Extremal maximal isotropic codes of Type I-IV

Annika Meyer

RWTH Aachen University

16.04.2010, Thurnau

Overview

Let $\mathbb{F}$ be a finite field, $N \in \mathbb{N}$. A *code* of length N is a subspace $C \leq \mathbb{F}^N$.

Let $\mathbb{F}$ be a finite field, $N \in \mathbb{N}$. A *code* of length N is a subspace $C \leq \mathbb{F}^N$.
Let α be an automorphism of $\mathbb{F}$, of order 1 or 2. The *dual* of C is

$$C^\perp := \{v \in \mathbb{F}^N \mid \sum_{i=1}^{N} v_i \cdot \alpha(c_i) = 0 \text{ for all } c \in C\},$$

which is, again, a code.

Let $\mathbb{F}$ be a finite field, $N \in \mathbb{N}$. A *code* of length N is a subspace $C \leq \mathbb{F}^N$.
Let α be an automorphism of $\mathbb{F}$, of order 1 or 2. The *dual* of C is

$$C^{\perp} := \{v \in \mathbb{F}^N \mid \sum_{i=1}^{N} v_i \cdot \alpha(c_i) = 0 \text{ for all } c \in C\},$$

which is, again, a code.
If $C \subseteq C^{\perp}$ then C is called *self-orthogonal*.

Let $\mathbb{F}$ be a finite field, $N \in \mathbb{N}$. A *code* of length N is a subspace $C \leq \mathbb{F}^N$.
Let α be an automorphism of $\mathbb{F}$, of order 1 or 2. The *dual* of C is

$$C^{\perp} := \{v \in \mathbb{F}^N \mid \sum_{i=1}^{N} v_i \cdot \alpha(c_i) = 0 \text{ for all } c \in C\},$$

which is, again, a code.
If $C \subseteq C^{\perp}$ then C is called *self-orthogonal*.
If $C = C^{\perp}$ then C is called *self-dual*.

The *(Hamming) weight* of $v \in \mathbb{F}^N$ is the number of nonzero entries in v, denoted by $\mathrm{wt}(v)$.

The *(Hamming) weight* of $v \in \mathbb{F}^N$ is the number of nonzero entries in v, denoted by $\mathrm{wt}(v)$.

The *minimum weight* of a code $C \leq \mathbb{F}^N$ is

$$d(C) := \min_{0 \neq c \in C} \mathrm{wt}(c).$$

The *(Hamming) weight* of $v \in \mathbb{F}^N$ is the number of nonzero entries in v, denoted by $\mathrm{wt}(v)$.

The *minimum weight* of a code $C \leq \mathbb{F}^N$ is

$$d(C) := \min_{0 \neq c \in C} \mathrm{wt}(c).$$

Due to the linearity of C,

$$d(C) = \min_{c \neq c' \in C} |\{i \in \{1, \ldots, N\} \mid c_i \neq c'_i\}|.$$

The *(Hamming) weight* of $v \in \mathbb{F}^N$ is the number of nonzero entries in v, denoted by $\mathrm{wt}(v)$.

The *minimum weight* of a code $C \leq \mathbb{F}^N$ is

$$d(C) := \min_{0 \neq c \in C} \mathrm{wt}(c).$$

Due to the linearity of C,

$$d(C) = \min_{c \neq c' \in C} |\{i \in \{1, \ldots, N\} \mid c_i \neq c'_i\}|.$$

Using C, one can

The *(Hamming) weight* of $v \in \mathbb{F}^N$ is the number of nonzero entries in v, denoted by $\mathrm{wt}(v)$.

The *minimum weight* of a code $C \leq \mathbb{F}^N$ is

$$d(C) := \min_{0 \neq c \in C} \mathrm{wt}(c).$$

Due to the linearity of C,

$$d(C) = \min_{c \neq c' \in C} |\{i \in \{1, \ldots, N\} \mid c_i \neq c'_i\}|.$$

Using C, one can

- detect up to $d(C) - 1$ errors,

The *(Hamming) weight* of $v \in \mathbb{F}^N$ is the number of nonzero entries in v, denoted by $\mathrm{wt}(v)$.

