C to itself is called an automorphism of C.
- The set of all automorphisms of C is called the automorphism group $Aut(C)$ of C.

Notation

For a self-dual code derived from the i-th inequivalent skew-Hadamard matrix of order n we shall use the notation $C_{n,i}$.

$[16, 8]$ Ternary Self-Dual Codes

- The unique skew-Hadamard matrix (up to equivalence) of order 8 is

$$H_8 = C + I_8 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ -1 & 1 & 1 & -1 & 1 & -1 & 1 & -1 \\ -1 & -1 & 1 & 1 & -1 & 1 & 1 & -1 \\ -1 & 1 & -1 & 1 & 1 & 1 & -1 & -1 \\ -1 & -1 & 1 & -1 & 1 & 1 & -1 & 1 \\ -1 & 1 & -1 & -1 & -1 & 1 & 1 & 1 \\ -1 & -1 & -1 & 1 & 1 & -1 & 1 & 1 \\ -1 & 1 & 1 & 1 & -1 & -1 & -1 & 1 \end{pmatrix}$$

$[16, 8]$ Ternary Self-Dual Codes

- The unique skew-Hadamard matrix (up to equivalence) of order 8 is

$$H_8 = C + I_8 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ -1 & 1 & 1 & -1 & 1 & -1 & 1 & -1 \\ -1 & -1 & 1 & 1 & -1 & 1 & 1 & -1 \\ -1 & 1 & -1 & 1 & 1 & 1 & -1 & -1 \\ -1 & -1 & 1 & -1 & 1 & 1 & -1 & 1 \\ -1 & 1 & -1 & -1 & -1 & 1 & 1 & 1 \\ -1 & -1 & -1 & 1 & 1 & -1 & 1 & 1 \\ -1 & 1 & 1 & 1 & -1 & -1 & -1 & 1 \end{pmatrix}$$

C	a	b	c	d	$\lvert Aut(C)\rvert$	$W(x, y)$
$C_{8,1}$	1	2	1	6	$43008 = 2^{11} \cdot 3 \cdot 7$	$x^{16} + 224x^{10}y^6 + 2720x^7y^9$ $+3360x^4y^{12} + 256xy^{15}$

[16, 8] Ternary Self-Dual Codes

- The unique skew-Hadamard matrix (up to equivalence) of order 8 is

$$H_8 = C + I_8 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ -1 & 1 & 1 & -1 & 1 & -1 & 1 & -1 \\ -1 & -1 & 1 & 1 & -1 & 1 & 1 & -1 \\ -1 & 1 & -1 & 1 & 1 & 1 & -1 & -1 \\ -1 & -1 & 1 & -1 & 1 & 1 & -1 & 1 \\ -1 & 1 & -1 & -1 & -1 & 1 & 1 & 1 \\ -1 & -1 & -1 & 1 & 1 & -1 & 1 & 1 \\ -1 & 1 & 1 & 1 & -1 & -1 & -1 & 1 \end{pmatrix}$$

C	a	b	c	d	$\lvert Aut(C)\rvert$	$W(x, y)$
$C_{8,1}$	1	2	1	6	$43008 = 2^{11} \cdot 3 \cdot 7$	$x^{16} + 224x^{10}y^6 + 2720x^7y^9 + 3360x^4y^{12} + 256xy^{15}$

- The code $C_{8,1}$ is extremal (i.e. the bound for $n = 8$ from Tonchev's theorem is 6).

