Additive Codes

Steven T. Dougherty

Lens 2021

(Semi)-Classical Situation

- R a finite Frobenius ring, ambient space R^n.

(Semi)-Classical Situation

- R a finite Frobenius ring, ambient space R^n.
- Linear code of length n – submodule of R^n

(Semi)-Classical Situation

- R a finite Frobenius ring, ambient space R^n.
- Linear code of length n – submodule of R^n
- $[\mathbf{v}, \mathbf{w}] = \sum \mathbf{v}_i \mathbf{w}_i$

(Semi)-Classical Situation

- R a finite Frobenius ring, ambient space R^n.
- Linear code of length n – submodule of R^n
- $[\mathbf{v}, \mathbf{w}] = \sum \mathbf{v}_i \mathbf{w}_i$
- $C^\perp = \{\mathbf{v} \mid [\mathbf{v}, \mathbf{w}] = 0, \ \forall \mathbf{w} \in C\}$

Non-commutative rings

- $\mathcal{L}(C) = \{\mathbf{v} \in R^n \mid [\mathbf{v}, \mathbf{c}] = 0, \forall \mathbf{c} \in C\}$

Non-commutative rings

- $\mathcal{L}(C) = \{\mathbf{v} \in R^n \mid [\mathbf{v}, \mathbf{c}] = 0, \forall \mathbf{c} \in C\}$
- $\mathcal{R}(C) = \{\mathbf{v} \in R^n \mid [\mathbf{c}, \mathbf{v}] = 0, \forall \mathbf{c} \in C\}$

Non-commutative rings

- $\mathcal{L}(C) = \{\mathbf{v} \in R^n \mid [\mathbf{v}, \mathbf{c}] = 0, \forall \mathbf{c} \in C\}$
- $\mathcal{R}(C) = \{\mathbf{v} \in R^n \mid [\mathbf{c}, \mathbf{v}] = 0, \forall \mathbf{c} \in C\}$
- Let C be a code, then $\mathcal{L}(C)$ is a left linear code and $\mathcal{R}(C)$ is a right linear code.

Non-commutative rings

- $\mathcal{L}(C) = \{\mathbf{v} \in R^n \mid [\mathbf{v}, \mathbf{c}] = 0, \forall \mathbf{c} \in C\}$
- $\mathcal{R}(C) = \{\mathbf{v} \in R^n \mid [\mathbf{c}, \mathbf{v}] = 0, \forall \mathbf{c} \in C\}$
- Let C be a code, then $\mathcal{L}(C)$ is a left linear code and $\mathcal{R}(C)$ is a right linear code.
- In the commutative case $C^\perp = \mathcal{L}(C) = \mathcal{R}(C)$ and is a linear code.

Orthogonal Cardinalities

Lemma (Wood) If C is a left linear code over a finite Frobenius ring, then $|\mathcal{R}(C)||C| = |R|^n$. If C is a right linear code then $|\mathcal{L}(C)||C| = |R|^n$.

Orthogonal Cardinalities

Lemma (Wood) If C is a left linear code over a finite Frobenius ring, then $|\mathcal{R}(C)||C| = |R|^n$. If C is a right linear code then $|\mathcal{L}(C)||C| = |R|^n$.

Commutative Case $|C||C^\perp| = |R|^n$ which generalizes classical case $dim(C) + dim(C^\perp) = n$.

Key points

- R is Frobenius ($\widehat{R}$ has a generating character).

Key points

- R is Frobenius ($\widehat{R}$ has a generating character).
- C linear (left, right), closed under addition **and** scalar multiplication.

Weight Enumerators

- For a code over an alphabet $A = \{a_0, a_1, \ldots, a_{s-1}\}$, the complete weight enumerator is the following polynomial in commuting indeterminants:

$$cwe_C(x_{a_0}, x_{a_1}, \ldots, x_{a_{s-1}}) = \sum_{\mathbf{c} \in C} \prod_{i=0}^{s-1} x_{a_i}^{n_i(\mathbf{c})} \tag{1}$$

where there are $n_i(\mathbf{c})$ occurrences of a_i in the vector $\mathbf{c}$.

Weight Enumerators

- For a code over an alphabet $A = \{a_0, a_1, \ldots, a_{s-1}\}$, the complete weight enumerator is the following polynomial in commuting indeterminants:

$$cwe_C(x_{a_0}, x_{a_1}, \ldots, x_{a_{s-1}}) = \sum_{\mathbf{c} \in C} \prod_{i=0}^{s-1} x_{a_i}^{n_i(\mathbf{c})} \tag{1}$$

where there are $n_i(\mathbf{c})$ occurrences of a_i in the vector $\mathbf{c}$.

- The Hamming weight enumerator of a code C of length n is defined to be

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

where $wt(\mathbf{c}) = |\{i \mid c_i \neq 0\}|$. It is immediate that $W_C(x, y) = cwe(x, y, y, \ldots, y)$.

