Counting Codes Over Rings With A Given Hull

Esengül Saltürk

Atlas University, İstanbul, Türkiye

joint work with
Steven T. Dougherty
University of Scranton, USA

Noncommutative Rings and Their Applications VIII,
Université d'Artois, Lens-France
August 30, 2023

Problem

Problem. Let R be a ring of order 4. Then what is the number of linear (additive) codes over R containing a hull of given size?

When R is a field, the number for linear codes is given by Sendrier[11].

Problem

Problem. Let R be a ring of order 4. Then what is the number of linear (additive) codes over R containing a hull of given size?

When R is a field, the number for linear codes is given by Sendrier[11].

Definitions

- A linear code over a ring R is a submodule of R^n.

Euclidean inner product

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

The orthogonal of C

$$C^\perp = \{\mathbf{x} \in R^n | [\mathbf{x}, \mathbf{y}] = 0 \text{ for all } y \in C\}.$$

If R is a finite commutative Frobenius ring, then $|C||C^\perp| = |R|^n$, by Wood[13].

- A linear code over a ring R is a submodule of R^n.

Euclidean inner product

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

The orthogonal of C

$$C^{\perp} = \{\mathbf{x} \in R^n | [\mathbf{x}, \mathbf{y}] = 0 \text{ for all } y \in C\}.$$

If R is a finite commutative Frobenius ring, then $|C||C^{\perp}| = |R|^n$, by Wood[13].

Hull of a Code

The Hull of a linear code C is

$$Hull(C) = C \cap C^{\perp}.$$

- So, it is a self-orthogonal code.
- The hull satisfies $1 \leq |Hull(C)| \leq \sqrt{|R|^n}$.

Important for. Determining the complexity of algorithms for permutation equivalence of linear codes and the automorphism group of a linear code.

These algorithms are very effective if the size of the hull is small.

Hull of a Code

The Hull of a linear code C is

$$Hull(C) = C \cap C^{\perp}.$$

- So, it is a self-orthogonal code.
- The hull satisfies $1 \leq |Hull(C)| \leq \sqrt{|R|^n}$.

Important for. Determining the complexity of algorithms for permutation equivalence of linear codes and the automorphism group of a linear code.

These algorithms are very effective if the size of the hull is small.

Hull of a Code

The Hull of a linear code C is

$$Hull(C) = C \cap C^{\perp}.$$

- So, it is a self-orthogonal code.
- The hull satisfies $1 \leq |Hull(C)| \leq \sqrt{|R|^n}$.

Important for. Determining the complexity of algorithms for permutation equivalence of linear codes and the automorphism group of a linear code.

These algorithms are very effective if the size of the hull is small.

Hull of a Code

- It was first introduced in the work of Assmus and Key to study the codes of finite projective and affine planes, 1990, [1].
- Dougherty used the hull for finite nets, 1993, 1994, [3], [4].
- Sendrier, calculated the number of distinct linear codes over finite fields which have a hull of given dimension were given. He also proved that the expected dimension of the hull of a linear code is a constant when the parameters n and k go to infinity, 1997, [11].

- An additive code over a ring R is an additive subgroup of R^n.

- Let G be a group. Then the set of all characters of G is denoted by $\widehat{G}$.
- Then $\phi : G \to \widehat{G}$ is an isomorphism, with $\phi(g_i) = \chi_{g_i},\ g_i \in G$.

Let C be a code over G with a duality M (a group isomorphism)

$$[\mathbf{g}, \mathbf{c}]_M = \prod \chi_{g_i}(c_i).$$

The orthogonal of C

$$C^M = \{(g_1, g_2, \ldots, g_n) | \prod_{i=1}^{n} \chi_{g_i}(c_i) = 1 \text{ for all } (c_1, \ldots, c_n) \in C\}$$

We have $|C||C^M| = |G|^n$, Dougherty[2].

Codes over Rings
Additive codes

- An additive code over a ring R is an additive subgroup of R^n.

- Let G be a group. Then the set of all characters of G is denoted by $\widehat{G}$.
- Then $\phi : G \to \widehat{G}$ is an isomorphism, with $\phi(g_i) = \chi_{g_i},\ g_i \in G$.

Let C be a code over G with a duality M (a group isomorphism)

$$[\mathbf{g}, \mathbf{c}]_M = \prod \chi_{g_i}(c_i).$$

The orthogonal of C

$$C^M = \{(g_1, g_2, \ldots, g_n) | \prod_{i=1}^{n} \chi_{g_i}(c_i) = 1 \text{ for all } (c_1, \ldots, c_n) \in C\}$$

We have $|C||C^M| = |G|^n$, Dougherty[2].

- An additive code over a ring R is an additive subgroup of R^n.
- Let G be a group. Then the set of all characters of G is denoted by $\widehat{G}$.
- Then $\phi : G \to \widehat{G}$ is an isomorphism, with $\phi(g_i) = \chi_{g_i},\ g_i \in G$.

Let C be a code over G with a duality M (a group isomorphism)

$$[\mathbf{g}, \mathbf{c}]_M = \prod \chi_{g_i}(c_i).$$

The orthogonal of C

$$C^M = \{(g_1, g_2, \ldots, g_n) | \prod_{i=1}^{n} \chi_{g_i}(c_i) = 1 \text{ for all } (c_1, \ldots, c_n) \in C\}$$

We have $|C||C^M| = |G|^n$, Dougherty[2].

- An additive code over a ring R is an additive subgroup of R^n.

- Let G be a group. Then the set of all characters of G is denoted by $\widehat{G}$.
- Then $\phi : G \to \widehat{G}$ is an isomorphism, with $\phi(g_i) = \chi_{g_i},\ g_i \in G$.