[24, 12] Ternary Self-Dual Codes

- The unique skew-Hadamard matrix (up to equivalence) of order 12 is

$$H_{12} = C + I_{12} = \begin{pmatrix}
1 & 1 & -1 & 1 & 1 & 1 & 1 & -1 & 1 & -1 & 1 & 1 \\
-1 & 1 & 1 & 1 & 1 & 1 & -1 & 1 & 1 & 1 & 1 & -1 \\
1 & -1 & 1 & 1 & 1 & 1 & 1 & 1 & -1 & 1 & -1 & 1 \\
-1 & -1 & -1 & 1 & 1 & -1 & 1 & -1 & 1 & 1 & -1 & -1 \\
-1 & -1 & -1 & -1 & 1 & 1 & -1 & 1 & 1 & -1 & -1 & 1 \\
-1 & -1 & -1 & 1 & -1 & 1 & 1 & 1 & -1 & -1 & 1 & -1 \\
-1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 & 1 & 1 & 1 \\
1 & -1 & -1 & 1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 & 1 \\
-1 & -1 & 1 & -1 & -1 & 1 & 1 & -1 & 1 & 1 & 1 & 1 \\
1 & -1 & -1 & -1 & 1 & 1 & -1 & -1 & -1 & 1 & 1 & -1 \\
-1 & -1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & -1 & 1 & 1 \\
-1 & 1 & -1 & 1 & -1 & 1 & -1 & -1 & -1 & 1 & -1 & 1
\end{pmatrix}$$

[24, 12] Ternary Self-Dual Codes

- The unique skew-Hadamard matrix (up to equivalence) of order 12 is

$$H_{12} = C + I_{12} = \begin{pmatrix}
1 & 1 & -1 & 1 & 1 & 1 & 1 & -1 & 1 & -1 & 1 & 1 \\
-1 & 1 & 1 & 1 & 1 & 1 & -1 & 1 & 1 & 1 & 1 & -1 \\
1 & -1 & 1 & 1 & 1 & 1 & 1 & 1 & -1 & 1 & -1 & 1 \\
-1 & -1 & -1 & 1 & 1 & -1 & 1 & -1 & 1 & 1 & -1 & -1 \\
-1 & -1 & -1 & -1 & 1 & 1 & -1 & 1 & 1 & -1 & -1 & 1 \\
-1 & -1 & -1 & 1 & -1 & 1 & 1 & 1 & -1 & -1 & 1 & -1 \\
-1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 & 1 & 1 & 1 \\
1 & -1 & -1 & 1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 & 1 \\
-1 & -1 & 1 & -1 & -1 & 1 & 1 & -1 & 1 & 1 & 1 & 1 \\
1 & -1 & -1 & -1 & 1 & 1 & -1 & -1 & -1 & 1 & 1 & -1 \\
-1 & -1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & -1 & 1 & 1 \\
-1 & 1 & -1 & 1 & -1 & 1 & -1 & -1 & -1 & 1 & -1 & 1
\end{pmatrix}$$

C	a	b	c	d	$\lvert Aut(C)\rvert$	$W(x, y)$
$C_{12,1}$	1	1	1	9	$5280 = 2^5 \cdot 3 \cdot 5 \cdot 11$	$x^{24} + 4048x^{15}y^9 + 61824x^{12}y^{12} + 242880x^9y^{15}$ $+198352x^6y^{18} + 24288x^3y^{21} + 48y^{24}$

[24, 12] Ternary Self-Dual Codes

- The unique skew-Hadamard matrix (up to equivalence) of order 12 is

$$H_{12} = C + I_{12} = \begin{pmatrix}
1 & 1 & -1 & 1 & 1 & 1 & 1 & -1 & 1 & -1 & 1 & 1 \\
-1 & 1 & 1 & 1 & 1 & 1 & -1 & 1 & 1 & 1 & 1 & -1 \\
1 & -1 & 1 & 1 & 1 & 1 & 1 & 1 & -1 & 1 & -1 & 1 \\
-1 & -1 & -1 & 1 & 1 & -1 & 1 & -1 & 1 & 1 & -1 & -1 \\
-1 & -1 & -1 & -1 & 1 & 1 & -1 & 1 & 1 & -1 & -1 & 1 \\
-1 & -1 & -1 & 1 & -1 & 1 & 1 & 1 & -1 & -1 & 1 & -1 \\
-1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 & 1 & 1 & 1 \\
1 & -1 & -1 & 1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 & 1 \\
-1 & -1 & 1 & -1 & -1 & 1 & 1 & -1 & 1 & 1 & 1 & 1 \\
1 & -1 & -1 & -1 & 1 & 1 & -1 & -1 & -1 & 1 & 1 & -1 \\
-1 & -1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & -1 & 1 & 1 \\
-1 & 1 & -1 & 1 & -1 & 1 & -1 & -1 & -1 & 1 & -1 & 1
\end{pmatrix}$$