We define the matrix T, where T is an $|R|$ by $|R|$ matrix given by:

$$(T)_{a,b} = (\chi(ab)) \tag{2}$$

where a and b are in R.

MacWilliams Relations

Theorem

(Wood) Let R be a Frobenius ring, with $|R| = k+1$. Let x_i correspond to the i-th element of R.
If C is a left submodule of R^n, then

$$cwe_C(x_0, x_1, \ldots, x_k) = \frac{1}{|\mathcal{R}(C)|} cwe_{\mathcal{R}(C)}(T^t \cdot (x_0, x_1, \ldots, x_k)).$$

If C is a right submodule of R^n, then

$$cwe_C(x_0, x_1, \ldots, x_k) = \frac{1}{|\mathcal{L}(C)|} cwe_{\mathcal{L}(C)}(T \cdot (x_0, x_1, \ldots, x_k)).$$

MacWilliams Relations

Theorem

(Wood) Let R be a Frobenius ring, with $|R| = k+1$. Let x_i be the indeterminate that corresponds to the i-th element of R.
If C is a left submodule of R^n, then

$$W_C(x,y) = \frac{1}{|\mathcal{R}(C)|} W_{\mathcal{R}(C)}(x + (|R|-1)y, x-y).$$

If C is a right submodule of R^n, then

$$W_C(x,y) = \frac{1}{|\mathcal{L}(C)|} W_{\mathcal{L}(C)}(x + (|R|-1)y, x-y).$$

Generating character

- χ **highly** non-unique.

Generating character

- χ **highly** non-unique.
- χ is a generating character if and only if *ker*(χ) contains no non-trivial ideal.

Generating character

- χ **highly** non-unique.
- χ is a generating character if and only if *ker*(χ) contains no non-trivial ideal.
- It is known how to construct χ, namely start with Socle and expand.

Additive Codes (So Far)

- Generally consider $\mathbb{F}_p$ linearity in $\mathbb{F}_{p^e}^n$.

Additive Codes (So Far)

- Generally consider $\mathbb{F}_p$ linearity in $\mathbb{F}_{p^e}^n$.
- Inner-product $[\mathbf{v}, \mathbf{w}] = \sum v_i w_i^2$ Important for quantum error correction.

Additive Codes (as I see it)

- G a finite abelian group (often the additive group of a ring – commutative or non-commutative)

Additive Codes (as I see it)

- G a finite abelian group (often the additive group of a ring – commutative or non-commutative)
- $\chi : G \to \mathbb{C}$, χ a homomorphism, that is a character of G

Additive Codes (as I see it)

- G a finite abelian group (often the additive group of a ring – commutative or non-commutative)
- $\chi : G \to \mathbb{C}$, χ a homomorphism, that is a character of G
- $\widehat{G} = \{\chi \mid \chi \text{ a character of } G\}$

Additive Codes (as I see it)

- G a finite abelian group (often the additive group of a ring – commutative or non-commutative)
- $\chi : G \to \mathbb{C}$, χ a homomorphism, that is a character of G
- $\widehat{G} = \{\chi \mid \chi \text{ a character of } G\}$
- G and $\widehat{G}$ are isomorphic but not canonically

Additive Codes (as I see it)

- Choose an isomorphism $\psi : G \to \widehat{G}$.

Additive Codes (as I see it)

- Choose an isomorphism $\psi : G \to \widehat{G}$.
- Fix a symmetric duality on the space G^n. Namely, let $\chi_a = \psi(a)$ with $\chi_a(b) = \chi_b(a)$.

Additive Codes (as I see it)

- Choose an isomorphism $\psi : G \to \widehat{G}$.
- Fix a symmetric duality on the space G^n. Namely, let $\chi_a = \psi(a)$ with $\chi_a(b) = \chi_b(a)$.
- The orthogonal depends on the given duality.

Additive Codes (as I see it)

- Choose an isomorphism $\psi : G \to \widehat{G}$.
- Fix a symmetric duality on the space G^n. Namely, let $\chi_a = \psi(a)$ with $\chi_a(b) = \chi_b(a)$.
- The orthogonal depends on the given duality.
- $C^\perp = \{(g_1, g_2, \ldots, g_n) | \prod_{i=1}^{i=n} \chi_{g_i}(c_i) = 1$ for all $(c_1, \ldots, c_n) \in C\}$.

Additive Codes (As I see it)

- $(C^{\perp})^{\perp} = C$

Additive Codes (As I see it)

- $(C^{\perp})^{\perp} = C$
- $C^{\perp}$ is additive

Additive Codes (As I see it)

- $(C^{\perp})^{\perp} = C$
- $C^{\perp}$ is additive
- $|C||C^{\perp}| = |G|^n$.