The *minimum weight* of a code $C \leq \mathbb{F}^N$ is

$$d(C) := \min_{0 \neq c \in C} \mathrm{wt}(c).$$

Due to the linearity of C,

$$d(C) = \min_{c \neq c' \in C} |\{i \in \{1, \ldots, N\} \mid c_i \neq c'_i\}|.$$

Using C, one can

- detect up to $d(C) - 1$ errors,
- correct up to $\lfloor \frac{d(C)-1}{2} \rfloor$ errors.

Theorem (Gleason, Pierce 1967)
Let $C = C^{\perp} \leq \mathbb{F}_q^N$ and let $m \in \mathbb{N}$ such that $\mathrm{wt}(c) \in m\mathbb{Z}$ *for all $c \in C$. Then one of the following holds.*

Theorem (Gleason, Pierce 1967)

Let $C = C^{\perp} \leq \mathbb{F}_q^N$ and let $m \in \mathbb{N}$ such that $\mathrm{wt}(c) \in m\mathbb{Z}$ *for all $c \in C$. Then one of the following holds.*

(I) *$q = 2$ and $m = 2$ (self-dual binary codes)*

Theorem (Gleason, Pierce 1967)

Let $C = C^\perp \leq \mathbb{F}_q^N$ and let $m \in \mathbb{N}$ such that $\mathrm{wt}(c) \in m\mathbb{Z}$ *for all $c \in C$. Then one of the following holds.*

(I) *$q = 2$ and $m = 2$ (self-dual binary codes),*

(II) *$q = 2$ and $m = 4$ (doubly-even self-dual binary codes)*

Theorem (Gleason, Pierce 1967)

Let $C = C^\perp \leq \mathbb{F}_q^N$ and let $m \in \mathbb{N}$ such that $\mathrm{wt}(c) \in m\mathbb{Z}$ *for all $c \in C$. Then one of the following holds.*

(I) *$q = 2$ and $m = 2$ (self-dual binary codes),*

(II) *$q = 2$ and $m = 4$ (doubly-even self-dual binary codes),*

(III) *$q = 3$ and $m = 3$ (self-dual ternary codes)*

Theorem (Gleason, Pierce 1967)
Let $C = C^{\perp} \leq \mathbb{F}_q^N$ and let $m \in \mathbb{N}$ such that $\mathrm{wt}(c) \in m\mathbb{Z}$ for all $c \in C$. Then one of the following holds.

(I) *$q = 2$ and $m = 2$ (self-dual binary codes),*

(II) *$q = 2$ and $m = 4$ (doubly-even self-dual binary codes),*

(III) *$q = 3$ and $m = 3$ (self-dual ternary codes),*

(IV) *$q = 4$ and $m = 2$ (quaternary Hermitian self-dual codes)*

Theorem (Gleason, Pierce 1967)

Let $C = C^{\perp} \leq \mathbb{F}_q^N$ and let $m \in \mathbb{N}$ such that $\mathrm{wt}(c) \in m\mathbb{Z}$ *for all $c \in C$. Then one of the following holds.*

(I) $q = 2$ *and* $m = 2$ *(self-dual binary codes),*

(II) $q = 2$ *and* $m = 4$ *(doubly-even self-dual binary codes),*

(III) $q = 3$ *and* $m = 3$ *(self-dual ternary codes),*

(IV) $q = 4$ *and* $m = 2$ *(quaternary Hermitian self-dual codes),*

(o) $q = 4$ *and* $m = 2$ *(certain Euclidean self-dual codes)*

Theorem (Gleason, Pierce 1967)

Let $C = C^{\perp} \leq \mathbb{F}_q^N$ and let $m \in \mathbb{N}$ such that $\mathrm{wt}(c) \in m\mathbb{Z}$ for all $c \in C$. Then one of the following holds.

(I) *$q = 2$ and $m = 2$ (self-dual binary codes),*

(II) *$q = 2$ and $m = 4$ (doubly-even self-dual binary codes),*

(III) *$q = 3$ and $m = 3$ (self-dual ternary codes),*

(IV) *$q = 4$ and $m = 2$ (quaternary Hermitian self-dual codes),*

(o) *$q = 4$ and $m = 2$ (certain Euclidean self-dual codes),*

(d) *$m = 2$ and $C \cong \perp^{N/2} (1, a)$, where either q is even and $a = 1$ or $q \equiv 1 \pmod 4$ and $a^2 = -1$ or α has order 2 and $a \cdot \alpha(a) = -1$.*

Extremality and a uniqueness result

The first four Types in the previous theorem are named I-IV.