Let C be a code over G with a duality M (a group isomorphism)

$$[\mathbf{g}, \mathbf{c}]_M = \prod \chi_{g_i}(c_i).$$

The orthogonal of C

$$C^M = \{(g_1, g_2, \ldots, g_n) | \prod_{i=1}^{n} \chi_{g_i}(c_i) = 1 \text{ for all } (c_1, \ldots, c_n) \in C\}$$

We have $|C||C^M| = |G|^n$, Dougherty[2].

Hull of a Code

Additive codes

The Hull of an additive code C is

$$Hull_M(C) = C \cap C^M.$$

Rings of order 4

Rings and Gray maps

$$Rings: \quad \mathbb{F}_4, \quad \mathbb{Z}_4, \quad \mathbb{F}_2[u]/\langle u^2 \rangle, \quad \mathbb{F}_2[v]/\langle v^2+v \rangle.$$

- Codes over $\mathbb{F}_4$

Generating matrix $(I_k \, |A)$.

$\alpha : \mathbb{F}_4 \to \mathbb{F}_2^2$ such that $\alpha(a+b\omega) = (a,b)$.

$$\alpha(C^\perp) = \alpha(C)^\perp.$$

- Codes over $\mathbb{Z}_4$

Generating matrix $G = \begin{pmatrix} I_{k_0} & A_{0,1} & A_{0,2} \\ 0 & 2I_{k_1} & 2A_{1,2} \end{pmatrix}$.

Type: (k_0, k_1)

Gray map: $\phi : \mathbb{Z}_4 \to \mathbb{F}_2^2$ such that $\phi(a+2b) = (b, a+b)$ (non-linear)

Rings and Gray maps

$$\textit{Rings}: \quad \mathbb{F}_4, \quad \mathbb{Z}_4, \quad \mathbb{F}_2[u]/\langle u^2\rangle, \quad \mathbb{F}_2[v]/\langle v^2+v\rangle.$$

- Codes over $\mathbb{F}_4$

Generating matrix $(I_k \,|A)$.

$\alpha : \mathbb{F}_4 \to \mathbb{F}_2^2$ such that $\alpha(a+b\omega) = (a,b)$.

$$\alpha(C^\perp) = \alpha(C)^\perp.$$

- Codes over $\mathbb{Z}_4$

Generating matrix $G = \begin{pmatrix} I_{k_0} & A_{0,1} & A_{0,2} \\ 0 & 2I_{k_1} & 2A_{1,2} \end{pmatrix}$.

Type: (k_0, k_1)

Gray map: $\phi : \mathbb{Z}_4 \to \mathbb{F}_2^2$ such that $\phi(a+2b) = (b, a+b)$ (non-linear)

Rings and Gray maps

$$\textit{Rings}: \quad \mathbb{F}_4, \quad \mathbb{Z}_4, \quad \mathbb{F}_2[u]/\langle u^2 \rangle, \quad \mathbb{F}_2[v]/\langle v^2+v \rangle.$$

- Codes over $\mathbb{F}_4$

Generating matrix $(I_k \, | A)$.

$\alpha : \mathbb{F}_4 \to \mathbb{F}_2^2$ such that $\alpha(a+b\omega) = (a,b)$.

$$\alpha(C^{\perp}) = \alpha(C)^{\perp}.$$

- Codes over $\mathbb{Z}_4$

Generating matrix $G = \begin{pmatrix} I_{k_0} & A_{0,1} & A_{0,2} \\ 0 & 2I_{k_1} & 2A_{1,2} \end{pmatrix}$.

Type: (k_0, k_1)

Gray map: $\phi : \mathbb{Z}_4 \to \mathbb{F}_2^2$ such that $\phi(a+2b) = (b, a+b)$ (non-linear)

Rings and Gray maps

- Codes over $\mathbb{F}_2[u]/\langle u^2 \rangle = \mathbb{F}_2 + u\mathbb{F}_2$

Generating matrix $G = \begin{pmatrix} I_{k_0} & A_{0,1} & A_{0,2} \\ 0 & uI_{k_1} & uA_{1,2} \end{pmatrix}$

Type: (k_0, k_1)

Gray map: $\psi : \mathbb{F}_2[u]/\langle u^2 \rangle \to \mathbb{F}_2^2$ such that $\psi(a + bu) = (b, a + b)$ (linear)

$$\psi(C^\perp) = \psi(C)^\perp.$$

- Codes over $\mathbb{F}_2[v]/\langle v^2 + v \rangle = \mathbb{F}_2 + v\mathbb{F}_2$

No generating matrix in standard form. No type.

Gray map: $\beta : \mathbb{F}_2[v]/\langle v^2 + v \rangle \to \mathbb{F}_2^2$ such that $\beta(a + bv) = (a, a + b)$. (isomorphism)

$$\beta(C^\perp) = \beta(C)^\perp.$$

Rings and Gray maps

- Codes over $\mathbb{F}_2[u]/\langle u^2\rangle = \mathbb{F}_2 + u\mathbb{F}_2$

Generating matrix $G = \begin{pmatrix} I_{k_0} & A_{0,1} & A_{0,2} \\ 0 & uI_{k_1} & uA_{1,2} \end{pmatrix}$

Type: (k_0, k_1)

Gray map: $\psi : \mathbb{F}_2[u]/\langle u^2\rangle \to \mathbb{F}_2^2$ such that $\psi(a + bu) = (b, a + b)$ (linear)

$$\psi(C^\perp) = \psi(C)^\perp.$$

- Codes over $\mathbb{F}_2[v]/\langle v^2 + v\rangle = \mathbb{F}_2 + v\mathbb{F}_2$

No generating matrix in standard form. No type.