MacWilliams Relations

$$M_{\alpha_i,\alpha_j} = \chi_{\alpha_i}(\alpha_j).$$

Theorem

Let $M_{\alpha_i,\alpha_j} = \chi_{\alpha_i}(\alpha_j)$*. Let* C *be an additive code over* G*,* $|G| = s$*, with weight enumerator* $W_C(x_0, x_1, \ldots, x_{s-1})$ *then the complete weight enumerator of the orthogonal is given by:*

$$W_{C^\perp}(x_0, x_1, \ldots, x_{s-1}) = \frac{1}{|C|} W_C(M \cdot (x_0, x_1, \ldots, x_{s-1}))$$

and

MacWilliams Relations

$$M_{\alpha_i,\alpha_j} = \chi_{\alpha_i}(\alpha_j).$$

Theorem

Let $M_{\alpha_i,\alpha_j} = \chi_{\alpha_i}(\alpha_j)$*. Let* C *be an additive code over* G*,* $|G| = s$*, with weight enumerator* $W_C(x_0, x_1, \ldots, x_{s-1})$ *then the complete weight enumerator of the orthogonal is given by:*

$$W_{C^\perp}(x_0, x_1, \ldots, x_{s-1}) = \frac{1}{|C|} W_C(M \cdot (x_0, x_1, \ldots, x_{s-1}))$$

and

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

Intuition

- When the ring is Frobenius, scalar multiplication "matches" the duality when it is based on a generating character.

Intuition

- When the ring is Frobenius, scalar multiplication "matches" the duality when it is based on a generating character.
- Can be used when the ring is not Frobenius!

Intuition

- When the ring is Frobenius, scalar multiplication "matches" the duality when it is based on a generating character.
- Can be used when the ring is not Frobenius!
- Can be used when the codes are not linear.

Examples

$$M_E = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & -1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \end{pmatrix} \tag{3}$$

Examples

$$M_E = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & -1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \end{pmatrix} \tag{3}$$

$$M_T = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \\ 1 & -1 & 1 & -1 \end{pmatrix}, M_{TH} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}. \tag{4}$$

Guide to Use

- Pick the duality that matches your particular application.

Guide to Use

- Pick the duality that matches your particular application.
- In need not be just $\mathbb{F}_p$ linearity. Any additive subgroup will work.

Linearity Example

- The finite field $\mathbb{F}_q$, $q = p^e$, is a vector space over $\mathbb{F}_p$ of dimension e, each element of $\mathbb{F}_q$ can be written as $a_0 + a_1\zeta + a_2\zeta^2 + \cdots + a_{e-1}\zeta^{e-1}$ for some ζ.

Linearity Example

- The finite field $\mathbb{F}_q$, $q = p^e$, is a vector space over $\mathbb{F}_p$ of dimension e, each element of $\mathbb{F}_q$ can be written as $a_0 + a_1\zeta + a_2\zeta^2 + \cdots + a_{e-1}\zeta^{e-1}$ for some ζ.
- $K_i = \{a_0 + a_1\zeta + a_2\zeta^2 + \cdots + a_{e-1}\zeta^{e-1} \mid a_j = 0 \text{ if } j > i - 1\}$.

Linearity Example

- The finite field $\mathbb{F}_q$, $q = p^e$, is a vector space over $\mathbb{F}_p$ of dimension e, each element of $\mathbb{F}_q$ can be written as $a_0 + a_1\zeta + a_2\zeta^2 + \cdots + a_{e-1}\zeta^{e-1}$ for some ζ.
- $K_i = \{a_0 + a_1\zeta + a_2\zeta^2 + \cdots + a_{e-1}\zeta^{e-1} \mid a_j = 0 \text{ if } j > i-1\}$.
- Then K_i is an additive subgroup of $(\mathbb{F}_q, +)$. **Not necessarily a subfield.**

Linearity Example

- $\langle N \rangle_{p^i}$ is the span of N with coefficients from K_i. Let N be any matrix with rows that are elements from $\mathbb{F}_q^n$, $q = p^e$, p prime. Then the $\langle N \rangle_{p^i}$ is a subgroup of $\mathbb{F}_q^n$.

Linearity Example

- $\langle N \rangle_{p^i}$ is the span of N with coefficients from K_i. Let N be any matrix with rows that are elements from $\mathbb{F}_q^n$, $q = p^e$, p prime. Then the $\langle N \rangle_{p^i}$ is a subgroup of $\mathbb{F}_q^n$.
- $$\langle N \rangle_p \subseteq \langle N \rangle_{p^2} \subseteq \cdots \subseteq \langle N \rangle_{p^e}.$$

Linearity Example

- $\langle N \rangle_{p^i}$ is the span of N with coefficients from K_i. Let N be any matrix with rows that are elements from $\mathbb{F}_q^n$, $q = p^e$, p prime. Then the $\langle N \rangle_{p^i}$ is a subgroup of $\mathbb{F}_q^n$.
- $$\langle N \rangle_p \subseteq \langle N \rangle_{p^2} \subseteq \cdots \subseteq \langle N \rangle_{p^e}.$$
  $$\langle N \rangle_{p^e}^\perp \subseteq \langle N \rangle_{p^{e-1}} \subseteq \cdots \subseteq \langle N \rangle_p^\perp$$

Questions

Questions

Merci André!!