The first four Types in the previous theorem are named I-IV.

Theorem

Let $T \in \{\mathrm{I}, \dots, \mathrm{IV}\}$ and let C be a self-dual Type T code of length N. Then $d(C) \leq \delta(T, N)$, where

$$\delta(T,N) := \begin{cases} 2 + 2\lfloor \frac{N}{8} \rfloor, & T = \mathrm{I} \\ 4 + 4\lfloor \frac{N}{24} \rfloor, & T = \mathrm{II} \\ 3 + 3\lfloor \frac{N}{12} \rfloor, & T = \mathrm{III} \\ 2 + 2\lfloor \frac{N}{6} \rfloor, & T = \mathrm{IV}\,. \end{cases}$$

The first four Types in the previous theorem are named I-IV.

Theorem

Let $T \in \{\mathrm{I}, \ldots, \mathrm{IV}\}$ and let C be a self-dual Type T code of length N. Then $d(C) \leq \delta(T, N)$, where

$$\delta(T,N) := \begin{cases} 2 + 2\lfloor \frac{N}{8} \rfloor, & T = \mathrm{I} \\ 4 + 4\lfloor \frac{N}{24} \rfloor, & T = \mathrm{II} \\ 3 + 3\lfloor \frac{N}{12} \rfloor, & T = \mathrm{III} \\ 2 + 2\lfloor \frac{N}{6} \rfloor, & T = \mathrm{IV}\,. \end{cases}$$

If $d(C)$ reaches the above bound then C is called *extremal*.

We can read off $d(C)$ from the *(Hamming) weight enumerator*

$$\mathrm{we}(C) := \sum_{c \in C} y^{\mathrm{wt}(c)} x^{N - \mathrm{wt}(c)} \in \mathbb{C}[x, y],$$

a homgeneous complex polynomial of degree N which counts the codewords of each Hamming weight.

We can read off $d(C)$ from the *(Hamming) weight enumerator*

$$\mathrm{we}(C) := \sum_{c \in C} y^{\mathrm{wt}(c)} x^{N-\mathrm{wt}(c)} \in \mathbb{C}[x, y],$$

a homgeneous complex polynomial of degree N which counts the codewords of each Hamming weight.

If C has minimum weight d then $\mathrm{we}(C)$ is of the form

We can read off $d(C)$ from the *(Hamming) weight enumerator*

$$\mathrm{we}(C) := \sum_{c\in C} y^{\mathrm{wt}(c)} x^{N-\mathrm{wt}(c)} \in \mathbb{C}[x,y],$$

a homgeneous complex polynomial of degree N which counts the codewords of each Hamming weight.

If C has minimum weight d then $\mathrm{we}(C)$ is of the form

$$x^N$$

We can read off $d(C)$ from the *(Hamming) weight enumerator*

$$\mathrm{we}(C) := \sum_{c \in C} y^{\mathrm{wt}(c)} x^{N-\mathrm{wt}(c)} \in \mathbb{C}[x, y],$$

a homgeneous complex polynomial of degree N which counts the codewords of each Hamming weight.

If C has minimum weight d then $\mathrm{we}(C)$ is of the form

$$x^N + a_d y^d x^{N-d}$$

We can read off $d(C)$ from the *(Hamming) weight enumerator*

$$\mathrm{we}(C) := \sum_{c \in C} y^{\mathrm{wt}(c)} x^{N-\mathrm{wt}(c)} \in \mathbb{C}[x, y],$$

a homgeneous complex polynomial of degree N which counts the codewords of each Hamming weight.

If C has minimum weight d then $\mathrm{we}(C)$ is of the form

$$x^N + a_d y^d x^{N-d} + \ldots + a_N y^N.$$

Theorem
If C is a self-dual Code of Type I, II, III *or* IV *then* $\mathrm{we}(C) \in \mathbb{C}[f_T, g_T]$ *according to the table below.*

T	f_T	g_T
I	$x^2 + y^2$ i_2	$x^2y^2(x^2 - y^2)^2$ Hamming code e_8
II	$x^8 + 14x^4y^4 + y^8$ Hamming code e_8	$x^4y^4(x^4 - y^4)^4$ binary Golay code g_{24}
III	$x^4 + 8xy^3$ tetracode t_4	$y^3(x^3 - y^3)^3$ ternary Golay code g_{12}
IV	$x^2 + 3y^2$ $i_2 \otimes \mathbb{F}_4$	$y^2(x^2 - y^2)^2$ hexacode h_6

Extremality and a uniqueness result

Fix an integer N and a Type $T \in \{\mathrm{I}, \ldots, \mathrm{IV}\}$ and let $\delta := \delta(T, N)$.