Gray map: $\beta : \mathbb{F}_2[v]/\langle v^2 + v\rangle \to \mathbb{F}_2^2$ such that $\beta(a + bv) = (a, a + b)$.
(isomorphism)

$$\beta(C^\perp) = \beta(C)^\perp.$$

Number of Codes

Number of Codes over Fields

Gaussian binomials

The number of subcodes of dimension k of a code of dimension n is given by a well-known formula:

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \frac{(q^n - 1)(q^{n-1} - 1)\cdots(q^{n-k+1} - 1)}{(q^k - 1)(q^{k-1} - 1)\cdots(q - 1)}.$$

Theorem

[6] Let R be one of the rings $\mathbb{Z}_4$ *or* $\mathbb{F}_2 + u\mathbb{F}_2$, $u^2 = 0$, *with type* (k_0, k_1), *with maximal ideal* $|R/m| = q = 2$ *and nilpotency* $e = 2$. *The number of linear codes over R is given by the following formula,*

$$\begin{bmatrix} n \\ k_0, k_1 \end{bmatrix}_{q,e} = \begin{bmatrix} n \\ k_0, k_1 \end{bmatrix}_{2,2} = \frac{\prod_{i=0}^{k_0-1} (2^{2n} - 2^{n+i}) \prod_{j=0}^{k_1-1} (2^n - 2^{k_0+j})}{\prod_{i=0}^{k_0-1} (2^{2k_0+k_1} - 2^{k_0+k_1+i}) \prod_{j=0}^{k_1-1} (2^{k_0+k_1} - 2^{k_0+j})}.$$

Number of Self-Orthogonal Codes

Theorem

[8, 9, 10] Let n and q be positive even integers and $k \leq n/2$*. The number of self-orthogonal codes over* $\mathbb{F}_q$ *of length n and dimension k is*

$$\sigma_{n,k} = \frac{q^{n-k}-1}{q^n-1} \prod_{i=1}^{k} \frac{q^{n-2i+2}-1}{q^i-1}.$$

The Number of Codes with the Hull of Given Dimension

Lemma

[11] Let C be a linear code over $\mathbb{F}_q$ of length n and dimension k. The number of self-orthogonal codes V of length n and dimension l such that $V \subseteq Hull(C)$ is the Gaussian binomial $\begin{bmatrix} dim(Hull(C)) \\ l \end{bmatrix}_q$.

Lemma

[11] Let V be a self-orthogonal code over $\mathbb{F}_q$ of length n and dimension l. The number of linear codes C over $\mathbb{F}_q$ of length n and dimension k such that $V \subseteq Hull(C)$ is $\begin{bmatrix} n-2l \\ k-l \end{bmatrix}_q$.

The Number of Codes with the Hull of Given Dimension

Theorem

[11] Let $\sigma_{n,i}$ denote the number of self-orthogonal codes over $\mathbb{F}_q$ of length n and dimension i. Let $k \leq n/2$ and $l \leq k$. The number of linear codes over $\mathbb{F}_q$ of length n and dimension k where the dimension of the hull is l is

$$\sum_{i=l}^{k} \begin{bmatrix} n-2i \\ k-i \end{bmatrix}_q \begin{bmatrix} i \\ l \end{bmatrix}_q (-1)^{i-l} q^{\binom{i-l}{2}} \sigma_{n,i}.$$

Results I

Number of Additive Codes

Duality on the additive group of $\mathbb{F}_4$

M_E	0	1	ω	$1+\omega$
0	1	1	1	1
1	1	-1	1	-1
ω	1	1	-1	-1
$1+\omega$	1	-1	-1	1

	00	10	01	11
00	0	0	0	0
10	0	1	0	1
01	0	0	1	1
11	0	1	1	0

Lemma
Let $\mathbf{x}, \mathbf{y} \in \mathbb{F}_4^n$. *Then* $[\mathbf{v}, \mathbf{w}]_{M_E} = 1$ *if and only if* $[\alpha(\mathbf{v}), \alpha(\mathbf{w})] = 0$.

Theorem
Let C *be an additive code over* $\mathbb{F}_4$. *Then*

$$Hull(\alpha(C)) = \alpha(Hull_{M_E}(C)).$$

Duality on the additive group of $\mathbb{F}_4$

M_E	0	1	ω	$1+\omega$
0	1	1	1	1
1	1	-1	1	-1
ω	1	1	-1	-1
$1+\omega$	1	-1	-1	1

	00	10	01	11
00	0	0	0	0
10	0	1	0	1
01	0	0	1	1
11	0	1	1	0

Lemma

Let $\mathbf{x}, \mathbf{y} \in \mathbb{F}_4^n$. *Then* $[\mathbf{v}, \mathbf{w}]_{M_E} = 1$ *if and only if* $[\alpha(\mathbf{v}), \alpha(\mathbf{w})] = 0$.

Theorem

Let C *be an additive code over* $\mathbb{F}_4$. *Then*

$$Hull(\alpha(C)) = \alpha(Hull_{M_E}(C)).$$

Duality on the additive group of $\mathbb{F}_4$

M_E	0	1	ω	$1+\omega$
0	1	1	1	1
1	1	-1	1	-1
ω	1	1	-1	-1
$1+\omega$	1	-1	-1	1

	00	10	01	11
00	0	0	0	0
10	0	1	0	1
01	0	0	1	1
11	0	1	1	0

Lemma
Let $\mathbf{x}, \mathbf{y} \in \mathbb{F}_4^n$. Then $[\mathbf{v}, \mathbf{w}]_{M_E} = 1$ if and only if $[\alpha(\mathbf{v}), \alpha(\mathbf{w})] = 0$.

