Self-Dual Codes

Steven T. Dougherty

July 2, 2013

Classical Theory of Self-Dual Codes

Linear Code

A linear code C is a vector subspace of $\mathbb{F}_q^n$. If the size of the code is q^k and its minimum Hamming weight is d we call it an $[n, k, d]$ code.

Orthogonals

Equip the ambient space with the inner-product

$$[\mathbf{v}, \mathbf{w}] = \sum v_i \overline{w_i}$$

and define

$$C^{\perp} = \{\mathbf{v} \mid [\mathbf{v}, \mathbf{w} = 0, \forall \mathbf{w} \in C\}.$$

We assume that $\overline{w_i} = w_i$ unless otherwise stated. In the case when it is not the identity we refer to it as the Hermitian inner-product.

Orthogonals

Equip the ambient space with the inner-product

$$[\mathbf{v}, \mathbf{w}] = \sum v_i \overline{w_i}$$

and define

$$C^{\perp} = \{\mathbf{v} \mid [\mathbf{v}, \mathbf{w} = 0, \forall \mathbf{w} \in C\}.$$

We assume that $\overline{w_i} = w_i$ unless otherwise stated. In the case when it is not the identity we refer to it as the Hermitian inner-product. $C^{\perp}$ is a linear code and $dim(C^{\perp}) = n - dim(C)$.

Self-Dual Codes

A code is self-orthogonal if $C \subseteq C^{\perp}$.

Self-Dual Codes

A code is self-orthogonal if $C \subseteq C^{\perp}$.

A code is self-dual if $C = C^{\perp}$.

Self-Dual Codes

Theorem

If C is a self-dual code of length n over $\mathbb{F}_q$ then n must be even.

Self-Dual Codes

Theorem

If C is a self-dual code of length n over $\mathbb{F}_q$ then n must be even.

Proof.

We have $dim(C) = dim(C^{\perp})$ and $dim(C) + dim(C^{\perp}) = n$ which gives $dim(C) = \frac{n}{2}$ and so n must be even. $\square$

Example

$\langle(1,2)\rangle = \{(0,0),(1,2),(2,4),(3,1),(4,3)\}$ is a self-dual code of length 2 over $\mathbb{F}_5$.

Example

$\langle(1,2)\rangle = \{(0,0),(1,2),(2,4),(3,1),(4,3)\}$ is a self-dual code of length 2 over $\mathbb{F}_5$.

$\begin{pmatrix} 1 & 0 & 2 & 3 \\ 0 & 1 & 3 & 5 \end{pmatrix}$ generates a self-dual code of length 4 over $\mathbb{F}_7$.
There are none of length 2.

Gleason-Pierce-Ward

Theorem

Let p be a prime, m, n be integers and $q = p^m$. Suppose C is a linear $[n, \frac{n}{2}]$ divisible code over $\mathbb{F}_q$ with divisor $\Delta > 1$. Then one (or more) of the following holds:
I. $q = 2$ and $\Delta = 2$,
II. $q = 2$, $\Delta = 4$, and C is self-dual,
III. $q = 3$, $\Delta = 3$, and C is self-dual,
IV. $q = 4$, $\Delta = 2$, and C is Hermitian self-dual,
V. $\Delta = 2$ and C is equivalent to the code over $\mathbb{F}_q$ with generator matrix $[I_{\frac{n}{2}} I_{\frac{n}{2}}]$, where $I_{\frac{n}{2}}$ is the identity matrix of size $\frac{n}{2}$ over $\mathbb{F}_q$.

Type I and Type II

A binary self-dual code with all weights congruent to $0 \pmod 4$ is said to be a **Type II** code.

Type I and Type II

A binary self-dual code with all weights congruent to $0 \pmod 4$ is said to be a **Type II** code.

A binary self-dual code with a least one weight not congruent to $0 \pmod 4$ is said to be **Type I**. In this case all weights are congruent to $0 \pmod 2$.

Type III and Type IV

A ternary self-dual code with all weights congruent to $0 \pmod 3$ is said to be a **Type III** code.

Type III and Type IV

A ternary self-dual code with all weights congruent to $0 \pmod 3$ is said to be a **Type III** code.

A quaternary Hermitian self-dual code with weights congruent to $0 \pmod 2$ is said to be a **Type IV** code.

Cross Products

Theorem

If C and D are self-dual codes over $\mathbb{F}_q$ of length n and m then $C \times D$ is self-dual of length $n + m$.

Example – Type I

$$A = \begin{pmatrix} 1 & 1 \end{pmatrix}$$

The matrix A generates a Type I code of length 2. Hence Type I codes exists for all even lengths.

Example – Type II

$$A = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{pmatrix}$$

The matrix A generates a Type II code of length 8. Hence Type II codes exists for all lengths congruent to $0 \pmod 8$.

Example – Type II

$$A = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{pmatrix}$$

The matrix A generates a Type II code of length 8. Hence Type II codes exists for all lengths congruent to $0 \pmod 8$.

This $[8, 4, 4]$ code is formed by adding a parity check to the $[7, 4, 3]$ Hamming code.

Example – Type III

$$A = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 2 & 1 \end{pmatrix}$$

The matrix A generates a Type III code of length 4. Hence Type III codes exists for all even lengths congruent to $0 \pmod 4$.

Example – Type IV

$$A = \begin{pmatrix} 1 & \omega \end{pmatrix}$$

A generates a Type IV code of length 2. Hence Type IV codes exists for all even lengths.

Hamming Weight Enumerator

Let C be a code in $\mathbb{F}_q^n$. Then

$$W_C(x, y) = \sum_{\mathbf{c} \in C} x^{n - wt(\mathbf{c})} y^{wt(\mathbf{c})}$$

where $wt(\mathbf{c}) = |\{i \mid c_i \neq 0\}|$.

