Counting self-dual codes over finite rings

Fidel Nemenzo

Institute of Mathematics, University of the Philippines

Algebra and Computation 2007, Tokyo
5 December 2007

Recent results are based on joint work with **Hideo Wada** (Sophia University) and **Kiyoshi Nagata** (Daito Bunka University).

Coding theory: Background

Errors occur during the transmission of information.

Coding theory deals with mathematical methods used to package information so that transmission errors are detected and corrected.

The goals of coding theory are:

1) the efficient transmission of information

2) the integrity of information transmitted.

Coding theory: Background

Errors occur during the transmission of information.

Coding theory deals with mathematical methods used to package information so that transmission errors are detected and corrected.

The goals of coding theory are:

1) the efficient transmission of information

2) the integrity of information transmitted.

Coding theory: Background

Errors occur during the transmission of information.

Coding theory deals with mathematical methods used to package information so that transmission errors are detected and corrected.

The goals of coding theory are:

1) the efficient transmission of information

2) the integrity of information transmitted.

Coding theory: Background

Errors occur during the transmission of information.

Coding theory deals with mathematical methods used to package information so that transmission errors are detected and corrected.

The goals of coding theory are:

1) the efficient transmission of information

2) the integrity of information transmitted.

Coding theory: Background

From its origins in engineering and information science, coding theory has also developed as an area of discrete mathematics, combining algebra, combinatorics, number theory and even geometry.

Coding theory: Background

Let A be a set of symbols, $n \in \mathbb{N}$

$A^n := \{(a_0, a_1, \ldots, a_{n-1}) \mid a_i \in A\}$, the set of n-tuples over A

code of length n **over** A: a subset of A^n

codeword: element of a code

A distance function is usually defined on A^n

Example: Hamming distance between two n-tuples $a = (a_0, a_1, \ldots, a_{n-1})$ and $b = (b_0, b_1, \ldots, b_{n-1})$:

$$d_H(a, b) := \#\{i \mid a_i \neq b_i\}$$

Coding theory: Background

Let A be a set of symbols, $n \in \mathbb{N}$

$A^n := \{(a_0, a_1, \ldots, a_{n-1}) \mid a_i \in A\}$, the set of n-tuples over A

code of length n **over** A: a subset of A^n

codeword: element of a code

A distance function is usually defined on A^n

Example: Hamming distance between two n-tuples $a = (a_0, a_1, \ldots, a_{n-1})$ and $b = (b_0, b_1, \ldots, b_{n-1})$:

$$d_H(a, b) := \#\{i \mid a_i \neq b_i\}$$

Coding theory: Background

Let A be a set of symbols, $n \in \mathbb{N}$

$A^n := \{(a_0, a_1, \ldots, a_{n-1}) \mid a_i \in A\}$, the set of n-tuples over A

code of length n **over** A: a subset of A^n

codeword: element of a code

A distance function is usually defined on A^n

Example: Hamming distance between two n-tuples $a = (a_0, a_1, \ldots, a_{n-1})$ and $b = (b_0, b_1, \ldots, b_{n-1})$:

$$d_H(a, b) := \#\{i \mid a_i \neq b_i\}$$

Coding theory: Background

Let A be a set of symbols, $n \in \mathbb{N}$

$A^n := \{(a_0, a_1, \ldots, a_{n-1}) \mid a_i \in A\}$, the set of n-tuples over A

code of length n **over** A: a subset of A^n

codeword: element of a code

A distance function is usually defined on A^n

Example: Hamming distance between two n-tuples $a = (a_0, a_1, \ldots, a_{n-1})$ and $b = (b_0, b_1, \ldots, b_{n-1})$:

$$d_H(a, b) := \#\{i \mid a_i \neq b_i\}$$

Coding theory: Background

Let A be a set of symbols, $n \in \mathbb{N}$

$A^n := \{(a_0, a_1, \ldots, a_{n-1}) \mid a_i \in A\}$, the set of n-tuples over A

code of length n **over** A: a subset of A^n

codeword: element of a code

A distance function is usually defined on A^n

Example: Hamming distance between two n-tuples $a = (a_0, a_1, \ldots, a_{n-1})$ and $b = (b_0, b_1, \ldots, b_{n-1})$:

$$d_H(a, b) := \#\{i \mid a_i \neq b_i\}$$

Coding theory: Background

Let A be a set of symbols, $n \in \mathbb{N}$

$A^n := \{(a_0, a_1, \ldots, a_{n-1}) \mid a_i \in A\}$, the set of n-tuples over A

code of length n over A: a subset of A^n

codeword: element of a code

A distance function is usually defined on A^n

Example: Hamming distance between two n-tuples
$a = (a_0, a_1, \ldots, a_{n-1})$ and $b = (b_0, b_1, \ldots, b_{n-1})$:

$$d_H(a, b) := \#\{i \mid a_i \neq b_i\}$$

Coding theory: Background

Parameters of a code: An $(n, k, d)_A$-code is a code over A with

- length n
- size k
- minimum distance d

The goal of coding theory in engineering is the construction of codes with

- small n
- large k
- large d

These are incompatible goals!

Coding theory: Background

Parameters of a code: An $(n, k, d)_A$-code is a code over A with

- length n
- size k
- minimum distance d

The goal of coding theory in engineering is the construction of codes with

- small n
- large k
- large d

These are incompatible goals!

Coding theory: Background

Parameters of a code: An $(n, k, d)_A$-code is a code over A with

- length n
- size k
- minimum distance d

The goal of coding theory in engineering is the construction of codes with

- small n
- large k
- large d

These are incompatible goals!

Coding theory: Background

Parameters of a code: An $(n, k, d)_A$-code is a code over A with

- length n
- size k
- minimum distance d

The goal of coding theory in engineering is the construction of codes with

- small n
- large k
- large d

These are incompatible goals!

Coding theory: Background

Parameters of a code: An $(n, k, d)_A$-code is a code over A with

- length n
- size k
- minimum distance d

The goal of coding theory in engineering is the construction of codes with

- small n
- large k
- large d

These are incompatible goals!

Coding theory: Background

Parameters of a code: An $(n, k, d)_A$-code is a code over A with

- length n
- size k
- minimum distance d

The goal of coding theory in engineering is the construction of codes with

- small n
- large k
- large d

These are incompatible goals!

Codes over fields

The traditional setting for codes: Galois fields $\mathbb{F}_q := GF(q)$

A **(linear) code** of length n over $\mathbb{F}_q$: a subspace of $\mathbb{F}_q^n$

Examples: Binary codes
$(2^4, 2^{11}, 4)$ Reed-Muller
$(2^4, 2^8, 6)$ Nordstrom-Robinson (a non-linear binary code)

Codes over fields

The traditional setting for codes: Galois fields $\mathbb{F}_q := GF(q)$

A **(linear) code** of length n over $\mathbb{F}_q$: a subspace of $\mathbb{F}_q^n$

Examples: Binary codes
$(2^4, 2^{11}, 4)$ Reed-Muller
$(2^4, 2^8, 6)$ Nordstrom-Robinson (a non-linear binary code)

Codes over fields

The traditional setting for codes: Galois fields $\mathbb{F}_q := GF(q)$

A **(linear) code** of length n over $\mathbb{F}_q$: a subspace of $\mathbb{F}_q^n$

Examples: Binary codes
$(2^4, 2^{11}, 4)$ Reed-Muller
$(2^4, 2^8, 6)$ Nordstrom-Robinson (a non-linear binary code)

Codes over fields

The traditional setting for codes: Galois fields $\mathbb{F}_q := GF(q)$

A **(linear) code** of length n over $\mathbb{F}_q$: a subspace of $\mathbb{F}_q^n$

Examples: Binary codes
$(2^4, 2^{11}, 4)$ Reed-Muller
$(2^4, 2^8, 6)$ Nordstrom-Robinson (a non-linear binary code)

Codes over finite rings

Generalizations of Nordstrom-Robinson code: Preparata, Kerdock codes, etc.

Recent interest in codes over **rings** is due to the discovery that certain non-linear binary codes can be constructed as images of codes over the finite ring $\mathbb{Z}_4 := \mathbb{Z}/4\mathbb{Z}$.

Definition. The *Gray map* $\phi : \mathbb{Z}_4 \longrightarrow \mathbb{Z}_2^2$ is given by

$$0 \longmapsto 00, \; 1 \longmapsto 01, \; 2 \longmapsto 11, \; 3 \longmapsto 10.$$

We can extend this to $\phi : \mathbb{Z}_4^n \longmapsto\longrightarrow \mathbb{Z}_2^{2n}$.