Fix an integer N and a Type $T \in \{\mathrm{I}, \ldots, \mathrm{IV}\}$ and let $\delta := \delta(T, N)$. There exists a *unique* element in $\mathbb{C}[f_T, g_T]$ of the form

$$x^N + a_\delta y^\delta x^{N-\delta} + \cdots + a_N y^N,$$

where $a_i \in \mathbb{Q}$ for $i = 1, \ldots, N$.

Fix an integer N and a Type $T \in \{\mathrm{I}, \ldots, \mathrm{IV}\}$ and let $\delta := \delta(T, N)$.
There exists a *unique* element in $\mathbb{C}[f_T, g_T]$ of the form

$$x^N + a_\delta y^\delta x^{N-\delta} + \cdots + a_N y^N,$$

where $a_i \in \mathbb{Q}$ for $i = 1, \ldots, N$.
Using the Bürmann-Lagrange formula, one computes that $a_\delta \neq 0$.

Fix an integer N and a Type $T \in \{\mathrm{I}, \ldots, \mathrm{IV}\}$ and let $\delta := \delta(T, N)$. There exists a *unique* element in $\mathbb{C}[f_T, g_T]$ of the form

$$x^N + a_\delta y^\delta x^{N-\delta} + \cdots + a_N y^N,$$

where $a_i \in \mathbb{Q}$ for $i = 1, \ldots, N$.
Using the Bürmann-Lagrange formula, one computes that $a_\delta \neq 0$.

Corollary

The weight enumerator of an extremal self-dual code of Type I-IV *is unique.*

The length of a self-dual Type T code, $T \in \{\mathrm{I}, \ldots, \mathrm{IV}\}$, is always a multiple of

$$o_T := \deg(f_T) = \min(\{\deg(f_T), \deg(g_T)\}).$$

The length of a self-dual Type T code, $T \in \{\mathrm{I}, \ldots, \mathrm{IV}\}$, is always a multiple of

$$o_T := \deg(f_T) = \min(\{\deg(f_T), \deg(g_T)\}).$$

T	I	II	III	IV
o_T	2	8	4	2

The length of a self-dual Type T code, $T \in \{\mathrm{I}, \ldots, \mathrm{IV}\}$, is always a multiple of

$$o_T := \deg(f_T) = \min(\{\deg(f_T), \deg(g_T)\}).$$

T	I	II	III	IV
o_T	2	8	4	2

Now assume that N is no multiple of o_T.

The length of a self-dual Type T code, $T \in \{\text{I}, \dots, \text{IV}\}$, is always a multiple of

$$o_T := \deg(f_T) = \min(\{\deg(f_T), \deg(g_T)\}).$$

T	I	II	III	IV
o_T	2	8	4	2

Now assume that N is no multiple of o_T.

Consider *maximal self-orthogonal* (m. s.-o.) codes,
i.e. $C \subseteq C^\perp$ and if $C \subseteq D$ for a code $D \subseteq D^\perp$, then $C = D$.

Extremality for maximal self-orthogonal codes

Theorem

Let C be a m. s.-o. Type II *code of length* $N \equiv 7 \pmod 8$. *Then* $d(C^{\perp}) \leq 3 + 4\lfloor \frac{N+1}{24} \rfloor$.

Theorem

Let C be a m. s.-o. Type II code of length $N \equiv 7 \pmod 8$. Then $d(C^{\perp}) \leq 3 + 4\lfloor \frac{N+1}{24} \rfloor$.

Proof.

Assume that $d(C^{\perp}) \geq 4 + 4\lfloor \frac{N+1}{24} \rfloor$.

Theorem

Let C be a m. s.-o. Type II *code of length $N \equiv 7 \pmod 8$. Then $d(C^\perp) \leq 3 + 4\lfloor \frac{N+1}{24} \rfloor$.*

Proof.