MacWilliams Relations

Let C be a linear code over $\mathbb{F}_q$, then

$$W_{C^\perp}(x, y) = \frac{1}{|C|} W_C(x + (q-1)y, x - y).$$

Invariant Theory

The theory of invariants came into existence about the middle of the nineteenth century somewhat like Minerva: a grown-up virgin, mailed in the shining armor of algebra, she sprang forth from Cayley's Jovian head.
Weyl – 1939

Invariant Theory

The theory of invariants came into existence about the middle of the nineteenth century somewhat like Minerva: a grown-up virgin, mailed in the shining armor of algebra, she sprang forth from Cayley's Jovian head.
Weyl – 1939

Like the Arabian phoenix rising out of its ashes, the theory of invariants, pronounced dead at the turn of the century, is once again at the forefront of mathematics.
Kung and Rota – 1984

Invariant Theory

If C is a self-dual code then the weight enumerator is held invariant by the MacWilliams relations and hence by the following matrix:

$$M = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

Invariant Theory

If C is a self-dual code then the weight enumerator is held invariant by the MacWilliams relations and hence by the following matrix:

$$M = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

If the code is doubly-even, then it is also held invariant by the following matrix:

$$A = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$$

Invariant Theory

The group $G = \langle G, A \rangle$ has order 192. The series $\Phi(\lambda) = \sum a_i \lambda^i$ where there are a_i independent polynomials held invariant by the group G.

Invariant Theory

The group $G = \langle G, A \rangle$ has order 192. The series $\Phi(\lambda) = \sum a_i \lambda^i$ where there are a_i independent polynomials held invariant by the group G.

Theorem

(Molien) For any finite group G of complex m by m matrices, $\Phi(\lambda)$ is given by

$$\Phi(\lambda) = \frac{1}{|G|} \sum_{A \in G} \frac{1}{det(I - \lambda A)} \tag{1}$$

where I is the identity matrix.

Invariant Theory

For our group G we get

$$\Phi(\lambda) = \frac{1}{(1-\lambda^8)(1-\lambda^{24})} = 1 + \lambda^8 + \lambda^{16} + 2\lambda^{24} + 2\lambda^{32} + \dots \quad (2)$$

Invariant Theory

For our group G we get

$$\Phi(\lambda) = \frac{1}{(1-\lambda^8)(1-\lambda^{24})} = 1 + \lambda^8 + \lambda^{16} + 2\lambda^{24} + 2\lambda^{32} + \dots \quad (2)$$

In particular, this shows that Type II codes exist only if the length is a multiple of 8.

Invariant Theory

The generating invariants in this case can be found. Specifically, we have:

$$W_1(x, y) = x^8 + 14x^4y^4 + y^8 \tag{3}$$

and

$$W_2(x, y) = x^4y^4(x^4 - y^4)^4 \tag{4}$$

Invariant Theory

The generating invariants in this case can be found. Specifically, we have:

$$W_1(x,y) = x^8 + 14x^4y^4 + y^8 \tag{3}$$

and

$$W_2(x,y) = x^4y^4(x^4 - y^4)^4 \tag{4}$$

Notice that W_1 is the weight enumerator of the $[8,4,4]$ code given earlier.

Gleason's Theorem

Then we have the well known Gleason's Theorem.

Theorem

(Gleason) The weight enumerator of an Type II self-dual code is a polynomial in $W_1(x, y)$ *and* $W_2(x, y)$*, i.e. if* C *is a Type II code then* $W_C(x, y) \in \mathbb{C}[W_1(x, y), W_2(x, y)]$.

Gleason's Theorem

It follows that if C is a Type II $[n, k, d]$ code then

$$d \leq 4\lfloor \frac{n}{24} \rfloor + 4 \tag{5}$$

Gleason's Theorem

It follows that if C is a Type II $[n, k, d]$ code then

$$d \leq 4\lfloor \frac{n}{24} \rfloor + 4 \tag{5}$$

Codes meeting this bound are called extremal. We investigate those with parameters $[24k, 12k, 4k + 4]$. It is not known whether these codes exist until $24k \geq 3720$ at which a coefficient becomes negative.

Gleason Type Theorem

Applying the same techniques of the invariant theory we have the following.

Gleason Type Theorem

Applying the same techniques of the invariant theory we have the following.

Theorem

(Gleason) The weight enumerator of an Type I self-dual code is a polynomial in $x^2 + y^2$ *and* $W_1(x, y)$*, i.e. if* C *is a Type I code then* $W_C(x, y) \in \mathbb{C}[x^2 + y^2, W_1(x, y)]$*.*

Gleason Type Theorem

Theorem

The weight enumerator of an Type III self-dual code is a polynomial in $x^4 + 8xy^3$ and $y^3(x^3 - y^3)^3$, i.e. if C is a Type I code then $W_C(x, y) \in \mathbb{C}[x^4 + 8xy^3, y^3(x^3 - y^3)^3]$.

Gleason Type Theorem

Theorem

The weight enumerator of an Type IV self-dual code is a polynomial in $x^2 + 3y^2$ *and* $y^2(x^2 - y^2)^2$*, i.e. if* C *is a Type IV code then* $W_C(x, y) \in \mathbb{C}[x^2 + 3y^2, y^2(x^2 - y^2)^2]$.

Assmus-Mattson Theorem

Let C be a code over $\mathbb{F}_q$ of length n with minimum weight d, and let $d^\perp$ denote the minimum weight of $C^\perp$. Let $w = n$ when $q = 2$ and otherwise the largest integer w satisfying $w - (\frac{w+q-2}{q-1}) < d$, define $w^\perp$ similarly. Suppose there is an integer t with $0 < t < d$ that satisfies the following condition: for $W_{C^\perp}(Z) = B_i Z^i$ at most $d - t$ of $B_1, B_2, \ldots, B_{n-t}$ are non-zero. Then for each i with $d \leq i \leq w$ the supports of the vectors of weight i of C, provided there are any, yield a t-design. Similarly, for each j with $d^\perp \leq j \leq min\{w^\perp, n-t\}$ the supports of the vectors of weight j in $C^\perp$, provided there are any, form a t-design.

Assmus-Mattson Corollary

Let C be a Type II $[24k, 12k, 4k+4]$ code, then the vectors of every weight form a 5 design.

Assmus-Mattson Corollary

Let C be a Type II $[24k, 12k, 4k+4]$ code, then the vectors of every weight form a 5 design.