Codes over finite rings

Generalizations of Nordstrom-Robinson code: Preparata, Kerdock codes, etc.

Recent interest in codes over **rings** is due to the discovery that certain non-linear binary codes can be constructed as images of codes over the finite ring $\mathbb{Z}_4 := \mathbb{Z}/4\mathbb{Z}$.

Definition. The *Gray map* $\phi : \mathbb{Z}_4 \longrightarrow \mathbb{Z}_2^2$ is given by

$$0 \longmapsto 00, \ 1 \longmapsto 01, \ 2 \longmapsto 11, \ 3 \longmapsto 10.$$

We can extend this to $\phi : \mathbb{Z}_4^n \longmapsto\longrightarrow \mathbb{Z}_2^{2n}$.

Codes over finite rings

Generalizations of Nordstrom-Robinson code: Preparata, Kerdock codes, etc.

Recent interest in codes over **rings** is due to the discovery that certain non-linear binary codes can be constructed as images of codes over the finite ring $\mathbb{Z}_4 := \mathbb{Z}/4\mathbb{Z}$.

Definition. The *Gray map* $\phi : \mathbb{Z}_4 \longrightarrow \mathbb{Z}_2^2$ is given by

$$0 \longmapsto 00, \; 1 \longmapsto 01, \; 2 \longmapsto 11, \; 3 \longmapsto 10.$$

We can extend this to $\phi : \mathbb{Z}_4^n \longmapsto\longrightarrow \mathbb{Z}_2^{2n}$.

Codes over finite rings

Generalizations of Nordstrom-Robinson code: Preparata, Kerdock codes, etc.

Recent interest in codes over **rings** is due to the discovery that certain non-linear binary codes can be constructed as images of codes over the finite ring $\mathbb{Z}_4 := \mathbb{Z}/4\mathbb{Z}$.

Definition. The *Gray map* $\phi : \mathbb{Z}_4 \longrightarrow \mathbb{Z}_2^2$ is given by

$$0 \longmapsto 00, \; 1 \longmapsto 01, \; 2 \longmapsto 11, \; 3 \longmapsto 10.$$

We can extend this to $\phi : \mathbb{Z}_4^n \longmapsto\longrightarrow \mathbb{Z}_2^{2n}$.

Codes over finite rings

Theorem. *(Hammons, Kumar, Calderbank, Sloane and Solé, 1992)* Let $(\mathcal{O})$ be the linear $(2, 256, 6)_{\mathbb{Z}_4}$ code with generator matrix

$$G = \begin{bmatrix} 3 & 3 & 2 & 3 & 1 & 0 & 0 & 0 \\ 3 & 0 & 3 & 2 & 3 & 1 & 0 & 0 \\ 3 & 0 & 0 & 3 & 2 & 3 & 1 & 0 \\ 3 & 0 & 0 & 0 & 3 & 2 & 3 & 1 \end{bmatrix}.$$

Then $\phi((\mathcal{O}) =$ Nordstrom-Robinson code. The non-linear binary codes are Gray map images of linear codes over $\mathbb{Z}_4$. There has been a lot of interest in codes over finite rings these

last 15 years.

Codes over finite rings

Theorem. *(Hammons, Kumar, Calderbank, Sloane and Solé, 1992)* Let $(\mathcal{O})$ be the linear $(2, 256, 6)_{\mathbb{Z}_4}$ code with generator matrix

$$G = \begin{bmatrix} 3 & 3 & 2 & 3 & 1 & 0 & 0 & 0 \\ 3 & 0 & 3 & 2 & 3 & 1 & 0 & 0 \\ 3 & 0 & 0 & 3 & 2 & 3 & 1 & 0 \\ 3 & 0 & 0 & 0 & 3 & 2 & 3 & 1 \end{bmatrix}.$$

Then $\phi((\mathcal{O}) =$ Nordstrom-Robinson code. The non-linear binary codes are Gray map images of linear codes over $\mathbb{Z}_4$. There has been a lot of interest in codes over finite rings these

last 15 years.

Codes over finite rings

Theorem. *(Hammons, Kumar, Calderbank, Sloane and Solé, 1992)* Let $(\mathcal{O})$ be the linear $(2, 256, 6)_{\mathbb{Z}_4}$ code with generator matrix

$$G = \begin{bmatrix} 3 & 3 & 2 & 3 & 1 & 0 & 0 & 0 \\ 3 & 0 & 3 & 2 & 3 & 1 & 0 & 0 \\ 3 & 0 & 0 & 3 & 2 & 3 & 1 & 0 \\ 3 & 0 & 0 & 0 & 3 & 2 & 3 & 1 \end{bmatrix}.$$

Then $\phi((\mathcal{O}) =$ Nordstrom-Robinson code. The non-linear binary codes are Gray map images of linear codes over $\mathbb{Z}_4$. There has been a lot of interest in codes over finite rings these

last 15 years.

Codes over finite rings

Theorem. *(Hammons, Kumar, Calderbank, Sloane and Solé, 1992)* Let $(\mathcal{O})$ be the linear $(2, 256, 6)_{\mathbb{Z}_4}$ code with generator matrix

$$G = \begin{bmatrix} 3 & 3 & 2 & 3 & 1 & 0 & 0 & 0 \\ 3 & 0 & 3 & 2 & 3 & 1 & 0 & 0 \\ 3 & 0 & 0 & 3 & 2 & 3 & 1 & 0 \\ 3 & 0 & 0 & 0 & 3 & 2 & 3 & 1 \end{bmatrix}.$$

Then $\phi((\mathcal{O}) =$ Nordstrom-Robinson code. The non-linear binary codes are Gray map images of linear codes over $\mathbb{Z}_4$.
There has been a lot of interest in codes over finite rings these

last 15 years.

Codes over finite rings

Theorem. *(Hammons, Kumar, Calderbank, Sloane and Solé, 1992)* Let $(\mathcal{O})$ be the linear $(2, 256, 6)_{\mathbb{Z}_4}$ code with generator matrix

$$G = \begin{bmatrix} 3 & 3 & 2 & 3 & 1 & 0 & 0 & 0 \\ 3 & 0 & 3 & 2 & 3 & 1 & 0 & 0 \\ 3 & 0 & 0 & 3 & 2 & 3 & 1 & 0 \\ 3 & 0 & 0 & 0 & 3 & 2 & 3 & 1 \end{bmatrix}.$$

Then $\phi((\mathcal{O}) =$ Nordstrom-Robinson code. The non-linear binary codes are Gray map images of linear codes over $\mathbb{Z}_4$. There has been a lot of interest in codes over finite rings these

last 15 years.

Codes over rings

Definition. Let R be a finite ring. (e.g. $\mathbb{Z}_m := \mathbb{Z}/m\mathbb{Z}$)

1) *code*: an R-submodule of $R^n := \{(x_1, x_2, \ldots, x_n) \mid x_i \in R\}$

2) *codeword*: element of a code

3) Two vectors $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n)$ are *orthogonal* if their Euclidean inner product is zero. i.e.

$$x \cdot y = \sum_i x_i y_i = 0$$

Codes over rings

Definition. Let R be a finite ring. (e.g. $\mathbb{Z}_m := \mathbb{Z}/m\mathbb{Z}$)

1) *code*: an R-submodule of $R^n := \{(x_1, x_2, \ldots, x_n) \mid x_i \in R\}$

2) *codeword*: element of a code

3) Two vectors $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n)$ are *orthogonal* if their Euclidean inner product is zero. i.e.

$$x \cdot y = \sum_i x_i y_i = 0$$

Codes over rings

Definition. Let R be a finite ring. (e.g. $\mathbb{Z}_m := \mathbb{Z}/m\mathbb{Z}$)

1) *code*: an R-submodule of $R^n := \{(x_1, x_2, \ldots, x_n) \mid x_i \in R\}$
2) *codeword*: element of a code
3) Two vectors $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n)$ are *orthogonal* if their Euclidean inner product is zero. i.e.

$$x \cdot y = \sum_i x_i y_i = 0$$

Codes over rings

Definition. Let R be a finite ring. (e.g. $\mathbb{Z}_m := \mathbb{Z}/m\mathbb{Z}$)

1) *code*: an R-submodule of $R^n := \{(x_1, x_2, \ldots, x_n) \mid x_i \in R\}$
2) *codeword*: element of a code
3) Two vectors $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n)$ are *orthogonal* if their Euclidean inner product is zero. i.e.

$$x \cdot y = \sum_i x_i y_i = 0$$

Self-dual codes

Definition. Let $\mathcal{C}$ be a code over a ring R.