C	a	b	c	d	$\lvert Aut(C)\rvert$	$W(x, y)$
$C_{12,1}$	1	1	1	9	$5280 = 2^5 \cdot 3 \cdot 5 \cdot 11$	$x^{24} + 4048x^{15}y^9 + 61824x^{12}y^{12} + 242880x^9y^{15}$ $+198352x^6y^{18} + 24288x^3y^{21} + 48y^{24}$

- The code $C_{12,1}$ is extremal (i.e. the bound for $n = 12$ from Tonchev's theorem is 9).

$[40, 20]$ Ternary Self-Dual Codes

- The unique skew-Hadamard matrix (up to equivalence) of order 20 is

$$H_{20} = C + I_{20} = \begin{pmatrix}
+ & - & + & - & + & + & - & - & + & + & - & - & - & - & + & - & - & - & - & + \\
+ & + & - & + & - & - & - & + & + & + & - & - & - & + & - & - & - & - & + & - \\
- & + & + & - & + & - & + & + & + & - & - & - & + & - & - & - & - & + & - & - \\
+ & - & + & + & - & + & + & + & - & - & - & + & - & - & - & - & + & - & - & - \\
- & + & - & + & + & + & + & - & - & + & + & - & - & - & + & - & - & - & - & - \\
- & + & + & - & - & + & - & + & - & + & - & - & - & - & + & + & + & + & + & - \\
+ & + & - & - & - & + & + & - & + & - & - & - & - & + & - & + & + & + & - & + \\
+ & - & - & - & + & - & + & + & - & + & - & - & + & - & - & + & + & - & + & + \\
- & - & - & + & + & + & - & + & + & - & - & + & - & - & - & + & - & + & + & + \\
- & - & + & + & - & - & + & - & + & + & + & - & - & - & - & - & + & + & + & + \\
+ & + & + & + & - & + & + & + & + & - & + & - & + & - & + & + & - & - & + & + \\
+ & + & + & - & + & + & + & - & + & + & + & - & + & - & - & - & + & + & + & + \\
+ & + & - & + & + & + & + & - & + & + & - & + & + & - & + & - & - & + & + & - \\
+ & - & + & + & + & + & - & + & + & + & + & - & + & + & - & + & + & + & - & - \\
- & + & + & + & + & - & + & + & + & + & - & + & - & + & + & + & - & - & - & + \\
+ & + & + & + & - & - & - & - & - & + & - & + & + & - & - & + & - & + & - & + \\
+ & + & + & - & + & - & - & - & + & - & + & + & - & - & - & + & + & - & + & - \\
+ & + & - & + & + & - & - & + & - & - & + & - & - & - & + & - & + & + & - & + \\
+ & - & + & + & + & - & + & - & - & - & - & - & - & + & + & + & - & + & + & - \\
- & + & + & + & + & + & - & - & - & - & - & - & + & + & - & - & + & - & + & + \\
\end{pmatrix}$$

$[40, 20]$ Ternary Self-Dual Codes (Continued)

C	a	b	c	d	$\lvert Aut(C)\rvert$	$W(x, y)$
$C_{20,1}$	1	2	1	12	$13680 = 2^4 \cdot 3^2 \cdot 5 \cdot 19$	$x^{40} + 19760x^{28}y^{12} + 1138176x^{25}y^{15} + 25549680x^{22}y^{18} + 236945280x^{19}y^{21} + 907161840x^{16}y^{24} + 1389711680x^{13}y^{27} + 783017664x^{10}y^{30} + 137826000x^{7}y^{33} + 5394480x^{4}y^{36} + 19840xy^{39}$

$[40, 20]$ Ternary Self-Dual Codes (Continued)

C	a	b	c	d	$\lvert Aut(C)\rvert$	$W(x, y)$
$C_{20,1}$	1	2	1	12	$13680 = 2^4 \cdot 3^2 \cdot 5 \cdot 19$	$x^{40} + 19760x^{28}y^{12} + 1138176x^{25}y^{15} + 25549680x^{22}y^{18} + 236945280x^{19}y^{21} + 907161840x^{16}y^{24} + 1389711680x^{13}y^{27} + 783017664x^{10}y^{30} + 137826000x^{7}y^{33} + 5394480x^{4}y^{36} + 19840xy^{39}$

- The code $C_{20,1}$ is extremal (i.e. the bound for $n = 20$ from Tonchev's theorem is 12).