The Golay code is a $[24, 12, 8]$ Type II code and the vectors of all weights hold 5 designs. This code is related to the Leech lattice and the Witt designs.

Invariant Theory

Theorem

- *Type I codes exist if and only if* $n \equiv 0 \pmod{2}$.

Invariant Theory

Theorem

- *Type I codes exist if and only if* $n \equiv 0 \pmod{2}$.
- *Type II codes exist if and only if* $n \equiv 0 \pmod{8}$.

Invariant Theory

Theorem

- *Type I codes exist if and only if* $n \equiv 0 \pmod{2}$.
- *Type II codes exist if and only if* $n \equiv 0 \pmod{8}$.
- *Type III codes exist if and only if* $n \equiv 0 \pmod{4}$.

Invariant Theory

Theorem

- *Type I codes exist if and only if* $n \equiv 0 \pmod 2$.
- *Type II codes exist if and only if* $n \equiv 0 \pmod 8$.
- *Type III codes exist if and only if* $n \equiv 0 \pmod 4$.
- *Type IV codes exist if and only if* $n \equiv 0 \pmod 2$.

Projective Plane of order 10

The proof of the non-existence of the projective plane of order 10 by Lam et al. was done by using the previous.

Projective Plane of order 10

The proof of the non-existence of the projective plane of order 10 by Lam et al. was done by using the previous.

If a projective plane of order 10 exists then there exists a Type II $[112, 56, 12]$ code with no vectors of weight 16.

Projective Plane of order 10

The proof of the non-existence of the projective plane of order 10 by Lam et al. was done by using the previous.

If a projective plane of order 10 exists then there exists a Type II $[112, 56, 12]$ code with no vectors of weight 16.

It was shown that no such code exists and hence no plane exists.

Self-Dual Codes over Rings

Definitions

Let R be a finite commutative Frobenius ring.

Definitions

Let R be a finite commutative Frobenius ring.
A linear code over R of length n is a submodule of R^n.

Orthogonals

Equip the ambient space R^n with the inner-product

$$[\mathbf{v}, \mathbf{w}] = \sum v_i w_i$$

and define

$$C^{\perp} = \{\mathbf{v} \mid [\mathbf{v}, \mathbf{w} = 0, \forall \mathbf{w} \in C\}.$$

Orthogonals

Equip the ambient space R^n with the inner-product

$$[\mathbf{v}, \mathbf{w}] = \sum v_i w_i$$

and define

$$C^\perp = \{\mathbf{v} \mid [\mathbf{v}, \mathbf{w} = 0, \forall \mathbf{w} \in C\}.$$

$C^\perp$ is a linear code and $|C||C^\perp| = |R|^n$.

Self-Dual Codes

Unlike for codes over fields the length does not have to be even.

Self-Dual Codes

Unlike for codes over fields the length does not have to be even.

E.g. Let C be the code of length 1 over $\mathbb{Z}_4$, $c = \{0, 2\}$. Then C is a self-dual code of length 1.

Euclidean weight

The *Euclidean weight* $wt_E(x)$ of a vector $(x_1, x_2, \ldots, x_n)$ is $\sum_{i=1}^{n} \min\{x_i^2, (2k - x_i)^2\}$.

Euclidean Divisible Codes

Theorem

Suppose that C is a self-dual code over $\mathbb{Z}_{2k}$ which has the property that every Euclidean weight is a multiple of a positive integer. Then the largest positive integer c is either $2k$ or $4k$.

Type I and Type II

A self-dual code over $\mathbb{Z}_{2k}$ is said to be Type II if the Euclidean weights of all vectors is congruent to $0 \pmod{4k}$.

Type I and Type II

A self-dual code over $\mathbb{Z}_{2k}$ is said to be Type II if the Euclidean weights of all vectors is congruent to $0 \pmod{4k}$.

A self-dual code over $\mathbb{Z}_{2k}$ is said to be Type I if the Euclidean weight of at least one vector is not congruent to $0 \pmod{4k}$. In this case the Euclidean weights of all vectors is congruent to $0 \pmod{2k}$.

Existence of Type II Codes

Theorem

There exists a Type II code C of length n over $\mathbb{Z}_{2k}$ if and only if n is a multiple of eight.

Proof

The matrix

$$(\ I_4 \ , \ M_4 \ ),$$

where I_4 is the identity matrix of order 4 and

$$M_4 = \begin{pmatrix} a & b & c & d \\ b & -a & -d & c \\ c & d & -a & -b \\ d & -c & b & -a \end{pmatrix},$$

then $M_4 \cdot {}^tM_4 = (a^2 + b^2 + c^2 + d^2)I_4$ over $\mathbb{Z}$ where ${}^tA$ denotes the transpose matrix of a matrix A.
From Lagrange's theorem on sums of squares we have the solution for a, b, c, d. Then the matrix generates a Type II code over $\mathbb{Z}_{2k}$.

Proof

The matrix

$$(\ I_4 \ , \ M_4 \ ),$$

where I_4 is the identity matrix of order 4 and

$$M_4 = \begin{pmatrix} a & b & c & d \\ b & -a & -d & c \\ c & d & -a & -b \\ d & -c & b & -a \end{pmatrix},$$

then $M_4 \cdot {}^tM_4 = (a^2 + b^2 + c^2 + d^2)I_4$ over $\mathbb{Z}$ where ${}^tA$ denotes the transpose matrix of a matrix A.
From Lagrange's theorem on sums of squares we have the solution for a, b, c, d. Then the matrix generates a Type II code over $\mathbb{Z}_{2k}$.

Invariant theory gives the other direction.

Example

Over $\mathbb{Z}_4$, $a^2 + b^2 + c^2 + d^2 = 7 \pmod 8 \implies a = 2, b = c = d = 1.$

Example

Over $\mathbb{Z}_4$, $a^2 + b^2 + c^2 + d^2 = 7 \pmod 8 \implies a = 2, b = c = d = 1$.

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 2 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 2 & 3 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 2 & 3 \\ 0 & 0 & 0 & 1 & 1 & 3 & 1 & 2 \end{pmatrix}$$

generates a Type II code over $\mathbb{Z}_4$.

Example

The code generated by (2) is a Type I code over $\mathbb{Z}_4$.