1) *dual* of $\mathcal{C}$:

$$\mathcal{C}^{\perp} := \{y \in R^n \mid x \cdot y = 0, \forall x \in \mathcal{C}\}$$

(Remark: $\mathcal{C}^{\perp}$ is a code.)

2) If $\mathcal{C} \subseteq \mathcal{C}^{\perp}$, $\mathcal{C}$ is *self-orthogonal*.
3) If $\mathcal{C} = \mathcal{C}^{\perp}$, $\mathcal{C}$ is *self-dual*.

Self-dual codes

Definition. Let $\mathcal{C}$ be a code over a ring R.

1) *dual* of $\mathcal{C}$:

$$\mathcal{C}^{\perp} := \{y \in R^n \mid x \cdot y = 0, \forall x \in \mathcal{C}\}$$

(Remark: $\mathcal{C}^{\perp}$ is a code.)

2) If $\mathcal{C} \subseteq \mathcal{C}^{\perp}$, $\mathcal{C}$ is *self-orthogonal*.

3) If $\mathcal{C} = \mathcal{C}^{\perp}$, $\mathcal{C}$ is *self-dual*.

Self-dual codes

Definition. Let $\mathcal{C}$ be a code over a ring R.

1) *dual* of $\mathcal{C}$:

$$\mathcal{C}^{\perp} := \{y \in R^n \mid x \cdot y = 0, \forall x \in \mathcal{C}\}$$

(Remark: $\mathcal{C}^{\perp}$ is a code.)

2) If $\mathcal{C} \subseteq \mathcal{C}^{\perp}$, $\mathcal{C}$ is *self-orthogonal*.

3) If $\mathcal{C} = \mathcal{C}^{\perp}$, $\mathcal{C}$ is *self-dual*.

Self-dual codes

Definition. Let $\mathcal{C}$ be a code over a ring R.

1) *dual* of $\mathcal{C}$:

$$\mathcal{C}^{\perp} := \{y \in R^n \mid x \cdot y = 0, \forall x \in \mathcal{C}\}$$

(Remark: $\mathcal{C}^{\perp}$ is a code.)

2) If $\mathcal{C} \subseteq \mathcal{C}^{\perp}$, $\mathcal{C}$ is *self-orthogonal*.

3) If $\mathcal{C} = \mathcal{C}^{\perp}$, $\mathcal{C}$ is *self-dual*.

Self-dual codes

Definition. Let $\mathcal{C}$ be a code over a ring R.

1) *dual* of $\mathcal{C}$:

$$\mathcal{C}^{\perp} := \{y \in R^n \mid x \cdot y = 0, \forall x \in \mathcal{C}\}$$

(Remark: $\mathcal{C}^{\perp}$ is a code.)

2) If $\mathcal{C} \subseteq \mathcal{C}^{\perp}$, $\mathcal{C}$ is *self-orthogonal*.
3) If $\mathcal{C} = \mathcal{C}^{\perp}$, $\mathcal{C}$ is *self-dual*.

Self-dual codes

Definition. Let $\mathcal{C}$ be a code over a ring R.

1) *dual* of $\mathcal{C}$:

$$\mathcal{C}^{\perp} := \{y \in R^n \mid x \cdot y = 0, \forall x \in \mathcal{C}\}$$

(Remark: $\mathcal{C}^{\perp}$ is a code.)

2) If $\mathcal{C} \subseteq \mathcal{C}^{\perp}$, $\mathcal{C}$ is *self-orthogonal*.
3) If $\mathcal{C} = \mathcal{C}^{\perp}$, $\mathcal{C}$ is *self-dual*.

Equivalent codes

Two codes of same length over $\mathbb{Z}_{p^s}$ are *equivalent* if one can be obtained from the other by permutation of coordinates, possibly followed by multiplication of some coordinates by -1.

$\mathcal{C}_1 \approx \mathcal{C}_2 \iff \exists\ n \times n$ matrix P such that

$$\mathcal{C}_1 = \mathcal{C}_2 P := \{cP \mid c \in \mathcal{C}_2\}$$

where P has exactly one entry ± 1 in every row and in every column and all other entries are zero.

Equivalent codes

Two codes of same length over $\mathbb{Z}_{p^s}$ are *equivalent* if one can be obtained from the other by permutation of coordinates, possibly followed by multiplication of some coordinates by -1.

$\mathcal{C}_1 \approx \mathcal{C}_2 \iff \exists\ n \times n$ matrix P such that

$$\mathcal{C}_1 = \mathcal{C}_2 P := \{cP \mid c \in \mathcal{C}_2\}$$

where P has exactly one entry ± 1 in every row and in every column and all other entries are zero.

Counting the number of codes

The number of codes *equivalent* to a code $\mathcal{C}$ of length n is

$$\frac{|E_n|}{|Aut(\mathcal{C})|},$$

where E_n is the group of all sign-permutations and *Aut($\mathcal{C}$)* is the automorphism group of $\mathcal{C}$, i.e. the group of all sign-permutations that send $\mathcal{C}$ to itself. Thus the number of *distinct* self-dual codes over $\mathbb{Z}_{p^s}$ of length n is given by

$$N_{p^s}(n) = \sum_{\mathcal{C}} \frac{2^n n!}{|Aut(\mathcal{C})|},$$

where the sum runs over all inequivalent self-dual codes $\mathcal{C}$. We wish to find a more explicit formula for $N_{p^s}(n)$. This is called the **mass formula**.

Counting the number of codes

The number of codes *equivalent* to a code $\mathcal{C}$ of length n is

$$\frac{|E_n|}{|Aut(\mathcal{C})|},$$

where E_n is the group of all sign-permutations and $Aut(\mathcal{C})$ is the automorphism group of $\mathcal{C}$, i.e. the group of all sign-permutations that send $\mathcal{C}$ to itself. Thus the number of *distinct* self-dual codes over $\mathbb{Z}_{p^s}$ of length n is given by

$$N_{p^s}(n) = \sum_{\mathcal{C}} \frac{2^n n!}{|Aut(\mathcal{C})|},$$

where the sum runs over all inequivalent self-dual codes $\mathcal{C}$. We wish to find a more explicit formula for $N_{p^s}(n)$. This is called the **mass formula**.

Counting the number of codes

The number of codes *equivalent* to a code $\mathcal{C}$ of length n is

$$\frac{|E_n|}{|Aut(\mathcal{C})|},$$

where E_n is the group of all sign-permutations and $Aut(\mathcal{C})$ is the automorphism group of $\mathcal{C}$, i.e. the group of all sign-permutations that send $\mathcal{C}$ to itself. Thus the number of *distinct* self-dual codes over $\mathbb{Z}_{p^s}$ of length n is given by

$$N_{p^s}(n) = \sum_{\mathcal{C}} \frac{2^n n!}{|Aut(\mathcal{C})|},$$

where the sum runs over all inequivalent self-dual codes $\mathcal{C}$. We wish to find a more explicit formula for $N_{p^s}(n)$. This is called the **mass formula**.

Counting the number of codes

The number of codes *equivalent* to a code $\mathcal{C}$ of length n is

$$\frac{|E_n|}{|Aut(\mathcal{C})|},$$

where E_n is the group of all sign-permutations and *Aut*($\mathcal{C}$) is the automorphism group of $\mathcal{C}$, i.e. the group of all sign-permutations that send $\mathcal{C}$ to itself. Thus the number of *distinct* self-dual codes over $\mathbb{Z}_{p^s}$ of length n is given by

$$N_{p^s}(n) = \sum_{\mathcal{C}} \frac{2^n n!}{|Aut(\mathcal{C})|},$$

where the sum runs over all inequivalent self-dual codes $\mathcal{C}$. We wish to find a more explicit formula for $N_{p^s}(n)$. This is called the **mass formula**.

Counting the number of codes

The number of codes *equivalent* to a code $\mathcal{C}$ of length n is

$$\frac{|E_n|}{|Aut(\mathcal{C})|},$$

where E_n is the group of all sign-permutations and $Aut(\mathcal{C})$ is the automorphism group of $\mathcal{C}$, i.e. the group of all sign-permutations that send $\mathcal{C}$ to itself. Thus the number of *distinct* self-dual codes over $\mathbb{Z}_{p^s}$ of length n is given by

$$N_{p^s}(n) = \sum_{\mathcal{C}} \frac{2^n n!}{|Aut(\mathcal{C})|},$$

where the sum runs over all inequivalent self-dual codes $\mathcal{C}$. We wish to find a more explicit formula for $N_{p^s}(n)$. This is called the **mass formula.**

What is it for?