Assume that $d(C^\perp) \geq 4 + 4\lfloor \frac{N+1}{24} \rfloor$. From the theory of Witt groups, $C^\perp = \langle C, v \rangle$, where $\mathrm{wt}(v) \equiv_4 3$.

Extremality for maximal self-orthogonal codes

Theorem

Let C be a m. s.-o. Type II *code of length* $N \equiv 7 \pmod 8$. *Then* $d(C^\perp) \leq 3 + 4\lfloor \frac{N+1}{24} \rfloor$.

Proof.

Assume that $d(C^\perp) \geq 4 + 4\lfloor \frac{N+1}{24} \rfloor$. From the theory of Witt groups, $C^\perp = \langle C, v \rangle$, where $\mathrm{wt}(v) \equiv_4 3$.

Let $E = \left(\begin{smallmatrix} C & 0 \\ v & 1 \end{smallmatrix}\right) \leq \mathbb{F}_2^{N+1}$. Then $E = E^\perp$ is Type II, and

Extremality for maximal self-orthogonal codes

Theorem
Let C be a m. s.-o. Type II *code of length* $N \equiv 7 \pmod 8$*. Then* $d(C^{\perp}) \leq 3 + 4\lfloor \frac{N+1}{24} \rfloor$.

Proof.
Assume that $d(C^{\perp}) \geq 4 + 4\lfloor \frac{N+1}{24} \rfloor$. From the theory of Witt groups, $C^{\perp} = \langle C, v \rangle$, where $\mathrm{wt}(v) \equiv_4 3$.

Let $E = \begin{pmatrix} C & 0 \\ v & 1 \end{pmatrix} \leq \mathbb{F}_2^{N+1}$. Then $E = E^{\perp}$ is Type II, and

- $d(E) \geq 4 + 4\lfloor \frac{N+1}{24} \rfloor$, hence E is extremal (i.e. equality holds). Thus the words in E of weight $d(E)$ hold a design.

Extremality for maximal self-orthogonal codes

Theorem
Let C be a m. s.-o. Type II *code of length $N \equiv 7$ (mod 8). Then $d(C^{\perp}) \leq 3 + 4\lfloor \frac{N+1}{24} \rfloor$.*

Proof.
Assume that $d(C^{\perp}) \geq 4 + 4\lfloor \frac{N+1}{24} \rfloor$. From the theory of Witt groups, $C^{\perp} = \langle C, v \rangle$, where $\mathrm{wt}(v) \equiv_4 3$.

Let $E = \left(\begin{smallmatrix} C & 0 \\ v & 1 \end{smallmatrix} \right) \leq \mathbb{F}_2^{N+1}$. Then $E = E^{\perp}$ is Type II, and

- $d(E) \geq 4 + 4\lfloor \frac{N+1}{24} \rfloor$, hence E is extremal (i.e. equality holds). Thus the words in E of weight $d(E)$ hold a design.
- $\{e \in E \mid \mathrm{wt}(e) = d(E)\} = \{(c\,0) \mid c \in C^{\perp},\ \mathrm{wt}(c) = d(E)\}$.

Theorem

Let C be a m. s.-o. Type II *code of length $N \equiv 7 \pmod 8$. Then $d(C^\perp) \leq 3 + 4\lfloor \frac{N+1}{24} \rfloor$.*

Proof.

Assume that $d(C^\perp) \geq 4 + 4\lfloor \frac{N+1}{24} \rfloor$. From the theory of Witt groups, $C^\perp = \langle C, v \rangle$, where $\mathrm{wt}(v) \equiv_4 3$.

Let $E = \left(\begin{smallmatrix} C & 0 \\ v & 1 \end{smallmatrix}\right) \leq \mathbb{F}_2^{N+1}$. Then $E = E^\perp$ is Type II, and

- $d(E) \geq 4 + 4\lfloor \frac{N+1}{24} \rfloor$, hence E is extremal (i.e. equality holds). Thus the words in E of weight $d(E)$ hold a design.
- $\{e \in E \mid \mathrm{wt}(e) = d(E)\} = \{(c\,0) \mid c \in C^\perp,\ \mathrm{wt}(c) = d(E)\}$.