Example

The code generated by (2) is a Type I code over $\mathbb{Z}_4$.

The code generated by $\begin{pmatrix} 2 & 2 \\ 0 & 4 \end{pmatrix}$ generates a Type I code over $\mathbb{Z}_8$.

Example

The code generated by (2) is a Type I code over $\mathbb{Z}_4$.

The code generated by $\begin{pmatrix} 2 & 2 \\ 0 & 4 \end{pmatrix}$ generates a Type I code over $\mathbb{Z}_8$.

Notice this code has $4^2 2^1$ vectors. It is not generated by a single element unlike self-dual codes over fields of length 1.

Free

A code C is free if it is isomorphic to R^k. Otherwise it is said to be not free.

Free

A code C is free if it is isomorphic to R^k. Otherwise it is said to be not free.

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 3 & 0 & 1 & 3 \\ 0 & 0 & 1 & 0 & 3 & 3 & 0 & 1 \\ 0 & 0 & 0 & 1 & 3 & 1 & 3 & 0 \end{pmatrix}$$

generates a free self-dual code over $\mathbb{Z}_4$ of length 8.

Invariant Theory

Theorem

The Hamming weight enumerator of a self-dual code over $\mathbb{Z}_4$ *is an element of*

$\mathbb{C}[x+y, xy(x^2+y^2-2y^4] + b^4(a-b)^4\mathbb{C}[x+y, xy(x^2+y^2-2y^4]$.

Connection to Lattices

Theorem

(**Bannai, Dougherty, Harada, Oura**) *If C is a self-dual code of length n over $\mathbb{Z}_{2k}$, then the lattice*

$$\Lambda(C) = \frac{1}{\sqrt{2k}}\{\rho(C) + 2k\mathbb{Z}^n\},$$

is an n-dimensional unimodular lattice, where $\rho(C) = \{(\rho(c_1), \ldots, \rho(c_n)) \mid (c_1, \ldots, c_n) \in C\}$. The minimum norm is $\min\{2k, d_E/2k\}$ where d_E is the minimum Euclidean weight of C. Moreover, if C is Type II then the lattice $\Lambda(C)$ is an even unimodular lattice.

Connection to Lattices

There exists a length 72 self-dual code with minimum Euclidean weight 64 which gives an extremal lattice of length 72.

Connection to Lattices

There exists a length 72 self-dual code with minimum Euclidean weight 64 which gives an extremal lattice of length 72.
No binary code can give this lattice.

Rings of Order 4

$$\mathbb{Z}_4 = \{0, 1, 2, 3\}$$

Rings of Order 4

$$\mathbb{Z}_4 = \{0, 1, 2, 3\}$$

$$\mathbb{F}_4 = \{0, 1, \omega, \omega^2\}$$

Rings of Order 4

$$\mathbb{Z}_4 = \{0, 1, 2, 3\}$$

$$\mathbb{F}_4 = \{0, 1, \omega, \omega^2\}$$

$$\mathbb{F}_2 + u\mathbb{F}_2 = \{0, 1, u, 1+u\}, u^2 = 0$$

Rings of Order 4

$$\mathbb{Z}_4 = \{0, 1, 2, 3\}$$

$$\mathbb{F}_4 = \{0, 1, \omega, \omega^2\}$$

$$\mathbb{F}_2 + u\mathbb{F}_2 = \{0, 1, u, 1 + u\}, u^2 = 0$$

$$\mathbb{F}_2 + v\mathbb{F}_2 = \{0, 1, v, 1 + v\}, v^2 = v$$

Rings of Order 4

$\mathbb{Z}_4$ is a chain ring

Rings of Order 4

$\mathbb{Z}_4$ is a chain ring
$\mathbb{F}_4$ is a finite field and so it is within the area of classical coding theory.

Rings of Order 4

$\mathbb{Z}_4$ is a chain ring
$\mathbb{F}_4$ is a finite field and so it is within the area of classical coding theory.
$\mathbb{F}_2 + u\mathbb{F}_2$ is a local ring with maximal ideal $\langle u \rangle$ (it is also a chain ring but its generalization is not).

Rings of Order 4

$\mathbb{Z}_4$ is a chain ring
$\mathbb{F}_4$ is a finite field and so it is within the area of classical coding theory.
$\mathbb{F}_2 + u\mathbb{F}_2$ is a local ring with maximal ideal $\langle u \rangle$ (it is also a chain ring but its generalization is not).
$\mathbb{F}_2 + v\mathbb{F}_2$ is a principal ideal ring isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$

Gray Maps

The following are the distance preserving Gray maps from the rings of order 4 to $\mathbb{F}_2^2$.

$\mathbb{Z}_4$	$\mathbb{F}_4$	$\mathbb{F}_2 + u\mathbb{F}_2$	$\mathbb{F}_2 + v\mathbb{F}_2$	$\mathbb{F}_2^2$
0	0	0	0	00
1	1	1	v	01
2	$1+\omega$	u	1	11
3	ω	$1+u$	$1+v$	10

Hermitian

Over $\mathbb{F}_2 + v\mathbb{F}_2$ we have an involution:

$$\begin{aligned} \overline{0} &= 0 \\ \overline{1} &= 1 \\ \overline{v} &= 1 + v \\ \overline{1+v} &= v \end{aligned}$$

Type IV

A Type IV code over a ring of order 4 is one in which all of the Hamming weights are $0 \pmod 2$.

Type IV

Theorem

If C is a Type IV $\mathbb{Z}_4$-code of length n then all the Lee weights of C are divisible by four and its Gray image $\phi(C)$ is a self-dual Type II binary code.

Type IV

Theorem
If C is a Type IV $\mathbb{Z}_4$-code of length n then all the Lee weights of C are divisible by four and its Gray image $\phi(C)$ is a self-dual Type II binary code.

Theorem
A Type IV code over $\mathbb{Z}_4$ of length n exists if and only if $n \equiv 0 \pmod 4$.

Type IV

Theorem

Let C, D be a dual pair of binary codes with even weights and $C \subseteq D$. Then $C + uD$ is a Type IV code over $\mathbb{F}_2 + u\mathbb{F}_2$.