The mass formula

$$N_{p^s}(n) = \sum_{\mathcal{C}} \frac{|E_n|}{|Aut(\mathcal{C})|},$$

is important for the computation of the number of inequivalent classes of self-dual codes over $\mathbb{Z}_{p^s}$ and the classification of such codes,...

... and hence, of codes over $\mathbb{Z}_m$.

What is it for?

The mass formula

$$N_{p^s}(n) = \sum_{\mathcal{C}} \frac{|E_n|}{|Aut(\mathcal{C})|},$$

is important for the computation of the number of inequivalent classes of self-dual codes over $\mathbb{Z}_{p^s}$ and the classification of such codes,...
... and hence, of codes over $\mathbb{Z}_m$.

Mass formulas for $\mathbb{Z}_{p^s}$

- In 1993, Conway and Sloane classified all self-dual codes over $\mathbb{Z}_4$ up to length $n = 9$, without the aid of a mass formula.
- Mass formula for self-dual codes over $\mathbb{Z}_4$ (Gaborit. *IEEE Transactions Information Theory*, 1996)
- Classification of all self-dual $\mathbb{Z}_4$-codes with $n \leq 15$ (Fields, Gaborit, Leon, Pless. *IEEE Transactions Information Theory*, 1998)

Mass formulas for $\mathbb{Z}_{p^s}$

- In 1993, Conway and Sloane classified all self-dual codes over $\mathbb{Z}_4$ up to length $n = 9$, without the aid of a mass formula.
- Mass formula for self-dual codes over $\mathbb{Z}_4$ (Gaborit. *IEEE Transactions Information Theory*, 1996)
- Classification of all self-dual $\mathbb{Z}_4$-codes with $n \leq 15$ (Fields, Gaborit, Leon, Pless. *IEEE Transactions Information Theory*, 1998)

Mass formulas for $\mathbb{Z}_{p^s}$

- In 1993, Conway and Sloane classified all self-dual codes over $\mathbb{Z}_4$ up to length $n = 9$, without the aid of a mass formula.
- Mass formula for self-dual codes over $\mathbb{Z}_4$ (Gaborit. *IEEE Transactions Information Theory*, 1996)
- Classification of all self-dual $\mathbb{Z}_4$-codes with $n \leq 15$ (Fields, Gaborit, Leon, Pless. *IEEE Transactions Information Theory*, 1998)

Mass formulas for $\mathbb{Z}_{p^s}$

- Mass formula for self-dual codes over $\mathbb{Z}_{p^2}$, odd prime p: Balmaceda, Betty, Nemenzo. *Discrete Mathematics* (to appear).
  Theorem. Let p be an odd prime. If $N_{p^2}(n)$ is the number of distinct self-dual codes over $\mathbb{Z}_{p^2}$ of length n then
  $$N_{p^2}(n) = \sum_{0 \le k \le \lfloor \frac{n}{2} \rfloor} \sigma_p(n,k)\, p^{\frac{k(k-1)}{2}},$$
  where $\sigma_p(n,k)$ is the number of distinct self-orthogonal codes over $\mathbf{F}_p$ of dimension k.
- Classification of all self-dual codes over $\mathbb{Z}_9$ (for lengths $n \le 8$ for $\mathbb{Z}_9$, $n \le 7$ for $\mathbb{Z}_{25}$ and $n \le 6$ for $\mathbb{Z}_{49}$)

Mass formulas for $\mathbb{Z}_{p^s}$

- Mass formula for self-dual codes over $\mathbb{Z}_{p^2}$, odd prime p: Balmaceda, Betty, Nemenzo. *Discrete Mathematics* (to appear).

  Theorem. Let p be an odd prime. If $N_{p^2}(n)$ is the number of distinct self-dual codes over $\mathbb{Z}_{p^2}$ of length n then

  $$N_{p^2}(n) = \sum_{0 \leq k \leq \lfloor \frac{n}{2} \rfloor} \sigma_p(n,k)\, p^{\frac{k(k-1)}{2}},$$

  where $\sigma_p(n,k)$ is the number of distinct self-orthogonal codes over $\mathbf{F}_p$ of dimension k.

- Classification of all self-dual codes over $\mathbb{Z}_9$ (for lengths $n \leq 8$ for $\mathbb{Z}_9$, $n \leq 7$ for $\mathbb{Z}_{25}$ and $n \leq 6$ for $\mathbb{Z}_{49}$)

Mass formulas for $\mathbb{Z}_{p^s}$

- Mass formula for self-dual codes over $\mathbb{Z}_{p^2}$, odd prime p: Balmaceda, Betty, Nemenzo. *Discrete Mathematics* (to appear).
  Theorem. Let p be an odd prime. If $N_{p^2}(n)$ is the number of distinct self-dual codes over $\mathbb{Z}_{p^2}$ of length n then

$$N_{p^2}(n) = \sum_{0 \le k \le \lfloor \frac{n}{2} \rfloor} \sigma_p(n,k)\, p^{\frac{k(k-1)}{2}},$$

  where $\sigma_p(n,k)$ is the number of distinct self-orthogonal codes over $\mathbf{F}_p$ of dimension k.
- Classification of all self-dual codes over $\mathbb{Z}_9$ (for lengths $n \le 8$ for $\mathbb{Z}_9$, $n \le 7$ for $\mathbb{Z}_{25}$ and $n \le 6$ for $\mathbb{Z}_{49}$)

Mass formulas for $\mathbb{Z}_{p^s}$

- Mass formula for self-dual codes over $\mathbb{Z}_{p^2}$, odd prime p: Balmaceda, Betty, Nemenzo. *Discrete Mathematics* (to appear).
  Theorem. Let p be an odd prime. If $N_{p^2}(n)$ is the number of distinct self-dual codes over $\mathbb{Z}_{p^2}$ of length n then

$$N_{p^2}(n) = \sum_{0 \le k \le \lfloor \frac{n}{2} \rfloor} \sigma_p(n,k)\, p^{\frac{k(k-1)}{2}},$$

  where $\sigma_p(n,k)$ is the number of distinct self-orthogonal codes over $\mathbf{F}_p$ of dimension k.

- Classification of all self-dual codes over $\mathbb{Z}_9$ (for lengths $n \le 8$ for $\mathbb{Z}_9$, $n \le 7$ for $\mathbb{Z}_{25}$ and $n \le 6$ for $\mathbb{Z}_{49}$)

How is classification done?

To count the number of inequivalent codes of given length n:

1. Set $SUM = 0$
2. Find a self-dual code $\mathcal{C}_1$ of length n
3. Compute $|Aut(\mathcal{C}_1)|$, $SUM = SUM + \frac{2^n n!}{|Aut(\mathcal{C}_1)|}$
4. For every $j = 2, 3, \ldots$, find a self-dual code $\mathcal{C}_j$, not equivalent to $\mathcal{C}_1, \ldots, \mathcal{C}_{j-1}$, and compute $|Aut(\mathcal{C}_j)|$, and $SUM = SUM + \frac{2^n n!}{|Aut(\mathcal{C}_1)|}$
5. Compare SUM to mass formula. If $SUM <$ mass formula, go to step (4); if $SUM =$ mass formula, done.

How is classification done?

To count the number of inequivalent codes of given length n:

1. Set $SUM = 0$
2. Find a self-dual code $\mathcal{C}_1$ of length n
3. Compute $|Aut(\mathcal{C}_1)|$, $SUM = SUM + \frac{2^n n!}{|Aut(\mathcal{C}_1)|}$
4. For every $j = 2, 3, \ldots$, find a self-dual code $\mathcal{C}_j$, not equivalent to $\mathcal{C}_1, \ldots, \mathcal{C}_{j-1}$, and compute $|Aut(\mathcal{C}_j)|$, and $SUM = SUM + \frac{2^n n!}{|Aut(\mathcal{C}_1)|}$
5. Compare SUM to mass formula. If $SUM <$ mass formula, go to step (4); if $SUM =$ mass formula, done.

How is classification done?

To count the number of inequivalent codes of given length n:

1. Set $SUM = 0$
2. Find a self-dual code $\mathcal{C}_1$ of length n
3. Compute $|Aut(\mathcal{C}_1)|$, $SUM = SUM + \frac{2^n n!}{|Aut(\mathcal{C}_1)|}$
4. For every $j = 2, 3, \ldots$, find a self-dual code $\mathcal{C}_j$, not equivalent to $\mathcal{C}_1, \ldots, \mathcal{C}_{j-1}$, and compute $|Aut(\mathcal{C}_j)|$, and $SUM = SUM + \frac{2^n n!}{|Aut(\mathcal{C}_1)|}$
5. Compare SUM to mass formula. If $SUM <$ mass formula, go to step (4); if $SUM =$ mass formula, done.