$[48, 24]$ Ternary Self-Dual Codes

- We used the sixteen inequivalent skew-Hadamard matrices of order 24.

$[48, 24]$ Ternary Self-Dual Codes

- We used the sixteen inequivalent skew-Hadamard matrices of order 24.

C	a	b	c	d	$\lvert Aut(C)\rvert$	C	a	b	c	d	$\lvert Aut(C)\rvert$
$C_{24,1}$	1	1	1	12	$48 = 2^4 \cdot 3$	$C_{24,9}$	1	1	1	12	$48 = 2^4 \cdot 3$
$C_{24,2}$	1	1	1	12	$24 = 2^3 \cdot 3$	$C_{24,10}$	1	1	1	12	$96 = 2^5 \cdot 3$
$C_{24,3}$	1	1	1	12	$48 = 2^4 \cdot 3$	$C_{24,11}$	1	1	1	12	$96 = 2^5 \cdot 3$
$C_{24,4}$	1	1	1	12	$80 = 2^4 \cdot 5$	$C_{24,12}$	1	1	1	12	$10560 = 2^6 \cdot 3 \cdot 5 \cdot 11$
$C_{24,5}$	1	1	1	12	$32 = 2^5$	$C_{24,13}$	1	1	1	12	$10560 = 2^6 \cdot 3 \cdot 5 \cdot 11$
$C_{24,6}$	1	1	1	12	$32 = 2^5$	$C_{24,14}$	1	1	1	15	$48576 = 2^6 \cdot 3 \cdot 11 \cdot 23$
$C_{24,7}$	1	1	1	12	$32 = 2^5$	$C_{24,15}$	1	1	1	12	$80 = 2^4 \cdot 5$
$C_{24,8}$	1	1	1	12	$48 = 2^4 \cdot 3$	$C_{24,16}$	1	1	1	12	$24 = 2^3 \cdot 3$

$[48, 24]$ Ternary Self-Dual Codes

- We used the sixteen inequivalent skew-Hadamard matrices of order 24.

C	a	b	c	d	$\lvert Aut(C)\rvert$	C	a	b	c	d	$\lvert Aut(C)\rvert$
$C_{24,1}$	1	1	1	12	$48 = 2^4 \cdot 3$	$C_{24,9}$	1	1	1	12	$48 = 2^4 \cdot 3$
$C_{24,2}$	1	1	1	12	$24 = 2^3 \cdot 3$	$C_{24,10}$	1	1	1	12	$96 = 2^5 \cdot 3$
$C_{24,3}$	1	1	1	12	$48 = 2^4 \cdot 3$	$C_{24,11}$	1	1	1	12	$96 = 2^5 \cdot 3$
$C_{24,4}$	1	1	1	12	$80 = 2^4 \cdot 5$	$C_{24,12}$	1	1	1	12	$10560 = 2^6 \cdot 3 \cdot 5 \cdot 11$
$C_{24,5}$	1	1	1	12	$32 = 2^5$	$C_{24,13}$	1	1	1	12	$10560 = 2^6 \cdot 3 \cdot 5 \cdot 11$
$C_{24,6}$	1	1	1	12	$32 = 2^5$	$C_{24,14}$	1	1	1	15	$48576 = 2^6 \cdot 3 \cdot 11 \cdot 23$
$C_{24,7}$	1	1	1	12	$32 = 2^5$	$C_{24,15}$	1	1	1	12	$80 = 2^4 \cdot 5$
$C_{24,8}$	1	1	1	12	$48 = 2^4 \cdot 3$	$C_{24,16}$	1	1	1	12	$24 = 2^3 \cdot 3$

- The code $C_{24,14}$ is extremal (i.e. the bound for $n = 24$ from Tonchev's theorem is 15).
- We have not computed the weight enumerators due to a computational complexity limit.