Type IV

$\mathbb{F}_2 + v\mathbb{F}_2$ is isomorphic via the Chinese Remainder Theorem to $\mathbb{F}_2 \times \mathbb{F}_2$.

Type IV

$\mathbb{F}_2 + v\mathbb{F}_2$ is isomorphic via the Chinese Remainder Theorem to $\mathbb{F}_2 \times \mathbb{F}_2$.

Theorem

$CRT(C_1, C_2)$ is a Hermitian self-dual code if and only if $C_1 = C_2^{\perp}$.

Type IV

Theorem

Let $CRT(C_1, C_2)$ be a Hermitian self-dual code. $CRT(C_1, C_2)$ is Type IV if and only if C_1 and C_2 are even.

Type IV

Theorem

Let $CRT(C_1, C_2)$ *be a Hermitian self-dual code.* $CRT(C_1, C_2)$ *is Type IV if and only if* C_1 *and* C_2 *are even.*

Theorem

A Hermitian Type IV $\mathbb{F}_2 + v\mathbb{F}_2$*-code of length* n *exists if and only if* n *is even.*

Generalizations

- $\mathbb{F}_2 + u\mathbb{F}_2$ generalizes to R_k, $R_k = \mathbb{F}_2[u_1, v_2, \ldots, u_k]$, $u_i^2 = 0$, which is a local ring.

Generalizations

- $\mathbb{F}_2 + u\mathbb{F}_2$ generalizes to R_k, $R_k = \mathbb{F}_2[u_1, v_2, \ldots, u_k]$, $u_i^2 = 0$, which is a local ring.
- $\mathbb{F}_2 + v\mathbb{F}_2$ generalizes to A_k, $A_k = \mathbb{F}_2[v_1, v_2, \ldots, v_k]$, $v_i^2 = v_i$, which is isomorphic to $\mathbb{F}_2^k$.

Self-dual codes over Frobenius Rings

Chinese Remainder Theorem

Let R be a finite ring, $\mathfrak{m}_1, \ldots, \mathfrak{m}_k$ the maximal ideals of R, $e_1, \ldots, e_k$ their indices of stability.

Chinese Remainder Theorem

Let R be a finite ring, $\mathfrak{m}_1, \ldots, \mathfrak{m}_k$ the maximal ideals of R, $e_1, \ldots, e_k$ their indices of stability.

Then the ideals $\mathfrak{m}_1^{e_1}, \ldots, \mathfrak{m}_k^{e_k}$ are relatively prime in pairs and $\prod_{i=1}^k \mathfrak{m}_i^{e_i} = \cap_{i=1}^k \mathfrak{m}_i^{e_i} = \{0\}$.

Chinese Remainder Theorem

By the ring version of the Chinese Remainder Theorem, the canonical ring homomorphism $\Psi : R \to \prod_{i=1}^{k} R/\mathfrak{m}_i^{e_i}$, defined by $x \mapsto (x + \mathfrak{m}_1^{e_1}, \ldots, x + \mathfrak{m}_k^{e_k})$, is an isomorphism.

Chinese Remainder Theorem

By the ring version of the Chinese Remainder Theorem, the canonical ring homomorphism $\Psi : R \to \prod_{i=1}^{k} R/\mathfrak{m}_i^{e_i}$, defined by $x \mapsto (x + \mathfrak{m}_1^{e_1}, \ldots, x + \mathfrak{m}_k^{e_k})$, is an isomorphism.

Denote the local rings $R/\mathfrak{m}_i^{e_i}$ by R_i $(i = 1, \ldots, k)$.

Chinese Remainder Theorem

Note that R is Frobenius if and only if each R_i is Frobenius.

Chinese Remainder Theorem

Note that R is Frobenius if and only if each R_i is Frobenius.

For a code $C \subset R^n$ over R and the maximal ideal $\mathfrak{m}_i$ of R, the $\mathfrak{m}_i$-*projection* of C is defined by

$$C_{(\mathfrak{m}_i)} = \Psi_{\mathfrak{m}_i^{e_i}}(C)$$

where $\Psi_{\mathfrak{m}_i^{e_i}} : R^n \to R_i^n$ is the canonical map.

Chinese Remainder Theorem

Note that R is Frobenius if and only if each R_i is Frobenius.

For a code $C \subset R^n$ over R and the maximal ideal $\mathfrak{m}_i$ of R, the $\mathfrak{m}_i$-*projection* of C is defined by

$$C_{(\mathfrak{m}_i)} = \Psi_{\mathfrak{m}_i^{e_i}}(C)$$

where $\Psi_{\mathfrak{m}_i^{e_i}} : R^n \to R_i^n$ is the canonical map.

We denote by $\Psi : R^n \to \prod_{i=1}^{k} R_i^n$ the map defined by

$$\Psi(\mathbf{v}) = (\Psi_{\mathfrak{m}_1^{e_1}}(\mathbf{v}), \ldots, \Psi_{\mathfrak{m}_k^{e_k}}(\mathbf{v}))$$

for $\mathbf{v} \in R^n$. By the module version of the Chinese Remainder Theorem, the map Ψ is an R-module isomorphism and

$$C \cong C_{(\mathfrak{m}_1)} \times \cdots \times C_{(\mathfrak{m}_k)}.$$

Chinese Remainder Theorem

Conversely, given codes C_i of length n over $R_i \quad (i = 1, \ldots, k)$, we define the code $C = \mathrm{CRT(C_1, \ldots, C_k)}$ of length n over R in the following way:

$$\begin{aligned} C &= \{\Psi^{-1}(\mathbf{v_1}, \ldots, \mathbf{v_k}) :\ \mathbf{v_i} \in C_i \,(i = 1, \ldots, k)\} \\ &= \{\mathbf{v} \in R^n :\ \Psi_{\mathfrak{m}_i^{t_i}}(\mathbf{v}) \in C_i \,(i = 1, \ldots, k)\}. \end{aligned}$$

Chinese Remainder Theorem

Conversely, given codes C_i of length n over R_i $(i = 1, \ldots, k)$, we define the code $C = \mathrm{CRT(C_1, \ldots, C_k)}$ of length n over R in the following way:

$$\begin{aligned} C &= \{\Psi^{-1}(\mathbf{v_1}, \ldots, \mathbf{v_k}) : \mathbf{v_i} \in C_i \, (i = 1, \ldots, k)\} \\ &= \{\mathbf{v} \in R^n : \Psi_{\mathfrak{m}_i^{t_i}}(\mathbf{v}) \in C_i \, (i = 1, \ldots, k)\}. \end{aligned}$$

Then $C_{(\mathfrak{m}_i)} = C_i \, (i = 1, \ldots, k)$. The code $C = \mathrm{CRT(C_1, \ldots, C_k)}$ is called the *Chinese product of the codes C_i*.