Theorem
Let C be an additive code over $\mathbb{F}_4$. Then

$$Hull(\alpha(C)) = \alpha(Hull_{M_E}(C)).$$

Duality on the additive group of $\mathbb{F}_4$

M_E	0	1	ω	$1+\omega$
0	1	1	1	1
1	1	-1	1	-1
ω	1	1	-1	-1
$1+\omega$	1	-1	-1	1

	00	10	01	11
00	0	0	0	0
10	0	1	0	1
01	0	0	1	1
11	0	1	1	0

Lemma

Let $\mathbf{x}, \mathbf{y} \in \mathbb{F}_4^n$. *Then* $[\mathbf{v}, \mathbf{w}]_{M_E} = 1$ *if and only if* $[\alpha(\mathbf{v}), \alpha(\mathbf{w})] = 0$.

Theorem

Let C be an additive code over $\mathbb{F}_4$. Then

$$Hull(\alpha(C)) = \alpha(Hull_{M_E}(C)).$$

Theorem

The number of additive codes over $\mathbb{F}_4$ of length n where $Hull_{M_E}(C)$ has size 2^k is equal to the number of binary linear codes of length $2n$ with hulls of dimension k.

Theorem

The number of additive codes over $\mathbb{F}_4$ of length n and size 2^k whose hull with respect to M_E has size 2^l with $l \leq k$ and $k \leq 2n/2$ is

$$\sum_{i=l}^{k} \begin{bmatrix} 2n-2i \\ k-i \end{bmatrix}_2 \begin{bmatrix} i \\ l \end{bmatrix}_2 (-1)^{i-l} 2^{\binom{i-l}{2}} \sigma_{2n,i},$$

where $\sigma_{n,i}$ is the number of binary self-orthogonal codes of length n and dimension i.

Theorem

The number of additive codes over $\mathbb{F}_4$ of length n where $Hull_{M_E}(C)$ has size 2^k is equal to the number of binary linear codes of length $2n$ with hulls of dimension k.

Theorem

The number of additive codes over $\mathbb{F}_4$ of length n and size 2^k whose hull with respect to M_E has size 2^l with $l \leq k$ and $k \leq 2n/2$ is

$$\sum_{i=l}^{k} \begin{bmatrix} 2n-2i \\ k-i \end{bmatrix}_2 \begin{bmatrix} i \\ l \end{bmatrix}_2 (-1)^{i-l} 2^{\binom{i-l}{2}} \sigma_{2n,i},$$

where $\sigma_{n,i}$ is the number of binary self-orthogonal codes of length n and dimension i.

Example

Let $n = 2$, $k = 2$ and $l = 1$. $\sigma_{4,1} = 7$ and $\sigma_{4,2} = 3$. The number of additive codes over $\mathbb{F}_4 = \{0, 1, w, 1 + w\}$ of length 2 and size 2^2 whose hull has size 2^1 is 12 :

$$\begin{pmatrix} 1 & 0 \\ w & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ w & w \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1+w \end{pmatrix}, \begin{pmatrix} w & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} w & 0 \\ 1 & w \end{pmatrix}, \begin{pmatrix} w & 0 \\ 0 & 1+w \end{pmatrix},$$

$$\begin{pmatrix} 0 & 1 \\ 1+w & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & w \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ w & w \end{pmatrix}, \begin{pmatrix} 0 & w \\ 1+w & 0 \end{pmatrix}, \begin{pmatrix} 0 & w \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & w \\ w & 1 \end{pmatrix}.$$

Ratio of The Number of Linear Codes and The Number of Additive Codes

Theorem

The ratio of the number of linear codes over $\mathbb{F}_4$ of length n and dimension k and the number of additive codes over $\mathbb{F}_4$ of length n and size 4^k goes to 0 as n goes to infinity:

$$\lim_{n\to\infty} \frac{\begin{bmatrix} n \\ k \end{bmatrix}_4}{\begin{bmatrix} 2n \\ 2k \end{bmatrix}_2} = 0.$$

Ratio of The Number of Linear Codes and The Number of Additive Codes

Theorem

The ratio of the number of linear codes over $\mathbb{F}_4$ *of length n and dimension k and the number of additive codes over* $\mathbb{F}_4$ *of length n and size* 4^k *goes to* 0 *as n goes to infinity:*

$$\lim_{n\to\infty} \frac{\begin{bmatrix} n \\ k \end{bmatrix}_4}{\begin{bmatrix} 2n \\ 2k \end{bmatrix}_2} = 0.$$

Ratio of The Number of Linear Codes and The Number of Additive Codes

Theorem

The ratio of the number of linear codes over $\mathbb{F}_4$ *of length n and dimension k with a given hull of dimension l and the number of additive codes over* $\mathbb{F}_4$ *of length n and size* 4^k *whose hull with respect to* M_E *has size* 4^l, $l \leq k$, *goes to* 0 *as n goes to infinity:*

$$\lim_{n\to\infty} \frac{\sum_{i=l}^{k} \begin{bmatrix} n-2i \\ k-i \end{bmatrix}_4 \begin{bmatrix} i \\ l \end{bmatrix}_4 (-1)^{i-l} 4^{\binom{i-l}{2}} \sigma_{n,i}}{\sum_{j=l}^{k} \begin{bmatrix} 2n-4j \\ 2k-2j \end{bmatrix}_2 \begin{bmatrix} 2j \\ 2l \end{bmatrix}_2 (-1)^{2j-2l} 2^{\binom{2j-2l}{2}} \sigma_{2n,2j}} = 0.$$