How is classification done?

To count the number of inequivalent codes of given length n:

1. Set $SUM = 0$
2. Find a self-dual code $\mathcal{C}_1$ of length n
3. Compute $|Aut(\mathcal{C}_1)|$, $SUM = SUM + \frac{2^n n!}{|Aut(\mathcal{C}_1)|}$
4. For every $j = 2, 3, \ldots$, find a self-dual code $\mathcal{C}_j$, not equivalent to $\mathcal{C}_1, \ldots, \mathcal{C}_{j-1}$, and compute $|Aut(\mathcal{C}_j)|$, and $SUM = SUM + \frac{2^n n!}{|Aut(\mathcal{C}_1)|}$
5. Compare SUM to mass formula. If $SUM <$ mass formula, go to step (4); if $SUM =$ mass formula, done.

How is classification done?

To count the number of inequivalent codes of given length n:

1. Set $SUM = 0$
2. Find a self-dual code $\mathcal{C}_1$ of length n
3. Compute $|Aut(\mathcal{C}_1)|$, $SUM = SUM + \frac{2^n n!}{|Aut(\mathcal{C}_1)|}$
4. For every $j = 2, 3, \ldots$, find a self-dual code $\mathcal{C}_j$, not equivalent to $\mathcal{C}_1, \ldots, \mathcal{C}_{j-1}$, and compute $|Aut(\mathcal{C}_j)|$, and $SUM = SUM + \frac{2^n n!}{|Aut(\mathcal{C}_1)|}$
5. Compare SUM to mass formula. If $SUM <$ mass formula, go to step (4); if $SUM =$ mass formula, done.

How is classification done?

To count the number of inequivalent codes of given length n:

1. Set $SUM = 0$
2. Find a self-dual code $\mathcal{C}_1$ of length n
3. Compute $|Aut(\mathcal{C}_1)|$, $SUM = SUM + \frac{2^n n!}{|Aut(\mathcal{C}_1)|}$
4. For every $j = 2, 3, \ldots$, find a self-dual code $\mathcal{C}_j$, not equivalent to $\mathcal{C}_1, \ldots, \mathcal{C}_{j-1}$, and compute $|Aut(\mathcal{C}_j)|$, and $SUM = SUM + \frac{2^n n!}{|Aut(\mathcal{C}_1)|}$
5. Compare SUM to mass formula. If $SUM <$ mass formula, go to step (4); if $SUM =$ mass formula, done.

An example

Classify self-dual codes of length $n = 8$ over $\mathbb{Z}_9$:

$$
\begin{aligned}
N_9(8) &= \sum_{0 \le k \le 4} \sigma_3(8,k) 3^{\frac{k(k-1)}{2}} \\
&= 1 + 1120 + 36400 \cdot 3 + 44800 \cdot 3^3 + 2240 \cdot 3^6 \\
&= \mathbf{2952881}
\end{aligned}
$$

We can also compute

$$
\begin{aligned}
\sum \frac{2^8 8!}{|Aut(\mathcal{C})|} &= 1 + 224 + 4480 + 20160 + 26880 + 1680 \\
&\quad +896 + 8960 + 53760 + 215040 + 40320 \\
&\quad +322560 + 645120 + 645120 + 322560 + 645120 \\
&= \mathbf{2952881}
\end{aligned}
$$

Therefore there are 16 inequivalent self-dual codes of length 8 over $\mathbb{Z}_9$.

An example

Classify self-dual codes of length $n = 8$ over $\mathbb{Z}_9$:

$$\begin{aligned} N_9(8) &= \sum_{0 \le k \le 4} \sigma_3(8, k) 3^{\frac{k(k-1)}{2}} \\ &= 1 + 1120 + 36400 \cdot 3 + 44800 \cdot 3^3 + 2240 \cdot 3^6 \\ &= \mathbf{2952881} \end{aligned}$$

We can also compute

$$\begin{aligned} \sum \frac{2^8 8!}{|Aut(\mathcal{C})|} &= 1 + 224 + 4480 + 20160 + 26880 + 1680 \\ &\quad +896 + 8960 + 53760 + 215040 + 40320 \\ &\quad +322560 + 645120 + 645120 + 322560 + 645120 \\ &= \mathbf{2952881} \end{aligned}$$

Therefore there are 16 inequivalent self-dual codes of length 8 over $\mathbb{Z}_9$.

An example

Classify self-dual codes of length $n = 8$ over $\mathbb{Z}_9$:

$$\begin{aligned} N_9(8) &= \sum_{0 \le k \le 4} \sigma_3(8,k) 3^{\frac{k(k-1)}{2}} \\ &= 1 + 1120 + 36400 \cdot 3 + 44800 \cdot 3^3 + 2240 \cdot 3^6 \\ &= \mathbf{2952881} \end{aligned}$$

We can also compute

$$\begin{aligned} \sum \frac{2^8 8!}{|Aut(\mathcal{C})|} &= 1 + 224 + 4480 + 20160 + 26880 + 1680 \\ &\quad +896 + 8960 + 53760 + 215040 + 40320 \\ &\quad +322560 + 645120 + 645120 + 322560 + 645120 \\ &= \mathbf{2952881} \end{aligned}$$

Therefore there are 16 inequivalent self-dual codes of length 8 over $\mathbb{Z}_9$.

An example

Classify self-dual codes of length $n = 8$ over $\mathbb{Z}_9$:

$$
\begin{aligned}
N_9(8) &= \sum_{0 \le k \le 4} \sigma_3(8,k) 3^{\frac{k(k-1)}{2}} \\
&= 1 + 1120 + 36400 \cdot 3 + 44800 \cdot 3^3 + 2240 \cdot 3^6 \\
&= \mathbf{2952881}
\end{aligned}
$$

We can also compute

$$
\begin{aligned}
\sum \frac{2^8 8!}{|Aut(\mathcal{C})|} &= 1 + 224 + 4480 + 20160 + 26880 + 1680 \\
&\quad +896 + 8960 + 53760 + 215040 + 40320 \\
&\quad +322560 + 645120 + 645120 + 322560 + 645120 \\
&= \mathbf{2952881}
\end{aligned}
$$

Therefore there are 16 inequivalent self-dual codes of length 8 over $\mathbb{Z}_9$.

An example

Classify self-dual codes of length $n = 8$ over $\mathbb{Z}_9$:

$$\begin{aligned} N_9(8) &= \sum_{0 \le k \le 4} \sigma_3(8,k) 3^{\frac{k(k-1)}{2}} \\ &= 1 + 1120 + 36400 \cdot 3 + 44800 \cdot 3^3 + 2240 \cdot 3^6 \\ &= \mathbf{2952881} \end{aligned}$$

We can also compute

$$\begin{aligned} \sum \frac{2^8 8!}{|Aut(\mathcal{C})|} &= 1 + 224 + 4480 + 20160 + 26880 + 1680 \\ &\quad +896 + 8960 + 53760 + 215040 + 40320 \\ &\quad +322560 + 645120 + 645120 + 322560 + 645120 \\ &= \mathbf{2952881} \end{aligned}$$

Therefore there are 16 inequivalent self-dual codes of length 8 over $\mathbb{Z}_9$.

An example

Classify self-dual codes of length $n = 8$ over $\mathbb{Z}_9$:

$$\begin{aligned} N_9(8) &= \sum_{0 \le k \le 4} \sigma_3(8,k) 3^{\frac{k(k-1)}{2}} \\ &= 1 + 1120 + 36400 \cdot 3 + 44800 \cdot 3^3 + 2240 \cdot 3^6 \\ &= \mathbf{2952881} \end{aligned}$$

We can also compute

$$\begin{aligned} \sum \frac{2^8 8!}{|Aut(\mathcal{C})|} &= 1 + 224 + 4480 + 20160 + 26880 + 1680 \\ &\quad + 896 + 8960 + 53760 + 215040 + 40320 \\ &\quad + 322560 + 645120 + 645120 + 322560 + 645120 \\ &= \mathbf{2952881} \end{aligned}$$

Therefore there are 16 inequivalent self-dual codes of length 8 over $\mathbb{Z}_9$.