Survey for Self-Dual Codes over $GF(5)$

- Classification:
  - Lengths ≤ 12 (Leon, Pless and Sloane, 1982)
  - Lengths 14 and 16 (Harada, Ostergard, 2003)

Survey for Self-Dual Codes over $GF(5)$

- Classification:
  - Lengths ≤ 12 (Leon, Pless and Sloane, 1982)
  - Lengths 14 and 16 (Harada, Ostergard, 2003)
- Largest minimum weights:
  - Determined for lengths ≤ 24 (Dougherty, Gulliver and Harada, 2000)

Survey for Self-Dual Codes over $GF(5)$

- Classification:
  - Lengths ≤ 12 (Leon, Pless and Sloane, 1982)
  - Lengths 14 and 16 (Harada, Ostergard, 2003)
- Largest minimum weights:
  - Determined for lengths ≤ 24 (Dougherty, Gulliver and Harada, 2000)
- Highest minimum distance known:
  - Tables and constructions for lengths ≤ 70 (Gaborit and Otmani, 2003)

Survey for Self-Dual Codes over $GF(5)$ (Cont.)

- Recent improvements on the upper bounds of minimum distance:
  - Lengths $26 \leq 2n \leq 40$ (Kim and Han, 2008)
  - Lengths $26 \leq 2n \leq 34$ (Kotsireas, Koukouvinos and Simos, 2009)

Survey for Self-Dual Codes over $GF(5)$ (Cont.)

- Recent improvements on the upper bounds of minimum distance:
  - Lengths $26 \leq 2n \leq 40$ (Kim and Han, 2008)
  - Lengths $26 \leq 2n \leq 34$ (Kotsireas, Koukouvinos and Simos, 2009)
- Construction methods from combinatorial designs:
  - Skew-Hadamard matrices: Lengths $20 \leq 2n \leq 60$ (Kim and Sole, 2008)
  - Conference matrices: Lengths $36, 48, 60, 64, 76$ (Gulliver and Harada, 2004)
  - Skew-Hadamard matrices: Lengths $8 \leq 2n \leq 40$ (Georgiou, Koukouvinos and Lappas, 2007)

Survey for Self-Dual Codes over $GF(5)$ (Cont.)

- Recent improvements on the upper bounds of minimum distance:
  - Lengths $26 \leq 2n \leq 40$ (Kim and Han, 2008)
  - Lengths $26 \leq 2n \leq 34$ (Kotsireas, Koukouvinos and Simos, 2009)
- Construction methods from combinatorial designs:
  - Skew-Hadamard matrices: Lengths $20 \leq 2n \leq 60$ (Kim and Sole, 2008)
  - Conference matrices: Lengths $36, 48, 60, 64, 76$ (Gulliver and Harada, 2004)
  - Skew-Hadamard matrices: Lengths $8 \leq 2n \leq 40$ (Georgiou, Koukouvinos and Lappas, 2007)
- New inequivalent optimal self-dual codes:
  - Length 24 (Han, Kim, Lee and Lee, 2009)
  - Lengths 48 and 56 (Koukouvinos and Simos, 2009)

A [72,36] Self-Dual Code over GF(5)

Construction of the $[72, 36]$ Self-Dual Code

- Design : Skew-Hadamard matrix of order 36

A [72,36] Self-Dual Code over GF(5)

Construction of the $[72, 36]$ Self-Dual Code

- Design : Skew-Hadamard matrix of order 36
- Constants : $a = b = 1$ and $c = 3$ for $p = 5$

A [72,36] Self-Dual Code over GF(5)

Construction of the $[72, 36]$ Self-Dual Code

- Design : Skew-Hadamard matrix of order 36
- Constants : $a = b = 1$ and $c = 3$ for $p = 5$
- Generator : $G = [aI_{36}\ 3H - I_{36}]$

A [72,36] Self-Dual Code over GF(5)