Ratio of The Number of Linear Codes and The Number of Additive Codes

Theorem

The ratio of the number of linear codes over $\mathbb{F}_4$ *of length n and dimension k with a given hull of dimension l and the number of additive codes over* $\mathbb{F}_4$ *of length n and size* 4^k *whose hull with respect to* M_E *has size* 4^l, $l \le k$, *goes to* 0 *as n goes to infinity:*

$$\lim_{n\to\infty} \frac{\sum_{i=l}^{k} \begin{bmatrix} n-2i \\ k-i \end{bmatrix}_4 \begin{bmatrix} i \\ l \end{bmatrix}_4 (-1)^{i-l} 4^{\binom{i-l}{2}} \sigma_{n,i}}{\sum_{j=l}^{k} \begin{bmatrix} 2n-4j \\ 2k-2j \end{bmatrix}_2 \begin{bmatrix} 2j \\ 2l \end{bmatrix}_2 (-1)^{2j-2l} 2^{\binom{2j-2l}{2}} \sigma_{2n,2j}} = 0.$$

Duality on the additive group of $\mathbb{F}_2[v]/\langle v^2+v \rangle$

M_E	0	1	v	$1+v$
0	1	1	1	1
1	1	1	−1	−1
v	1	−1	−1	1
$1+v$	1	−1	1	−1

	0	11	01	10
0	0	0	0	0
11	0	0	1	1
01	0	1	1	0
10	0	1	0	1

Lemma

Let $\mathbf{v}, \mathbf{w} \in \mathbb{F}_2[v]/\langle v^2+v \rangle^n$. Then $[\mathbf{v}, \mathbf{w}]_M = 1$ if and only if $[\beta(\mathbf{v}), \beta(\mathbf{w})] = 0$.

Theorem

Let C be an additive code over $\mathbb{F}_2[v]/\langle v^2+v \rangle$. Then

$$Hull(\beta(C)) = \beta(Hull_{M_E}(C)).$$

Duality on the additive group of $\mathbb{F}_2[v]/\langle v^2 + v\rangle$

M_E	0	1	v	$1+v$
0	1	1	1	1
1	1	1	-1	-1
v	1	-1	-1	1
$1+v$	1	-1	1	-1

	0	11	01	10
0	0	0	0	0
11	0	0	1	1
01	0	1	1	0
10	0	1	0	1

Lemma
Let $\mathbf{v}, \mathbf{w} \in \mathbb{F}_2[v]/\langle v^2 + v\rangle^n$. *Then* $[\mathbf{v}, \mathbf{w}]_M = 1$ *if and only if* $[\beta(\mathbf{v}), \beta(\mathbf{w})] = 0$.

Theorem
Let C *be an additive code over* $\mathbb{F}_2[v]/\langle v^2 + v\rangle$. *Then*

$$Hull(\beta(C)) = \beta(Hull_{M_E}(C)).$$

Duality on the additive group of $\mathbb{F}_2[v]/\langle v^2+v\rangle$

M_E	0	1	v	$1+v$
0	1	1	1	1
1	1	1	−1	−1
v	1	−1	−1	1
$1+v$	1	−1	1	−1

	0	11	01	10
0	0	0	0	0
11	0	0	1	1
01	0	1	1	0
10	0	1	0	1

Lemma
Let $\mathbf{v},\mathbf{w}\in\mathbb{F}_2[v]/\langle v^2+v\rangle^n$. *Then* $[\mathbf{v},\mathbf{w}]_M=1$ *if and only if* $[\beta(\mathbf{v}),\beta(\mathbf{w})]=0$.

Theorem
Let C be an additive code over $\mathbb{F}_2[v]/\langle v^2+v\rangle$. Then

$$Hull(\beta(C))=\beta(Hull_{M_E}(C)).$$

Duality on the additive group of $\mathbb{F}_2[v]/\langle v^2+v\rangle$

M_E	0	1	v	$1+v$
0	1	1	1	1
1	1	1	−1	−1
v	1	−1	−1	1
$1+v$	1	−1	1	−1

	0	11	01	10
0	0	0	0	0
11	0	0	1	1
01	0	1	1	0
10	0	1	0	1

Lemma
Let $\mathbf{v}, \mathbf{w} \in \mathbb{F}_2[v]/\langle v^2+v\rangle^n$. *Then* $[\mathbf{v}, \mathbf{w}]_M = 1$ *if and only if* $[\beta(\mathbf{v}), \beta(\mathbf{w})] = 0$.

Theorem
Let C *be an additive code over* $\mathbb{F}_2[v]/\langle v^2+v\rangle$. *Then*

$$Hull(\beta(C)) = \beta(Hull_{M_E}(C)).$$

Theorem

The number of additive codes over $\mathbb{F}_2[v]/\langle v^2+v\rangle$ of length n where $Hull_{M_E}(C)$ has size 2^k is equal to the number of binary linear codes of length $2n$ with hulls of dimension k.

Theorem

The number of additive codes over $\mathbb{F}_2[v]/\langle v^2+v\rangle$ of length n and size 2^k whose hull size is 2^l, $l \le k$, is

$$\sum_{i=l}^{k} \begin{bmatrix} 2n-2i \\ k-i \end{bmatrix}_2 \begin{bmatrix} i \\ l \end{bmatrix}_2 (-1)^{i-l} 2^{\binom{i-l}{2}} \sigma_{2n,i},$$

where $\sigma_{n,i}$ is the number of binary self-orthogonal codes of length n and dimension i.