Chinese Remainder Theorem

Theorem

Let R be a finite Frobenius ring, n a positive integer, then

$$R^n = \mathrm{CRT}(R_1^n, R_2^n, \cdots, R_k^n),$$

where each R_i is a local Frobenius ring.

Chinese Remainder Theorem

Theorem

Let $C_1, C_2, \cdots, C_k$ *be codes of length* n *with* C_i *a code over* R_i*, and let* $C = CRT(C_1, C_2, \ldots, C_k)$*. Then:*

- $|C| = \prod_{i=1}^{t} |C_i|$;
- C *is a free code if and only if each* C_i *is a free code of the same free rank.*

Chinese Remainder Theorem

Theorem

If C_i is a self-dual code over R_i then $C = CRT(C_1, C_2, \ldots, C_k)$ is a self-dual code over R.

Self-Dual Codes

Lemma

If $|R|$ is not a square and C is a self-dual code of length n then n must be even.

Self-Dual Codes

Lemma

If $|R|$ is not a square and C is a self-dual code of length n then n must be even.

Lemma

Let C be a self-dual code of length n over R and D be a self-dual code of length m over R then the direct product $C \times D$ is a self-dual code of length $n+m$ over R.

Non-Free Self-Dual Codes

Theorem

Let R be a finite local ring with maximal ideal $\mathfrak{m}$. If $R/\mathfrak{m}$ has characteristic $1 \pmod 4$ or 2 then there exists a self-dual code of length 2 over R that is not free.

Non-Free Self-Dual Codes

Proof

We can assume e, the nilpotency index of $\mathfrak{m}$, is odd since if it were even we would have a self-dual code of length 2.

Non-Free Self-Dual Codes

Proof

We can assume e, the nilpotency index of $\mathfrak{m}$, is odd since if it were even we would have a self-dual code of length 2.

Since $R/\mathfrak{m}$ is a field of characteristic order 1 (mod 4) or 2 then there exists $(1, \alpha)$ which generates a self-dual code of length 2 over $R/\mathfrak{m}$.

Non-Free Self-Dual Codes

Proof

We can assume e, the nilpotency index of $\mathfrak{m}$, is odd since if it were even we would have a self-dual code of length 2.

Since $R/\mathfrak{m}$ is a field of characteristic order $1 \pmod 4$ or 2 then there exists $(1, \alpha)$ which generates a self-dual code of length 2 over $R/\mathfrak{m}$.

Let

$$A = \{(a, a\alpha) \mid a \in \mathfrak{m}^{\frac{e-1}{2}}\}.$$

Then

$$[(a_1, a_1\alpha), (a_2, a_2\alpha)] = a_1 a_2 + a_1 a_2 \alpha^2 = a_1 a_2 (1 + \alpha^2).$$

Non-Free Self-Dual Codes

We know that $1+\alpha^2 \in \mathfrak{m}$ and $a_1a_2 \in \mathfrak{m}^{\frac{e-1}{2}}\mathfrak{m}^{\frac{e-1}{2}} = \mathfrak{m}^{e-1}$. Then we have $a_1a_2 + a_1a_2\alpha^2 \in \mathfrak{m}^e$ and then $a_1a_2 + a_1a_2\alpha^2 = 0$. Therefore A is self-orthogonal and obviously linear with $|A| = |\mathfrak{m}^{\frac{e-1}{2}}|$.

Non-Free Self-Dual Codes

We know that $1+\alpha^2 \in \mathfrak{m}$ and $a_1 a_2 \in \mathfrak{m}^{\frac{e-1}{2}}\mathfrak{m}^{\frac{e-1}{2}} = \mathfrak{m}^{e-1}$. Then we have $a_1 a_2 + a_1 a_2 \alpha^2 \in \mathfrak{m}^{e}$ and then $a_1 a_2 + a_1 a_2 \alpha^2 = 0$. Therefore A is self-orthogonal and obviously linear with $|A| = |\mathfrak{m}^{\frac{e-1}{2}}|$.

Let $B = \{(0,b) \mid b \in (\mathfrak{m}^{\frac{e-1}{2}})^{\perp} = \mathfrak{m}^{\frac{e-1}{2}+1}\}$.

Non-Free Self-Dual Codes

We know that $1+\alpha^2 \in \mathfrak{m}$ and $a_1a_2 \in \mathfrak{m}^{\frac{e-1}{2}}\mathfrak{m}^{\frac{e-1}{2}} = \mathfrak{m}^{e-1}$. Then we have $a_1a_2 + a_1a_2\alpha^2 \in \mathfrak{m}^e$ and then $a_1a_2 + a_1a_2\alpha^2 = 0$. Therefore A is self-orthogonal and obviously linear with $|A| = |\mathfrak{m}^{\frac{e-1}{2}}|$.

Let $B = \{(0,b) \mid b \in (\mathfrak{m}^{\frac{e-1}{2}})^{\perp} = \mathfrak{m}^{\frac{e-1}{2}+1}\}$.

We know $|B| = |\mathfrak{m}^{\frac{e-1}{2}+1}|$.

Non-Free Self-Dual Codes

We know that $1+\alpha^2 \in \mathfrak{m}$ and $a_1a_2 \in \mathfrak{m}^{\frac{e-1}{2}}\mathfrak{m}^{\frac{e-1}{2}} = \mathfrak{m}^{e-1}$. Then we have $a_1a_2 + a_1a_2\alpha^2 \in \mathfrak{m}^e$ and then $a_1a_2 + a_1a_2\alpha^2 = 0$. Therefore A is self-orthogonal and obviously linear with $|A| = |\mathfrak{m}^{\frac{e-1}{2}}|$.