Construction of the $[72, 36]$ Self-Dual Code

- Design : Skew-Hadamard matrix of order 36
- Constants : $a = b = 1$ and $c = 3$ for $p = 5$
- Generator : $G = [aI_{36}\ 3H - I_{36}]$

Computation of Minimum Weight in MAGMA

```
Linear Code over GF(5) of length 72 with 36 generators.
Enumerating using 8 generators at a time:
Completed Matrix  1:
lower = 16, upper = 16.
Computation complete
72574065912 vectors enumerated
in total (0.000000% of 72 36 code)
Final Results: lower = 16, upper = 16
IsSelfDual: True
```

A [72,36] Self-Dual Code over GF(5) (Continued)

Theorem

There exists a $[72, 36, 16]$ *self-dual code over* $GF(5)$

Updated Table with Optimal Minimum Distances

- Code lengths: First and fourth columns
- Optimal minimum distances: Second and fifth columns
- Number of inequivalent optimal codes: Third and sixth columns

Length	d	N	Length	d	N
2	2	1	28	$10-11$	≥ 20
4	2	1	30	$10-12$	≥ 204
6	4	1	32	$11-12$	≥ 1
8	4	1	34	$11-12$	≥ 11
10	4	3	36	$12-13$	≥ 1
12	6	1	38	$12-14$	≥ 1
14	6	3	40	$13-15$	≥ 1
16	7	1	48	$14-20$	≥ 2
18	7	9	56	$16-23$	≥ 2
20	8	≥ 8	72	16–?	≥ 1
22	8	≥ 59	80	17–?	≥ 1
24	9	≥ 2	88	19–?	≥ 1
26	$9-10$	≥ 1			

Conclusion

1. We constructed some new extremal ternary self-dual codes from skew-Hadamard matrices.

Conclusion

1. We constructed some new extremal ternary self-dual codes from skew-Hadamard matrices.
2. We constructed a new self-dual code of length 72 and dimension 36 whose minimum weight is 16 over $GF(5)$, for the first time.

Conclusion

1. We constructed some new extremal ternary self-dual codes from skew-Hadamard matrices.
2. We constructed a new self-dual code of length 72 and dimension 36 whose minimum weight is 16 over $GF(5)$, for the first time.

Future Work

- Develop an upper bound on the minimum distance of the generated self-dual codes; independent of the Galois field, $GF(p)$

Conclusion

1. We constructed some new extremal ternary self-dual codes from skew-Hadamard matrices.
2. We constructed a new self-dual code of length 72 and dimension 36 whose minimum weight is 16 over $GF(5)$, for the first time.

Future Work

- Develop an upper bound on the minimum distance of the generated self-dual codes; independent of the Galois field, $GF(p)$
- Construct extremal ternary self-dual codes for larger lengths

Conclusion

1. We constructed some new extremal ternary self-dual codes from skew-Hadamard matrices.
2. We constructed a new self-dual code of length 72 and dimension 36 whose minimum weight is 16 over $GF(5)$, for the first time.

Future Work

- Develop an upper bound on the minimum distance of the generated self-dual codes; independent of the Galois field, $GF(p)$
- Construct extremal ternary self-dual codes for larger lengths
- Find new self-dual codes for larger fields, i.e. $GF(7)$

References


Koukouvinos, C., Simos, D.E.: Construction of new self-dual codes over $GF(5)$ using skew-Hadamard matrices, to appear in Adv Math. Commun.


Kim, J.-L., Sole, P.: Skew Hadamard designs and their codes, Des. Codes Cryptogr. 49, 135–145 (2008)


Leon, J.S., Pless, V., Sloane, N.J.A.: Self-dual codes over $GF(5)$, J. Combin. Theory Ser. A 32, 178–194 (1982)


MacWilliams, F.J., Sloane, N.J.A.: The Theory of Error-Correcting Codes, The Netherlands, North-Holland, Amsterdam (1977)


Tonchev, V.D.: Codes, In: Colbourn, C.J., Dinitz, J.H., (eds.) The CRC Handbook of Combinatorial Designs. pp. 517–543. CRC Press, Boca Raton, Fla., (1996)