Theorem

The number of additive codes over $\mathbb{F}_2[v]/\langle v^2+v\rangle$ of length n where $Hull_{M_E}(C)$ has size 2^k is equal to the number of binary linear codes of length $2n$ with hulls of dimension k.

Theorem

The number of additive codes over $\mathbb{F}_2[v]/\langle v^2+v\rangle$ of length n and size 2^k whose hull size is 2^l, $l \le k$, is

$$\sum_{i=l}^{k} \begin{bmatrix} 2n-2i \\ k-i \end{bmatrix}_2 \begin{bmatrix} i \\ l \end{bmatrix}_2 (-1)^{i-l} 2^{\binom{i-l}{2}} \sigma_{2n,i},$$

where $\sigma_{n,i}$ is the number of binary self-orthogonal codes of length n and dimension i.

Example

Let $n = 2$, $k = 2$ and $l = 1$. $\sigma_{4,1} = 7$ and $\sigma_{4,2} = 3$. The number of additive codes over $\mathbb{F}_2[v]/\langle v^2 + v\rangle = \{0, 1, v, 1 + v\}$, $v^2 = v$, of length 2 and size 2^2 whose hull has size 2^1 is 12 :

$$\begin{pmatrix} 1+v & 0 \\ v & 1+v \end{pmatrix}, \begin{pmatrix} 1+v & 0 \\ v & v \end{pmatrix}, \begin{pmatrix} 1+v & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} v & 0 \\ 1+v & 1+v \end{pmatrix},$$

$$\begin{pmatrix} v & 0 \\ 1+v & v \end{pmatrix}, \begin{pmatrix} v & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1+v \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1+v \\ 1+v & v \end{pmatrix},$$

$$\begin{pmatrix} 0 & 1+v \\ v & v \end{pmatrix}, \begin{pmatrix} 0 & v \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & v \\ 1+v & 1+v \end{pmatrix}, \begin{pmatrix} 0 & v \\ v & 1+v \end{pmatrix}.$$

Duality on the additive group of $\mathbb{F}_2[u]/\langle u^2\rangle$

	0	1	u	$1+u$
0	1	1	1	1
1	1	−1	1	−1
u	1	−1	1	−1
$1+u$	1	1	−1	−1

	00	01	11	10
00	0	0	0	0
01	0	1	0	1
11	0	1	0	1
10	0	0	1	1

Lemma
Let $\mathbf{v}, \mathbf{w} \in \mathbb{F}_2[u]/\langle u^2\rangle^n$. *Then* $[\mathbf{v}, \mathbf{w}]_M = 1$ *if and only if* $[\psi(\mathbf{v}), \beta(\mathbf{w})] = 0$.

Theorem
Let C be an additive code over $\mathbb{F}_2[u]/\langle u^2\rangle$. *Then*

$$Hull(\psi(C)) = \psi(Hull_{M_E}(C)).$$

Duality on the additive group of $\mathbb{F}_2[u]/\langle u^2 \rangle$

	0	1	u	$1+u$
0	1	1	1	1
1	1	-1	1	-1
u	1	-1	1	-1
$1+u$	1	1	-1	-1

	00	01	11	10
00	0	0	0	0
01	0	1	0	1
11	0	1	0	1
10	0	0	1	1

Lemma
Let $\mathbf{v}, \mathbf{w} \in \mathbb{F}_2[u]/\langle u^2 \rangle^n$. *Then* $[\mathbf{v}, \mathbf{w}]_M = 1$ *if and only if* $[\psi(\mathbf{v}), \beta(\mathbf{w})] = 0$.

Theorem
Let C *be an additive code over* $\mathbb{F}_2[u]/\langle u^2 \rangle$. *Then*

$$Hull(\psi(C)) = \psi(Hull_{M_E}(C)).$$

Duality on the additive group of $\mathbb{F}_2[u]/\langle u^2\rangle$

	0	1	u	$1+u$
0	1	1	1	1
1	1	−1	1	−1
u	1	−1	1	−1
$1+u$	1	1	−1	−1

	00	01	11	10
00	0	0	0	0
01	0	1	0	1
11	0	1	0	1
10	0	0	1	1

Lemma
Let $\mathbf{v}, \mathbf{w} \in \mathbb{F}_2[u]/\langle u^2\rangle^n$. *Then* $[\mathbf{v}, \mathbf{w}]_M = 1$ *if and only if* $[\psi(\mathbf{v}), \beta(\mathbf{w})] = 0$.

Theorem
Let C *be an additive code over* $\mathbb{F}_2[u]/\langle u^2\rangle$. *Then*

$$Hull(\psi(C)) = \psi(Hull_{M_E}(C)).$$

Duality on the additive group of $\mathbb{F}_2[u]/\langle u^2\rangle$

	0	1	u	$1+u$
0	1	1	1	1
1	1	−1	1	−1
u	1	−1	1	−1
$1+u$	1	1	−1	−1

	00	01	11	10
00	0	0	0	0
01	0	1	0	1
11	0	1	0	1
10	0	0	1	1

Lemma
Let $\mathbf{v}, \mathbf{w} \in \mathbb{F}_2[u]/\langle u^2\rangle^n$. *Then* $[\mathbf{v}, \mathbf{w}]_M = 1$ *if and only if* $[\psi(\mathbf{v}), \beta(\mathbf{w})] = 0$.

Theorem
Let C be an additive code over $\mathbb{F}_2[u]/\langle u^2\rangle$. *Then*

$$Hull(\psi(C)) = \psi(Hull_{M_E}(C)).$$

Theorem

The number of additive codes over $\mathbb{F}_2[u]/\langle u^2 \rangle$ of length n where $Hull_{M_E}(C)$ has size 2^k is equal to the number of binary linear codes of length $2n$ with hulls of dimension k.