An example

Classify self-dual codes of length $n = 8$ over $\mathbb{Z}_9$:

$$\begin{aligned} N_9(8) &= \sum_{0 \le k \le 4} \sigma_3(8,k) 3^{\frac{k(k-1)}{2}} \\ &= 1 + 1120 + 36400 \cdot 3 + 44800 \cdot 3^3 + 2240 \cdot 3^6 \\ &= \mathbf{2952881} \end{aligned}$$

We can also compute

$$\begin{aligned} \sum \frac{2^8 8!}{|Aut(\mathcal{C})|} &= 1 + 224 + 4480 + 20160 + 26880 + 1680 \\ &\quad + 896 + 8960 + 53760 + 215040 + 40320 \\ &\quad + 322560 + 645120 + 645120 + 322560 + 645120 \\ &= \mathbf{2952881} \end{aligned}$$

Therefore there are 16 inequivalent self-dual codes of length 8 over $\mathbb{Z}_9$.

Codes over $\mathbb{Z}_{p^3}$, for primes p

A code $\mathcal{C}$ of length n over $\mathbb{Z}_{p^3}$ has a “generator matrix" which can be written as

$$G = \begin{bmatrix} I_k & A_2 & A_3 & A_4 \\ 0 & pI_l & pB_3 & pB_4 \\ 0 & 0 & p^2 I_m & p^2 C_4 \end{bmatrix} = \begin{bmatrix} A \\ pB \\ p^2 C \end{bmatrix}$$

I_i: $i \times i$identity matrix
$A_3 = A_{30} + pA_{31}$
$B_4 = B_{40} + pB_{41}$
$A_4 = A_{40} + pA_{41} + p^2 A_{42}$
A_2, B_3, C_4, A_{ij} and B_{ij} have entries from $\{0, 1, \ldots, p-1\}$
Columns have sizes k, l, m and h, with $n = k + l + m + h$.
$\mathcal{C}$ has $p^{3k+2l+m}$ codewords.

Codes over $\mathbb{Z}_{p^3}$, for primes p

A code $\mathcal{C}$ of length n over $\mathbb{Z}_{p^3}$ has a “generator matrix" which can be written as

$$G = \begin{bmatrix} I_k & A_2 & A_3 & A_4 \\ 0 & pI_l & pB_3 & pB_4 \\ 0 & 0 & p^2 I_m & p^2 C_4 \end{bmatrix} = \begin{bmatrix} A \\ pB \\ p^2 C \end{bmatrix}$$

I_i: $i \times i$identity matrix

$A_3 = A_{30} + pA_{31}$

$B_4 = B_{40} + pB_{41}$

$A_4 = A_{40} + pA_{41} + p^2 A_{42}$

A_2, B_3, C_4, A_{ij} and B_{ij} have entries from $\{0, 1, \ldots, p-1\}$

Columns have sizes k, l, m and h, with $n = k + l + m + h$.

$\mathcal{C}$ has $p^{3k+2l+m}$ codewords.

Codes over $\mathbb{Z}_{p^3}$, for primes p

A code $\mathcal{C}$ of length n over $\mathbb{Z}_{p^3}$ has a "generator matrix" which can be written as

$$G = \begin{bmatrix} I_k & A_2 & A_3 & A_4 \\ 0 & pI_l & pB_3 & pB_4 \\ 0 & 0 & p^2 I_m & p^2 C_4 \end{bmatrix} = \begin{bmatrix} A \\ pB \\ p^2 C \end{bmatrix}$$

I_i: $i \times i$identity matrix
$A_3 = A_{30} + pA_{31}$
$B_4 = B_{40} + pB_{41}$
$A_4 = A_{40} + pA_{41} + p^2 A_{42}$
A_2, B_3, C_4, A_{ij} and B_{ij} have entries from $\{0, 1, \ldots, p-1\}$
Columns have sizes k, l, m and h, with $n = k + l + m + h$.
$\mathcal{C}$ has $p^{3k+2l+m}$ codewords.

Codes over $\mathbb{Z}_{p^3}$, for primes p

A code $\mathcal{C}$ of length n over $\mathbb{Z}_{p^3}$ has a “generator matrix" which can be written as

$$G = \left[\begin{array}{cccc} I_k & A_2 & A_3 & A_4 \\ 0 & pI_l & pB_3 & pB_4 \\ 0 & 0 & p^2 I_m & p^2 C_4 \end{array} \right] = \left[\begin{array}{c} A \\ pB \\ p^2 C \end{array} \right]$$

I_i: $i \times i$identity matrix
$A_3 = A_{30} + pA_{31}$
$B_4 = B_{40} + pB_{41}$
$A_4 = A_{40} + pA_{41} + p^2 A_{42}$
A_2, B_3, C_4, A_{ij} and B_{ij} have entries from $\{0, 1, \ldots, p-1\}$
Columns have sizes k, l, m and h, with $n = k + l + m + h$.
$\mathcal{C}$ has $p^{3k+2l+m}$ codewords.

Codes over $\mathbb{Z}_{p^3}$, for primes p

A code $\mathcal{C}$ of length n over $\mathbb{Z}_{p^3}$ has a “generator matrix" which can be written as

$$G = \left[\begin{array}{cccc} I_k & A_2 & A_3 & A_4 \\ 0 & pI_l & pB_3 & pB_4 \\ 0 & 0 & p^2 I_m & p^2 C_4 \end{array}\right] = \left[\begin{array}{c} A \\ pB \\ p^2 C \end{array}\right]$$

I_i: $i \times i$identity matrix
$A_3 = A_{30} + pA_{31}$
$B_4 = B_{40} + pB_{41}$
$A_4 = A_{40} + pA_{41} + p^2 A_{42}$
A_2, B_3, C_4, A_{ij} and B_{ij} have entries from $\{0, 1, \ldots, p-1\}$
Columns have sizes k, l, m and h, with $n = k + l + m + h$.
$\mathcal{C}$ has $p^{3k+2l+m}$ codewords.

Self-dual codes over $\mathbb{Z}_{p^3}$

The dual code $\mathcal{C}^\perp$ is of type $\{h, m, l\}$ and has $p^{3h+2m+l}$ codewords.

Thus: whenever $\mathcal{C} = \mathcal{C}^\perp$, $k = h$ and $l = m$.

A self-dual code then is of even length $n = 2(k + l)$.

Self-dual codes over $\mathbb{Z}_{p^3}$

The dual code $\mathcal{C}^\perp$ is of type $\{h, m, l\}$ and has $p^{3h+2m+l}$ codewords.
Thus: whenever $\mathcal{C} = \mathcal{C}^\perp$, $k = h$ and $l = m$.
A self-dual code then is of even length $n = 2(k + l)$.

Self-dual codes over $\mathbb{Z}_{p^3}$

The dual code $\mathcal{C}^\perp$ is of type $\{h, m, l\}$ and has $p^{3h+2m+l}$ codewords.
Thus: whenever $\mathcal{C} = \mathcal{C}^\perp$, $k = h$ and $l = m$.
A self-dual code then is of even length $n = 2(k + l)$.

Self-dual codes over $\mathbb{Z}_{p^3}$

We can characterize self-dual codes:

Proposition. Let $\mathcal{C}$ be a code over $\mathbb{Z}_{p^3}$. Then $\mathcal{C}$ is a self-dual code if and only if $k = h$, $l = m$ and the following hold:

$$
\begin{aligned}
AA^t &\equiv 0 \pmod{p^3} &(1)\\
AB^t &\equiv 0 \pmod{p^2} &(2)\\
BB^t &\equiv 0 \pmod{p} &(3)\\
AC^t &\equiv 0 \pmod{p}. &(4)
\end{aligned}
$$

(We shall examine conditions (1)-(4) further, in terms of the matrices over $\mathbb{Z}_p$.)

Self-dual codes over $\mathbb{Z}_{p^3}$

We can characterize self-dual codes:

Proposition. Let $\mathcal{C}$ be a code over $\mathbb{Z}_{p^3}$. Then $\mathcal{C}$ is a self-dual code if and only if $k = h$, $l = m$ and the following hold:

$$\begin{aligned} AA^t &\equiv 0 \pmod{p^3} & (1)\\ AB^t &\equiv 0 \pmod{p^2} & (2)\\ BB^t &\equiv 0 \pmod{p} & (3)\\ AC^t &\equiv 0 \pmod{p}. & (4) \end{aligned}$$

(We shall examine conditions (1)-(4) further, in terms of the matrices over $\mathbb{Z}_p$.)