This is a contradiction, hence $d(C^\perp) \leq 3 + 4\lfloor \frac{N+1}{24} \rfloor$. □

Extremality for maximal self-orthogonal codes

Theorem

Let $T \in \{\mathrm{I}, \ldots, \mathrm{IV}\}$ and let C be a maximal self-orthogonal Type T code of length N. Then $d(C^{\perp}) \leq \delta(T, N)$, where $\delta(T, N)$ is given in the table below.

Extremality for maximal self-orthogonal codes

Theorem
Let $T \in \{\mathrm{I}, \ldots, \mathrm{IV}\}$ and let C be a maximal self-orthogonal Type T code of length N. Then $d(C^{\perp}) \leq \delta(T, N)$, where $\delta(T, N)$ is given in the table below.

Definition
A m. s.-o. code whose minimum distance reaches the above bound is called *dual extremal*.

Extremality for maximal self-orthogonal codes

T	N	$\delta(T,N)$
I	$N \not\equiv_{24} 23$	$\delta(\mathrm{I}, N+1)$
	23 (24)	$3+4\lfloor \frac{N}{24} \rfloor$
II	1, 9 or 17 (24)	$1+\lfloor \frac{N}{24} \rfloor + 3\lfloor \frac{N+7}{24} \rfloor$
	2 (24)	$\lfloor \frac{N+8}{6} \rfloor$
	3,11 or 19 (24)	$1+2\lfloor \frac{N}{24} \rfloor + \lfloor \frac{N+5}{24} \rfloor + \lfloor \frac{N+13}{24} \rfloor$
	4 (24)	$\frac{N+8}{6}$
	5 (24)	$1+4\lfloor \frac{N}{24} \rfloor$
	6 (24)	$2+4\lfloor \frac{N}{24} \rfloor$
	7, 13, 14 or 15 (24)	$3+4\lfloor \frac{N}{24} \rfloor$
	10 or 18 (24)	$1+\lfloor \frac{N}{8} \rfloor + \lfloor \frac{N+8}{24} \rfloor$
	12 (24)	$\frac{N}{6}$

T	N	$\delta(T,N)$
II	20 (24)	$\frac{N+4}{6}$
	21 (24)	$5+4\lfloor \frac{N}{24} \rfloor$
	22 (24)	$6+4\lfloor \frac{N}{24} \rfloor$
	23 (24)	$7+4\lfloor \frac{N}{24} \rfloor$
III	1, 5 or 9 (12)	$3+3\lfloor \frac{N}{12} \rfloor$
	2 (12)	$1+3\lfloor \frac{N}{12} \rfloor$
	3, 6 or 7 (12)	$2+3\lfloor \frac{N}{12} \rfloor$
	10 (12)	$4+3\lfloor \frac{N}{12} \rfloor$
	11 (12)	$5+3\lfloor \frac{N}{12} \rfloor$
IV	1 or 3 (6)	$1+2\lfloor \frac{N}{6} \rfloor$
	5 (6)	$3+2\lfloor \frac{N}{6} \rfloor$

A uniqueness result

Theorem

The Hamming weight enumerator of a dual extremal m. s.-o. code of Type II, III *or* IV *is uniquely determined.*

A uniqueness result

Theorem

The Hamming weight enumerator of a dual extremal m. s.-o. code of Type II, III *or* IV *is uniquely determined.*

What is the algebraic structure of the vector space generated by weight enumerators of m. s.-o. codes of Type I-IV?

A uniqueness result

Theorem

The Hamming weight enumerator of a dual extremal m. s.-o. code of Type II, III *or* IV *is uniquely determined.*

What is the algebraic structure of the vector space generated by weight enumerators of m. s.-o. codes of Type I-IV?

Definition

For $T \in \{\mathrm{I}, \ldots, \mathrm{IV}\}$ and $k \in \{1, \ldots, o_T - 1\}$, let

$$I_k^T := \langle \mathrm{we}(C) \mid C \text{ m. s.-o. Type } T \text{ code of length } \equiv k (\mathrm{mod}\, o_T) \rangle_{\mathbb{C}}.$$

Theorem

The Hamming weight enumerator of a dual extremal m. s.-o. code of Type II*,* III *or* IV *is uniquely determined.*

What is the algebraic structure of the vector space generated by weight enumerators of m. s.-o. codes of Type I-IV?