Theorem

The number of additive codes over $\mathbb{F}_2[u]/\langle u^2 \rangle$, $u^2 = 0$, of length n and size 2^k whose hull size is 2^l, $l \leq k$, is

$$\sum_{i=l}^{k} \begin{bmatrix} 2n-2i \\ k-i \end{bmatrix} \begin{bmatrix} i \\ l \end{bmatrix} (-1)^{i-l} 2^{\binom{i-l}{2}} \sigma_{2n,i},$$

where $\sigma_{n,i}$ is the number of binary self-orthogonal codes of length n and dimension i.

Theorem

The number of additive codes over $\mathbb{F}_2[u]/\langle u^2\rangle$ of length n where $Hull_{M_E}(C)$ has size 2^k is equal to the number of binary linear codes of length 2n with hulls of dimension k.

Theorem

The number of additive codes over $\mathbb{F}_2[u]/\langle u^2\rangle$, $u^2 = 0$, of length n and size 2^k whose hull size is 2^l, $l \leq k$, is

$$\sum_{i=l}^{k} \begin{bmatrix} 2n-2i \\ k-i \end{bmatrix} \begin{bmatrix} i \\ l \end{bmatrix} (-1)^{i-l} 2^{\binom{i-l}{2}} \sigma_{2n,i},$$

where $\sigma_{n,i}$ is the number of binary self-orthogonal codes of length n and dimension i.

Example

Let $n = 2$, $k = 2$ and $l = 1$. $\sigma_{4,1} = 7$ and $\sigma_{4,2} = 3$. The number of additive codes over $\mathbb{F}_2[u]/\langle u^2 \rangle$ of length 2 and size 2^2 whose hull has size 2^1 is 12 :

$$\begin{pmatrix} 1+u & 0 \\ 1 & 1+u \end{pmatrix}, \begin{pmatrix} 1+u & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1+u & 0 \\ 0 & u \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1+u & 1+u \end{pmatrix},$$

$$\begin{pmatrix} 1 & 0 \\ 1+u & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & u \end{pmatrix}, \begin{pmatrix} 0 & 1+u \\ u & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1+u \\ 1+u & 1 \end{pmatrix},$$

$$\begin{pmatrix} 0 & 1+u \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ u & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1+u & 1+u \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1+u \end{pmatrix}.$$

Corollary for Additive Codes

Corollary

Let R be one of the rings $\mathbb{F}_4$, $\mathbb{F}_2[v]/\langle v^2 + v\rangle$ or $\mathbb{F}_2[u]/\langle u^2\rangle$. Then the number of additive codes over the ring R of length n and size 2^k whose hull size is 2^l is equal.

Results II

Number of Linear Codes

-Codes over $\mathbb{F}_2[v]/\langle v^2 + v\rangle = \mathbb{F}_2 + v\mathbb{F}_2$

Counting Codes over $\mathbb{F}_2[v]/\langle v^2 + v \rangle$

$$\beta : \mathbb{F}_2[v]/\langle v^2 + v \rangle \to \mathbb{F}_2^2 \quad \text{such that} \quad \beta(a + bv) = (a, a + b).$$

- The ring $\mathbb{F}_2[v]/\langle v^2 + v \rangle$ is isomorphic to $\mathbb{F}_2 \times \mathbb{F}_2$ via the Chinese Remainder Theorem.
- The map β is the inverse of CRT.
- Let $C = \beta^{-1}(C_1, C_2)$ be a code over $\mathbb{F}_2[v]/\langle v^2 + v \rangle$, then C is denoted by $CRT(C_1, C_2)$, where C_1 and C_2 are binary codes and C is uniquely determined by C_1 and C_2.

Counting Codes over $\mathbb{F}_2[v]/\langle v^2+v\rangle$

$$\beta : \mathbb{F}_2[v]/\langle v^2+v\rangle \to \mathbb{F}_2^2 \quad \text{such that} \quad \beta(a+bv) = (a, a+b).$$

- The ring $\mathbb{F}_2[v]/\langle v^2+v\rangle$ is isomorphic to $\mathbb{F}_2 \times \mathbb{F}_2$ via the Chinese Remainder Theorem.
- The map β is the inverse of CRT.
- Let $C = \beta^{-1}(C_1, C_2)$ be a code over $\mathbb{F}_2[v]/\langle v^2+v\rangle$, then C is denoted by $CRT(C_1, C_2)$, where C_1 and C_2 are binary codes and C is uniquely determined by C_1 and C_2.

Counting Codes over $\mathbb{F}_2[v]/\langle v^2+v \rangle$

$$\beta : \mathbb{F}_2[v]/\langle v^2+v \rangle \to \mathbb{F}_2^2 \quad \text{such that} \quad \beta(a+bv) = (a, a+b).$$

- The ring $\mathbb{F}_2[v]/\langle v^2+v \rangle$ is isomorphic to $\mathbb{F}_2 \times \mathbb{F}_2$ via the Chinese Remainder Theorem.
- The map β is the inverse of CRT.
- Let $C = \beta^{-1}(C_1, C_2)$ be a code over $\mathbb{F}_2[v]/\langle v^2+v \rangle$, then C is denoted by $CRT(C_1, C_2)$, where C_1 and C_2 are binary codes and C is uniquely determined by C_1 and C_2.