Constructing self-dual codes from below

Proposition. Let p be an odd prime. A self-dual code over $\mathbb{Z}_{p^3}$ can be induced from a self-dual code $\mathcal{C}_1$ over $\mathbb{Z}_p$; there are $p^{k(\frac{n}{2}-1)}$ self-dual codes over $\mathbb{Z}_{p^3}$ corresponding to each subspace of $\mathcal{C}_1$ of dimension k $(0 \leq k \leq \frac{n}{2})$.

Proposition. Define ε as follows: 1) if $\vec{1}_n \in A$ and $8 \mid n$, then $\varepsilon = 1$; 2) if $\vec{1}_n \notin A$, then $\varepsilon = 0$. Any self-dual code over $\mathbb{Z}_{2^3}$ is induced from a self-dual code $\mathcal{C}_1$ over $\mathbb{Z}_2$. There are $2^{kl+k^2+\varepsilon}$ self-dual codes over $\mathbb{Z}_{2^3}$ corresponding to each subspace of dimension k $(0 \leq k \leq \frac{n}{2})$ of $\mathcal{C}_1$.

Constructing self-dual codes from below

Proposition. Let p be an odd prime. A self-dual code over $\mathbb{Z}_{p^3}$ can be induced from a self-dual code $\mathcal{C}_1$ over $\mathbb{Z}_p$; there are $p^{k(\frac{n}{2}-1)}$ self-dual codes over $\mathbb{Z}_{p^3}$ corresponding to each subspace of $\mathcal{C}_1$ of dimension k $(0 \le k \le \frac{n}{2})$.

Proposition. Define ε as follows: 1) if $\vec{1}_n \in A$ and $8 \mid n$, then $\varepsilon = 1$; 2) if $\vec{1}_n \notin A$, then $\varepsilon = 0$. Any self-dual code over $\mathbb{Z}_{2^3}$ is induced from a self-dual code $\mathcal{C}_1$ over $\mathbb{Z}_2$. There are $2^{kl+k^2+\varepsilon}$ self-dual codes over $\mathbb{Z}_{2^3}$ corresponding to each subspace of dimension k $(0 \le k \le \frac{n}{2})$ of $\mathcal{C}_1$.

Constructing self-dual codes from below

Proposition. Let p be an odd prime. A self-dual code over $\mathbb{Z}_{p^3}$ can be induced from a self-dual code $\mathcal{C}_1$ over $\mathbb{Z}_p$; there are $p^{k(\frac{n}{2}-1)}$ self-dual codes over $\mathbb{Z}_{p^3}$ corresponding to each subspace of $\mathcal{C}_1$ of dimension k $(0 \leq k \leq \frac{n}{2})$.

Proposition. Define ε as follows: 1) if $\vec{1}_n \in A$ and $8 \mid n$, then $\varepsilon = 1$; 2) if $\vec{1}_n \notin A$, then $\varepsilon = 0$. Any self-dual code over $\mathbb{Z}_{2^3}$ is induced from a self-dual code $\mathcal{C}_1$ over $\mathbb{Z}_2$. There are $2^{kl+k^2+\varepsilon}$ self-dual codes over $\mathbb{Z}_{2^3}$ corresponding to each subspace of dimension k $(0 \leq k \leq \frac{n}{2})$ of $\mathcal{C}_1$.

The number of underlying self-dual codes over $\mathbb{Z}_p$

Lemma. (Pless, 1965) Let p be an odd prime and $\sigma_p(n,k)$ the number of self-orthogonal codes of even length n and dimension k over $\mathbb{Z}_p$. Then :

1. If $(-1)^{\frac{n}{2}}$ is a square,

$$\sigma_p(n,k) = \frac{(p^{n-k} - p^{n/2-k} + p^{n/2} - 1)\prod_{i=1}^{k-1}(p^{n-2i} - 1)}{\prod_{i=1}^{k}(p^i - 1)}, \quad k \geq 1.$$

2. If $(-1)^{\frac{n}{2}}$ is not a square ,

$$\sigma_p(n,k) = \frac{(p^{n-k} + p^{n/2-k} - p^{n/2} - 1)\prod_{i=1}^{k-1}(p^{n-2i} - 1)}{\prod_{i=1}^{k}(p^i - 1)}, \quad k \geq 1.$$

The number of underlying self-dual codes over $\mathbb{Z}_p$

Lemma. (Pless, 1965) Let p be an odd prime and $\sigma_p(n,k)$ the number of self-orthogonal codes of even length n and dimension k over $\mathbb{Z}_p$. Then :

1. If $(-1)^{\frac{n}{2}}$ is a square,

$$\sigma_p(n,k) = \frac{(p^{n-k} - p^{n/2-k} + p^{n/2} - 1)\prod_{i=1}^{k-1}(p^{n-2i} - 1)}{\prod_{i=1}^{k}(p^i - 1)}, \quad k \geq 1.$$

2. If $(-1)^{\frac{n}{2}}$ is not a square ,

$$\sigma_p(n,k) = \frac{(p^{n-k} + p^{n/2-k} - p^{n/2} - 1)\prod_{i=1}^{k-1}(p^{n-2i} - 1)}{\prod_{i=1}^{k}(p^i - 1)}, \quad k \geq 1.$$

The number of subspaces

Lemma. Let V be an n-dimensional vector space over the integers modulo p. The number $\rho(n,k)$ of subspaces $T \subset V$ of dimension $k \leq n$ is given by

$$\rho(n,k) = \frac{(p^n - 1)(p^n - p)...(p^n - p^{k-1})}{(p^k - 1)(p^k - p)...(p^k - p^{k-1})}.$$

Main results

Theorem. Let $N_{p^3}(n)$ denote the number of distinct self-dual codes of even length n over $\mathbb{Z}_{p^3}$.

1. If p is odd then

$$N_{p^3}(n) = \left(1 + \left(\frac{-1}{p}\right)^{\frac{n}{2}}\right) \prod_{i=1}^{\frac{n}{2}-1} \frac{p^{n-2i}-1}{p^i-1} \sum_{k=0}^{\frac{n}{2}} \left(\prod_{i=0}^{k-1} \frac{p^{n-i}-1}{p^{k-i}-1} \right) p^{k(\frac{n}{2}-1)}.$$

2. If $n \equiv 2, 6 \pmod 8$ then

$$N_8(n) = \sum_{k=0}^{\frac{n}{2}-1} \left(\prod_{i=0}^{k-1} \frac{2^{n-2i-2}-1}{2^{i+1}-1} \right) \left(\prod_{i=k}^{\frac{n}{2}-2} \frac{2^{n-2i-2}-1}{2^{i+1-k}-1} \right) 2^{\frac{kn}{2}}.$$

Main results

Theorem. Let $N_{p^3}(n)$ denote the number of distinct self-dual codes of even length n over $\mathbb{Z}_{p^3}$.

1. If p is odd then

$$N_{p^3}(n) = \left(1 + \left(\frac{-1}{p}\right)^{\frac{n}{2}}\right) \prod_{i=1}^{\frac{n}{2}-1} \frac{p^{n-2i}-1}{p^i-1} \sum_{k=0}^{\frac{n}{2}} \left(\prod_{i=0}^{k-1} \frac{p^{n-i}-1}{p^{k-i}-1}\right) p^{k(\frac{n}{2}-1)}.$$

2. If $n \equiv 2, 6 \pmod 8$ then

$$N_8(n) = \sum_{k=0}^{\frac{n}{2}-1} \left(\prod_{i=0}^{k-1} \frac{2^{n-2i-2}-1}{2^{i+1}-1}\right) \left(\prod_{i=k}^{\frac{n}{2}-2} \frac{2^{n-2i-2}-1}{2^{i+1-k}-1}\right) 2^{\frac{kn}{2}}.$$

Main results

Theorem. Let $N_{p^3}(n)$ denote the number of distinct self-dual codes of even length n over $\mathbb{Z}_{p^3}$.