Let $B = \{(0, b) \mid b \in (\mathfrak{m}^{\frac{e-1}{2}})^{\perp} = \mathfrak{m}^{\frac{e-1}{2}+1}\}$.

We know $|B| = |\mathfrak{m}^{\frac{e-1}{2}+1}|$.

We know $B \subseteq B^{\perp}$ since $b \in \mathfrak{m}^{\frac{e-1}{2}+1} = \mathfrak{m}^{\frac{e+1}{2}} \subset \mathfrak{m}^{\frac{e-1}{2}}$ so that $b^2 = 0$.

Non-Free Self-Dual Codes

Let $C = \langle A, B \rangle$. The code C is self-orthogonal since $[(a, a\alpha), (0, b)] = ab\alpha$ and $ab = 0$.

Non-Free Self-Dual Codes

Let $C = \langle A, B \rangle$. The code C is self-orthogonal since $[(a, a\alpha), (0, b)] = ab\alpha$ and $ab = 0$.

Next assume $(a, a\alpha + b) = (a', a'\alpha + b')$. Then we have $a = a'$ by equating the first coordinate and then $a\alpha + b = a\alpha + b'$. By equating the second coordinate we have $b = b'$. This gives that $|C| = |A||B| = |\mathfrak{m}^{\frac{e-1}{2}}||\mathfrak{m}^{\frac{e-1}{2}+1}| = |\mathfrak{m}^{\frac{e-1}{2}}||\mathfrak{m}^{\frac{e+1}{2}}| = |R|$, by the fact that the product of the cardinality of a code and the cardinality of its orthogonal is the cardinality of the ambient space. Then C is a self-dual code. **QED**

Non-free Self-Dual Codes

Corollary

Let R be a finite local ring with maximal ideal $\mathfrak{m}$. If $R/\mathfrak{m}$ has characteristic $1 \pmod 4$ or 2 then there exists self-dual codes over R of all even lengths that are not free.

Non-Free Self-Dual Codes

Theorem

Let R be a finite local ring with maximal ideal $\mathfrak{m}$. If $R/\mathfrak{m}$ has characteristic $3 \pmod 4$ then there exists a self-dual code of length 4 over R that is not free.

Non-Free Self-Dual Codes

Theorem

Let R be a finite local ring with maximal ideal $\mathfrak{m}$. If $R/\mathfrak{m}$ has characteristic $3 \pmod 4$ then there exists a self-dual code of length 4 over R that is not free.

Corollary

Let R be a finite local ring with maximal ideal $\mathfrak{m}$. If $|R/\mathfrak{m}| \equiv 3 \pmod 4$ then there exist self-dual codes over R of all even lengths divisible by 4.

Self-Dual Codes

Theorem

Let R be a finite Frobenius ring with maximal ideals $\mathfrak{m}_1, \ldots, \mathfrak{m}_k$ whose indices of stability are $e_1, \ldots, e_k$ and the corresponding residue fields are $\mathbb{F}_1, \ldots, \mathbb{F}_k$. Then the following results hold.

Self-Dual Codes

Theorem

Let R be a finite Frobenius ring with maximal ideals $\mathfrak{m}_1, \ldots, \mathfrak{m}_k$ whose indices of stability are $e_1, \ldots, e_k$ and the corresponding residue fields are $\mathbb{F}_1, \ldots, \mathbb{F}_k$. Then the following results hold.
(1) If e_i is even for all i then there exist self-dual codes of all lengths;

Self-Dual Codes

Theorem

Let R be a finite Frobenius ring with maximal ideals $\mathfrak{m}_1, \dots, \mathfrak{m}_k$ whose indices of stability are $e_1, \dots, e_k$ and the corresponding residue fields are $\mathbb{F}_1, \dots, \mathbb{F}_k$. Then the following results hold.
(1) If e_i is even for all i then there exist self-dual codes of all lengths;
(2) If for all i either $\mathbb{F}_i$ has characteristic 2 or $1 \pmod 4$ or the index of stability is even, then self-dual codes exist for all even lengths;

Self-Dual Codes

Theorem

Let R be a finite Frobenius ring with maximal ideals $\mathfrak{m}_1, \dots, \mathfrak{m}_k$ whose indices of stability are $e_1, \dots, e_k$ and the corresponding residue fields are $\mathbb{F}_1, \dots, \mathbb{F}_k$. Then the following results hold.
(1) If e_i is even for all i then there exist self-dual codes of all lengths;
(2) If for all i either $\mathbb{F}_i$ has characteristic 2 or $1 \pmod 4$ or the index of stability is even, then self-dual codes exist for all even lengths;
(3) If $\mathbb{F}_i$ has characteristic $3 \pmod 4$ for some i then there exist self-dual codes over R of all lengths congruent to $0 \pmod 4$.

Free Self-Dual Codes

Theorem

Let R be a local ring with characteristic congruent to $1 \pmod 4$ then there exist free self-dual codes for all even lengths over R.

Free Self-Dual Codes

Proof
We know that there exists an element $a \in R$ such that $a^2 = -1$. Let C be a code generated by $(1, a)$. Then $|C| = |R|$, C is free, and C is self-orthogonal. We know that

$$|C| \cdot |C^{\perp}| = |R|^2,$$

since R is a Frobenius ring.

Free Self-Dual Codes

Proof
We know that there exists an element $a \in R$ such that $a^2 = -1$. Let C be a code generated by $(1, a)$. Then $|C| = |R|$, C is free, and C is self-orthogonal. We know that

$$|C| \cdot |C^{\perp}| = |R|^2,$$

since R is a Frobenius ring.