Counting Codes over $\mathbb{F}_2[v]/\langle v^2 + v\rangle$

$$\beta : \mathbb{F}_2[v]/\langle v^2 + v\rangle \to \mathbb{F}_2^2 \quad \text{such that} \quad \beta(a + bv) = (a, a + b).$$

- The ring $\mathbb{F}_2[v]/\langle v^2 + v\rangle$ is isomorphic to $\mathbb{F}_2 \times \mathbb{F}_2$ via the Chinese Remainder Theorem.
- The map β is the inverse of CRT.
- Let $C = \beta^{-1}(C_1, C_2)$ be a code over $\mathbb{F}_2[v]/\langle v^2 + v\rangle$, then C is denoted by $CRT(C_1, C_2)$, where C_1 and C_2 are binary codes and C is uniquely determined by C_1 and C_2.

Theorem

Let $k \leq n/2$ and $l \leq k$. The number of linear codes over $\mathbb{F}_2[v]/\langle v^2+v\rangle$ of length n and size 2^k where the size of the hull is 2^l is equal to

$$\sum_{k=k_1+k_2}\sum_{l=l_1+l_2}\mathfrak{N}_{n,k_1,l_1}\cdot\mathfrak{N}_{n,k_2,l_2}$$
$$=\sum_{k=k_1+k_2}\sum_{l=l_1+l_2}\left(\sum_{i=l_1}^{k_1}\begin{bmatrix} n-2i \\ k_1-i \end{bmatrix}\begin{bmatrix} i \\ l_1 \end{bmatrix}(-1)^{i-l_1}2^{\binom{i-l_1}{2}}\sigma_{n,i}\right)$$
$$\cdot\left(\sum_{j=l_2}^{k_2}\begin{bmatrix} n-2j \\ k_2-j \end{bmatrix}\begin{bmatrix} j \\ l_2 \end{bmatrix}(-1)^{j-l_2}2^{\binom{j-l_2}{2}}\sigma_{n,j}\right)$$

where $\sigma_{n,i}$ is the number of binary self-orthogonal codes of length n and size 2^i.

Counting Codes over $\mathbb{F}_2[v]/\langle v^2 + v\rangle$

Linear codes

Table 1: The number of codes over $\mathbb{F}_2[v]/\langle v^2 + v\rangle$ of length n and size 2^k, with a hull of size 2^l

n	k	l	Number	n	k	l	Number	n	k	l	Number
2	0	0	1	**8**	0	0	1	**10**	0	0	1
	1	0	4		1	0	256		1	0	1024
	1	1	2		1	1	254		1	1	1022
4	0	0	1		2	0	27264		2	0	436736
	1	0	16		2	1	40576		2	1	653824
	1	1	14		2	2	18775		2	2	304471
	2	0	104		3	0	1478656		3	0	94961664
	2	1	136		3	1	2499296		3	1	161622912
	2	2	55		3	2	1382976		3	2	90282240
6	0	0	1		3	3	338832		3	3	22346160
	1	0	64		4	0	40786432		4	0	$10^{10} \cdot 10520$
	1	1	62		4	1	65877504		4	1	$10^{10} \cdot 17134$
	2	0	1696		4	2	44123352		4	2	$10^{10} \cdot 11603$
	2	1	2464		4	3	13590432		4	3	$10^{9} \cdot 36314$
	2	2	1111		4	4	2104929		4	4	569194425
	3	0	22784						5	0	$10^{11} \cdot 51070$
	3	1	37432						5	1	$10^{11} \cdot 89580$
	3	2	199206						5	2	$10^{11} \cdot 63325$
	3	3	4680						5	3	$10^{11} \cdot 23516$
									5	4	$10^{10} \cdot 43198$
									5	5	$10^{9} \cdot 42609$

Appendix

E.F. Assmus, J.D. Key.
Affine and projective planes
Discrete Math., **83**, 161-187, 1990.

S.T. Dougherty.
Algebraic Coding Theory Over Finite Commutative Rings
SpringerBriefs in Mathematics. Springer, Cham, 2017, ISBN: 978-3-319-59805-5; 978-3-319-59806-2.

S.T. Dougherty.
Nets and their codes
Des., Codes and Cryptog., **3**, 315-331, 1993.

S.T. Dougherty.
A soding-theoretic solution to the 36 officer problem
Des., Codes and Cryptog., **4**, 123-128, 1994.

S.T. Dougherty, M. Harada and P. Solé.
Self-dual codes over rings and the chinese remainder theorem
Hokkaido Math. J., **28**, 253-283, 1999.

S.T. Dougherty and E. Salturk.
Counting codes over rings
Designs, Codes and Crypt.**73**, 151-165, 2014.

F.J. MacWilliams, N.J.A Sloane.
The Theory Of Error Correcting Codes.
North-Holland Pub. Co., 1977.

V. Pless.
The number of isotropic subspaces in a finite geometry
Rend. Sc. Fis. Mat. e Nat., Accad. Naz. Lincie, Ser. VIII, **39**, 418-421, 1965.

V. Pless.
On the uniqueness of the Golay codes
J. Combin. Theory., **5**, 215-228, 1968.

B. Segre.
Le geometrie di Galois
Annali di Mat. Pura Appl., Ser. 4a, **49**, 1-96, 1959.

N. Sendrier.
On the dimension of the hull
SIAM J. Discrete Math., **10**, No. 2, 282-293, 1997.

N.J.A. Sloane.
The on-line encyclopedia of integer sequences (OEIS)
Available online at https://oeis.org/.

J. Wood.
Duality for modules over finite rings and applications to coding theory
Amer. J. Math. **121**, 555-575, 1999.

S. Zhu, Y. Wang and M. Shi.
Some results on cyclic codes over $\mathbb{F}_2 + v\mathbb{F}_2$
IEEE Transactions on Information Theory, **56**, No. 4, 1680-1684, 2010.

Thank you

Thank you for your attention!