Definition

For $T \in \{\mathrm{I}, \ldots, \mathrm{IV}\}$ and $k \in \{1, \ldots, o_T - 1\}$, let

$$I_k^T := \langle \mathrm{we}(C) \mid C \text{ m. s.-o. Type } T \text{ code of length } \equiv k (\mathrm{mod}\, o_T) \rangle_{\mathbb{C}}.$$

Let C be a m. s.-o. Type T code of length $\equiv k \pmod{o_T}$, and let D be a self-dual Type T code.

Theorem

The Hamming weight enumerator of a dual extremal m. s.-o. code of Type II, III *or* IV *is uniquely determined.*

What is the algebraic structure of the vector space generated by weight enumerators of m. s.-o. codes of Type I-IV?

Definition

For $T \in \{\mathrm{I}, \ldots, \mathrm{IV}\}$ and $k \in \{1, \ldots, o_T - 1\}$, let

$$I_k^T := \langle \mathrm{we}(C) \mid C \text{ m. s.-o. Type} T \text{ code of length } \equiv k (\mathrm{mod} o_T) \rangle_{\mathbb{C}}.$$

Let C be a m. s.-o. Type T code of length $\equiv k \pmod{o_T}$, and let D be a self-dual Type T code.

Then $C \perp D$ is a m. s.-o. Type T code of length $\equiv k \pmod{o_T}$.

Theorem
The Hamming weight enumerator of a dual extremal m. s.-o. code of Type II*,* III *or* IV *is uniquely determined.*

What is the algebraic structure of the vector space generated by weight enumerators of m. s.-o. codes of Type I-IV?

Definition
For $T \in \{\text{I}, \ldots, \text{IV}\}$ and $k \in \{1, \ldots, o_T - 1\}$, let

$$I_k^T := \langle \text{we}(C) \mid C \text{ m. s.-o. Type} T \text{ code of length } \equiv k (\text{mod} o_T) \rangle_{\mathbb{C}}.$$

Let C be a m. s.-o. Type T code of length $\equiv k \pmod{o_T}$, and let D be a self-dual Type T code.

Then $C \perp D$ is a m. s.-o. Type T code of length $\equiv k \pmod{o_T}$.

A uniqueness result

Remark

The space I_k^T is a module for $\mathbb{C}[f_T, g_T]$.

A uniqueness result

Remark
The space I_k^T is a module for $\mathbb{C}[f_T, g_T]$.

Theorem
The $\mathbb{C}[f_T, g_T]$-module I_k^T is free and finitely generated.

Remark

The space I_k^T is a module for $\mathbb{C}[f_T, g_T]$.

Theorem

The $\mathbb{C}[f_T, g_T]$-module I_k^T is free and finitely generated.

Bases for the $\mathbb{C}[f_T, g_T]$-module I_k^T are given in the book "Self-dual codes and invariant theory" by Nebe, Rains and Sloane.

Remark
The space I_k^T is a module for $\mathbb{C}[f_T, g_T]$.

Theorem
The $\mathbb{C}[f_T, g_T]$-module I_k^T is free and finitely generated.
Bases for the $\mathbb{C}[f_T, g_T]$-module I_k^T are given in the book "Self-dual codes and invariant theory" by Nebe, Rains and Sloane. There exists a *triangular* basis $p_0, \dots, p_r$ of

$$(I_k^T)_N := \{p \in I_k^T \mid p \text{ homogeneous of degree } N\},$$

for every integer $N \equiv k \pmod{o_T}$.

A uniqueness result

$$p_i(1, y) = c_i^{(0)} y^0 + \ldots + c_i^{(N)} y^N$$

A uniqueness result

$$p_i(1,y) = c_i^{(0)}y^0 + \ldots + c_i^{(N)}y^N$$

$$\begin{array}{c|cccccccc}
 & y^0 & y^1 & \ldots & y^k & y^{k+1} & y^{k+2} & \ldots \\
\hline
p_0 & c_0^{(0)} & c_1^{(0)} & \ldots & c_k^{(0)} & 0 & c_{k+2}^{(0)} & \ldots \\
p_1 & 0 & c_1^{(1)} & \ldots & c_k^{(1)} & 0 & c_{k+2}^{(1)} & \ldots \\
\vdots & \vdots & & \ddots & \vdots & \vdots & \vdots & \\
p_k & \vdots & & & c_k^{(k)} & 0 & & \\
p_{k+1} & 0 & \ldots & & & 0 & c_{k+1}^{(k+2)} & \\
\vdots & \vdots & & & & 0 & \vdots &
\end{array}$$

Examples

If $T \in \{\mathrm{II}, \mathrm{III}, \mathrm{IV}\}$ and $N \equiv -1 \pmod{o_T}$ then puncturing an extremal self-dual code of length $N+1$ yields the dual of a dual extremal m. s.-o. code of length N.