This implies that $|C^{\perp}| = |R|$, and so C is a self-dual code of length 2. The direct product of this code with itself gives self-dual codes of all even lengths. **QED**

Self-Dual Codes

Theorem

Let R be a local ring with characteristic congruent to $3 \pmod 4$ *then there exist self-dual codes for all lengths congruent to* $0 \pmod 4$ *over R.*

Self-Dual Codes

Theorem

Let R be a finite local ring with the unique maximal ideal $\mathfrak{m}$ and the even nilpotency index e of R. Then
(i) if $R/\mathfrak{m}$ has characteristic $1 \pmod 4$ then there exist free and non-free self-dual codes of length n for all $n \equiv 0 \pmod 2$;
(ii) if $R/\mathfrak{m}$ has characteristic $3 \pmod 4$ then there exist free and non-free self-dual codes of length n for all $n \equiv 0 \pmod 4$.

Self-Dual Codes

Corollary

Let R be a finite Frobenius ring whose residue fields (with respect to the maximal ideals) are $\mathbb{F}_1, \ldots, \mathbb{F}_k$. Then
(1) If $\mathbb{F}_i$ has characteristic $1 \pmod 4$ for all i then there exist free self-dual codes of all even lengths.
(2) If for each i, $\mathbb{F}_i$ has characteristic 1 or $3 \pmod 4$, then there exist free self-dual codes of all lengths congruent to $0 \pmod 4$.

Generalization of Type II

A ring R is even if there exist a ring S and a surjective homomorphism $\eta : S \to R$ such that if $s \in \mathrm{Ker}(\eta)$ then $2s = 0$ and $s^2 = 0$ in S.

Generalization of Type II

We know that $S/\mathrm{Ker}(\eta) \cong R$. We denote this isomorphism by $\bar{\eta}$. Namely

$$\bar{\eta} : S/\mathrm{Ker}(\eta) \to R, \quad s + \mathrm{Ker}(\eta) \mapsto \eta(s).$$

Generalization of Type II

For each $a \in R$, there exist $s \in S$ such that $a = \eta(s) = \bar{\eta}(s + \mathrm{Ker}(\eta))$. If $s' \in s + \mathrm{Ker}(\eta)$, then $s' = s + z$, where $z \in \mathrm{Ker}(\eta)$. Then we have that

$$s'^2 = (s+z)^2 = s^2 + 2sz + z^2.$$

Since $z \in \mathrm{Ker}(\eta)$, we have that $2sz = z^2 = 0$ in S, and this gives that $s'^2 = s^2$. This means that for any $a \in R$, although we may have that $s \neq s'$, where both s and s' correspond to a, we must have that $s'^2 = s^2$ in S.

Example of R and S

For example, considering the rings $\mathbb{Z}_3$ and $\mathbb{Z}_6$.

Example of R and S

For example, considering the rings $\mathbb{Z}_3$ and $\mathbb{Z}_6$.
The choice of $\mathbb{Z}_6$ is a natural choice for the Euclidean weight of $\mathbb{Z}_3$.

Example of R and S

For example, considering the rings $\mathbb{Z}_3$ and $\mathbb{Z}_6$.
The choice of $\mathbb{Z}_6$ is a natural choice for the Euclidean weight of $\mathbb{Z}_3$. There is a natural surjective homomorphism $\eta : \mathbb{Z}_6 \to \mathbb{Z}_3$ with $\mathbb{Z}_6/\mathrm{Ker}(\eta) \cong \mathbb{Z}_3$. Notice that $3 \in \mathrm{Ker}(\eta)$ and $2 \cdot 3 = 0$ in $\mathbb{Z}_6$, but $3^2 = 3 \neq 0 \in \mathbb{Z}_6$.

Example of R and S

For example, considering the rings $\mathbb{Z}_3$ and $\mathbb{Z}_6$.
The choice of $\mathbb{Z}_6$ is a natural choice for the Euclidean weight of $\mathbb{Z}_3$. There is a natural surjective homomorphism $\eta : \mathbb{Z}_6 \to \mathbb{Z}_3$ with $\mathbb{Z}_6/\mathrm{Ker}(\eta) \cong \mathbb{Z}_3$. Notice that $3 \in \mathrm{Ker}(\eta)$ and $2 \cdot 3 = 0$ in $\mathbb{Z}_6$, but $3^2 = 3 \neq 0 \in \mathbb{Z}_6$.
This has the following implication. The vector $(1, 1, 2)$ has Euclidean weight 0 in $\mathbb{Z}_6$ but $(1, 1, 2) + (1, 1, 2) = (2, 2, 1)$, which has Euclidean weight 3 in $\mathbb{Z}_6$ and hence the sum of two doubly-even vectors is not necessarily doubly-even. So $\mathbb{Z}_3$ is not an even ring.

Example of R and S

Let R be a finite chain ring with nilpotency index e such that $R/(\gamma) \cong \mathbb{F}_{2^r}$, where $\mathbb{F}_{2^r}$ denotes the finite field with 2^r elements. We construct S by using R as follows:

$$S = R + R\gamma = \{a + b\gamma \mid a, b \in R\},$$

where γ^e is not zero in S, but γ^{e+1} is zero in S.

Euclidean Weight

Let a be an element of an even ring R, the Euclidean weight of a, denoted by $\mathrm{Euc}(a)$, is defined to be $(\epsilon(a))^2 = s^2$, where $a = \bar{\eta}(s + \mathrm{Ker}(\eta))$. For a vector $v = (v_1, \cdots, v_n) \in R^n$ the Euclidean weight of v is $\mathrm{Euc}(v) = \sum_{i=1}^{n} \mathrm{Euc}(v_i)$.

Type II

A code C of length n over an even ring R is called Type II if C is self-dual and

$$\mathrm{Euc}(c) = \sum_{i=1}^{n} \mathrm{Euc}(c_i) = 0 \in S, \ \text{for all } c = (c_1, \cdots, c_n) \in C.$$

Even rings

Theorem

Let $R = \mathrm{CRT}(R_1, \cdots, R_t)$, *where* R_i *are finite rings. If there exists* i, $1 \leq i \leq t$, *such that* R_i *is even, then* R *is even.*

Type II

Theorem

Let $R = \mathrm{CRT}(R_1, \ldots, R_t)$ *with* R_i *even for some* i*. If* C_j *is self-dual over* R_j *for all* j *and* C_i *is Type II over* R_i*, then* $\mathrm{CRT}(C_1, \ldots, C_t)$ *is a Type II code over* R*.*