1. If p is odd then

$$N_{p^3}(n) = \left(1 + (\frac{-1}{p})^{\frac{n}{2}}\right) \prod_{i=1}^{\frac{n}{2}-1} \frac{p^{n-2i}-1}{p^i-1} \sum_{k=0}^{\frac{n}{2}} \left(\prod_{i=0}^{k-1} \frac{p^{n-i}-1}{p^{k-i}-1} \right) p^{k(\frac{n}{2}-1)}.$$

2. If $n \equiv 2, 6 \pmod 8$ then

$$N_8(n) = \sum_{k=0}^{\frac{n}{2}-1} \left(\prod_{i=0}^{k-1} \frac{2^{n-2i-2}-1}{2^{i+1}-1} \right) \left(\prod_{i=k}^{\frac{n}{2}-2} \frac{2^{n-2i-2}-1}{2^{i+1-k}-1} \right) 2^{\frac{kn}{2}}.$$

Main results

3. If $n \equiv 4 \pmod 8$ then

$$N_8(n) = \sum_{k=0}^{\frac{n}{2}-1} \left(\prod_{i=0}^{k-1} \frac{2^{n-2i-2} - 2^{\frac{n}{2}-i-1} - 2}{2^{i+1}-1} \right) \left(\prod_{i=k}^{\frac{n}{2}-2} \frac{2^{n-2i-2}-1}{2^{i+1-k}-1} \right) 2^{\frac{kn}{2}}.$$

4. If $n \equiv 0 \pmod 8$ then

$$\begin{aligned} N_8(n) &= \sum_{k=0}^{\frac{n}{2}-1} \left(\prod_{i=0}^{k-1} \frac{2^{n-2i-2} + 2^{\frac{n}{2}-i-1} - 2}{2^{i+1}-1} \right) \left(\prod_{i=k}^{\frac{n}{2}-2} \frac{2^{n-2i-2}-1}{2^{i+1-k}-1} \right) 2^{\frac{kn}{2}} \\ &\quad + \sum_{k=1}^{\frac{n}{2}} \left(\prod_{i=0}^{k-2} \frac{2^{n-2i-3} + 2^{\frac{n}{2}-i-2} - 1}{2^{i+1}-1} \right) \left(\prod_{i=k}^{\frac{n}{2}-1} \frac{2^{n-2i}-1}{2^{i+1-k}-1} \right) 2^{\frac{kn}{2}+1}. \end{aligned}$$

Main results

3. If $n \equiv 4 \pmod 8$ then

$$N_8(n) = \sum_{k=0}^{\frac{n}{2}-1} \left(\prod_{i=0}^{k-1} \frac{2^{n-2i-2} - 2^{\frac{n}{2}-i-1} - 2}{2^{i+1} - 1} \right) \left(\prod_{i=k}^{\frac{n}{2}-2} \frac{2^{n-2i-2} - 1}{2^{i+1-k} - 1} \right) 2^{\frac{kn}{2}}.$$

4. If $n \equiv 0 \pmod 8$ then

$$\begin{aligned} N_8(n) &= \sum_{k=0}^{\frac{n}{2}-1} \left(\prod_{i=0}^{k-1} \frac{2^{n-2i-2} + 2^{\frac{n}{2}-i-1} - 2}{2^{i+1} - 1} \right) \left(\prod_{i=k}^{\frac{n}{2}-2} \frac{2^{n-2i-2} - 1}{2^{i+1-k} - 1} \right) 2^{\frac{kn}{2}} \\ &+ \sum_{k=1}^{\frac{n}{2}} \left(\prod_{i=0}^{k-2} \frac{2^{n-2i-3} + 2^{\frac{n}{2}-i-2} - 1}{2^{i+1} - 1} \right) \left(\prod_{i=k}^{\frac{n}{2}-1} \frac{2^{n-2i} - 1}{2^{i+1-k} - 1} \right) 2^{\frac{kn}{2}+1}. \end{aligned}$$

A (partial) classification of self-dual codes over $\mathbb{Z}_8$ and $\mathbb{Z}_9$ by Gulliver, et.al.

Dougherty, Gulliver and Wong. *Self-dual codes over $\mathbb{Z}_8$ and $\mathbb{Z}_9$*. Designs, Codes and Cryptography 41 (Nov 2006):

- $n = 2$. There is only one self-dual code over $\mathbb{Z}_8$ of length 2.

$$G_2 = \begin{pmatrix} 2 & 2 \\ 0 & 4 \end{pmatrix}$$

- $n = 4$. There is only one self-dual code over $\mathbb{Z}_8$ of length 4.

$$G_4 = \begin{pmatrix} 2 & 0 & 0 & 2 \\ 0 & 2 & 2 & 0 \\ 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 4 \end{pmatrix}$$

A (partial) classification of self-dual codes over $\mathbb{Z}_8$ and $\mathbb{Z}_9$ by Gulliver, et.al.

Dougherty, Gulliver and Wong. *Self-dual codes over* $\mathbb{Z}_8$ *and* $\mathbb{Z}_9$. Designs, Codes and Cryptography 41 (Nov 2006):

- $n = 2$. There is only one self-dual code over $\mathbb{Z}_8$ of length 2.

$$G_2 = \begin{pmatrix} 2 & 2 \\ 0 & 4 \end{pmatrix}$$

- $n = 4$. There is only one self-dual code over $\mathbb{Z}_8$ of length 4.

$$G_4 = \begin{pmatrix} 2 & 0 & 0 & 2 \\ 0 & 2 & 2 & 0 \\ 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 4 \end{pmatrix}$$

A (partial) classification of self-dual codes over $\mathbb{Z}_8$ and $\mathbb{Z}_9$ by Gulliver, et.al.

Dougherty, Gulliver and Wong. *Self-dual codes over $\mathbb{Z}_8$ and $\mathbb{Z}_9$*. Designs, Codes and Cryptography 41 (Nov 2006):

- $n = 6$. One self-dual code over $\mathbb{Z}_8$ of length 6.

$$G_4 = \begin{pmatrix} 2 & 0 & 0 & 0 & 0 & 2 \\ 0 & 2 & 0 & 0 & 2 & 0 \\ 0 & 0 & 2 & 2 & 0 & 0 \\ 0 & 0 & 0 & 4 & 0 & 0 \\ 0 & 0 & 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 0 & 0 & 4 \end{pmatrix}$$

Example: self-dual codes over $\mathbb{Z}_8$ with $n = 6$, $k = 2$, $l = 1$.

We start with a self-dual binary code

$$\begin{bmatrix} A \\ B \end{bmatrix} = \begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 \end{bmatrix}$$

with

$$A_2 = \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \; A_{30} = \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \; A_{40} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Example: self-dual codes over $\mathbb{Z}_8$ with $n = 6$, $k = 2$, $l = 1$.

$$\mathcal{C} = \begin{bmatrix} 1 & 0 & 1 & 1+2x & 1+2y+4z & 2+4z' \\ 0 & 1 & 1 & 3-2x & 2+4(z'+y+y') & 1+2y'+4z'' \\ 0 & 0 & 2 & 2 & 4(1-x) & 4x \\ 0 & 0 & 0 & 4 & 4 & 4 \end{bmatrix},$$

where x, y, y', z, z', and z'' are arbitrary elements of $\mathbf{F}_2$.

The code $\mathcal{C}$ is self-dual over $\mathbb{Z}_8$.

Example: self-dual codes over $\mathbb{Z}_8$ with $n = 6$, $k = 2$, $l = 1$.

$$\mathcal{C} = \begin{bmatrix} 1 & 0 & 1 & 1+2x & 1+2y+4z & 2+4z' \\ 0 & 1 & 1 & 3-2x & 2+4(z'+y+y') & 1+2y'+4z'' \\ 0 & 0 & 2 & 2 & 4(1-x) & 4x \\ 0 & 0 & 0 & 4 & 4 & 4 \end{bmatrix},$$

where x, y, y', z, z', and z'' are arbitrary elements of $\mathbf{F}_2$.

The code $\mathcal{C}$ is self-dual over $\mathbb{Z}_8$.

what next

- Classification for $\mathbb{Z}_{p^3}$ codes of moderate lengths; develop efficient methods for computing automorphism groups
- Generalize to $\mathbb{Z}_{p^s}$
- Explore other rings: Galois rings, finite chain rings, Frobenius rings
- another track: Generalization of Hammons, et. al. result for other ring settings

what next

- Classification for $\mathbb{Z}_{p^3}$ codes of moderate lengths; develop efficient methods for computing automorphism groups
- Generalize to $\mathbb{Z}_{p^s}$
- Explore other rings: Galois rings, finite chain rings, Frobenius rings
- another track: Generalization of Hammons, et. al. result for other ring settings

what next

- Classification for $\mathbb{Z}_{p^3}$ codes of moderate lengths; develop efficient methods for computing automorphism groups
- Generalize to $\mathbb{Z}_{p^s}$
- Explore other rings: Galois rings, finite chain rings, Frobenius rings
- another track: Generalization of Hammons, et. al. result for other ring settings

what next

- Classification for $\mathbb{Z}_{p^3}$ codes of moderate lengths; develop efficient methods for computing automorphism groups
- Generalize to $\mathbb{Z}_{p^s}$
- Explore other rings: Galois rings, finite chain rings, Frobenius rings
- another track: Generalization of Hammons, et. al. result for other ring settings

Thank you.