Examples

If $T \in \{\mathrm{II}, \mathrm{III}, \mathrm{IV}\}$ and $N \equiv -1 \pmod{o_T}$ then puncturing an extremal self-dual code of length $N + 1$ yields the dual of a dual extremal m. s.-o. code of length N.

- The dual of the binary $[7, 4, 3]$ Hamming code is the unique dual extremal Type II code of length 7.

If $T \in \{\mathrm{II}, \mathrm{III}, \mathrm{IV}\}$ and $N \equiv -1 \pmod{o_T}$ then puncturing an extremal self-dual code of length $N+1$ yields the dual of a dual extremal m. s.-o. code of length N.

- The dual of the binary $[7,4,3]$ Hamming code is the unique dual extremal Type II code of length 7.
- The dual of the ternary $[11,6,5]$ Golay code is the unique dual extremal Type III code of length 11.

Examples

If $T \in \{\mathrm{II}, \mathrm{III}, \mathrm{IV}\}$ and $N \equiv -1 \pmod{o_T}$ then puncturing an extremal self-dual code of length $N+1$ yields the dual of a dual extremal m. s.-o. code of length N.

- The dual of the binary $[7,4,3]$ Hamming code is the unique dual extremal Type II code of length 7.
- The dual of the ternary $[11,6,5]$ Golay code is the unique dual extremal Type III code of length 11.

This is false for $T = \mathrm{I}$ and $N = 17$, e.g. ($\delta(\mathrm{I}, 18) = 4 = \delta(1, 17)$).

Examples

If $T \in \{\mathrm{II}, \mathrm{III}, \mathrm{IV}\}$ and $N \equiv -1 \pmod{o_T}$ then puncturing an extremal self-dual code of length $N+1$ yields the dual of a dual extremal m. s.-o. code of length N.

- The dual of the binary $[7,4,3]$ Hamming code is the unique dual extremal Type II code of length 7.
- The dual of the ternary $[11,6,5]$ Golay code is the unique dual extremal Type III code of length 11.

This is false for $T = \mathrm{I}$ and $N = 17$, e.g. $(\delta(\mathrm{I},18) = 4 = \delta(1,17))$. Let C, D be the two extremal self-dual $[18,9,4]$ codes.

Examples

If $T \in \{\mathrm{II}, \mathrm{III}, \mathrm{IV}\}$ and $N \equiv -1 \pmod{o_T}$ then puncturing an extremal self-dual code of length $N+1$ yields the dual of a dual extremal m. s.-o. code of length N.

- The dual of the binary $[7, 4, 3]$ Hamming code is the unique dual extremal Type II code of length 7.
- The dual of the ternary $[11, 6, 5]$ Golay code is the unique dual extremal Type III code of length 11.

This is false for $T = \mathrm{I}$ and $N = 17$, e.g. $(\delta(\mathrm{I}, 18) = 4 = \delta(1, 17))$. Let C, D be the two extremal self-dual $[18, 9, 4]$ codes.

- Puncturing C at a particular position yields the dual of a dual extremal $[17, 8]$ code.

Examples

If $T \in \{\text{II}, \text{III}, \text{IV}\}$ and $N \equiv -1 \pmod{o_T}$ then puncturing an extremal self-dual code of length $N+1$ yields the dual of a dual extremal m. s.-o. code of length N.

- The dual of the binary $[7,4,3]$ Hamming code is the unique dual extremal Type II code of length 7.
- The dual of the ternary $[11,6,5]$ Golay code is the unique dual extremal Type III code of length 11.

This is false for $T = \text{I}$ and $N = 17$, e.g. ($\delta(\text{I}, 18) = 4 = \delta(1, 17)$).
Let C, D be the two extremal self-dual $[18,9,4]$ codes.

- Puncturing C at a particular position yields the dual of a dual extremal $[17,8]$ code.
- Puncturing D at any position yields codes of minimum weight 3.