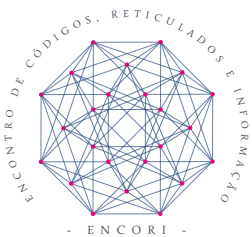
Idempotentes Essenciais Projetivos e Teoria de Códigos

André Duarte

IME-USP e *FATEC Adib Moisés Dib*

Encontro de Códigos, Reticulados e Informação (EnCoRI)
IMECC (Unicamp)
16 de Junho de 2023



Conceitos Básicos

Conceitos Básicos

- $\mathbb{F} = \mathbb{F}_q$ um corpo finito com q elementos.

Conceitos Básicos

- $\mathbb{F} = \mathbb{F}_q$ um corpo finito com q elementos.
- Um $[n, k]$-**código linear** $\mathcal{C}$ sobre $\mathbb{F}$ é um subespaço de $\mathbb{F}^n$ de dimensão k.

Conceitos Básicos

- $\mathbb{F} = \mathbb{F}_q$ um corpo finito com q elementos.
- Um $[n, k]$-**código linear** $\mathcal{C}$ sobre $\mathbb{F}$ é um subespaço de $\mathbb{F}^n$ de dimensão k.
- Seja $\mathcal{B} = \{v_1, \ldots, v_k\}$ uma base ordenada para $\mathcal{C}$ com $v_i = (v_{i1}, \ldots, v_{in})$, para todo $i = 1, \ldots, k$. A matriz

$$\mathcal{G} = \begin{bmatrix} v_{11} & \cdots & v_{1n} \\ \vdots & & \vdots \\ v_{k1} & \cdots & v_{kn} \end{bmatrix}$$

é dita uma **matriz generadora** de $\mathcal{C}$.

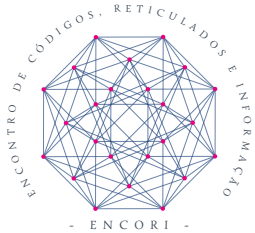
Conceitos Básicos

- $\mathbb{F} = \mathbb{F}_q$ um corpo finito com q elementos.
- Um $[n, k]$-**código linear** $\mathcal{C}$ sobre $\mathbb{F}$ é um subespaço de $\mathbb{F}^n$ de dimensão k.
- Seja $\mathcal{B} = \{v_1, \ldots, v_k\}$ uma base ordenada para $\mathcal{C}$ com $v_i = (v_{i1}, \ldots, v_{in})$, para todo $i = 1, \ldots, k$. A matriz

$$\mathcal{G} = \begin{bmatrix} v_{11} & \cdots & v_{1n} \\ \vdots & & \vdots \\ v_{k1} & \cdots & v_{kn} \end{bmatrix}$$

  é dita uma **matriz generadora** de $\mathcal{C}$.
- Um $[n, k]$-código linear $\mathcal{C}$ em $\mathbb{F}^n$, com matriz geradora $\mathcal{G}$, é um q-ário **código simplex** se as colunas de $\mathcal{G}$ são não-nulas e nenhuma coluna é um múltiplo escalar de outra.

Códigos Simplex



Códigos Simplex

- são códigos constacíclicos;

Códigos Simplex

- são códigos constacíclicos;
- são códigos de peso constante;

Códigos Simplex

- são códigos constacíclicos;
- são códigos de peso constante;
- atingem a cota de Griesmer, logo são ótimos;

Códigos Simplex

- são códigos constacíclicos;
- são códigos de peso constante;
- atingem a cota de Griesmer, logo são ótimos;
- são universalmente ótimos.

Álgebra de Grupo Twisted

Seja G um grupo finito. Uma **álgebra de grupo twisted** $\mathbb{F}^tG$ de G sobre $\mathbb{F}$ é um anel associativo que contém $\mathbb{F}$ e tem uma cópia $\overline{G}$ de G como uma $\mathbb{F}$-base. A multiplicação em $\mathbb{F}^tG$ é definida por:

$$\bar{x}.\bar{y} = t(x,y)\overline{xy} \qquad \text{para todo } x, y \in G,$$
$$\bar{x}\lambda = \lambda\bar{x} \qquad \text{para todo } x \in G \text{ e } \lambda \in \mathbb{F},$$

onde $t : G \times G \to \mathbb{F}^*$ é uma função chamada **twisting** (**normalizado**) de G sobre $\mathbb{F}$.

Códigos de Grupo Twisted

Um código $\mathcal{C} \subset \mathbb{F}^n$ é um **código de grupo twisted** se existe um enumeração $G = \{g_1, g_2, \ldots, g_n\}$ dos elementos de G tal que a imagem de $\mathcal{C}$ pela função $\varphi : \mathbb{F}^n \to \mathbb{F}^t G$ dada por

$$\varphi(\lambda_1, \ldots, \lambda_n) = \sum_{i=1}^{n} \lambda_i \bar{g}_i, \tag{1}$$

é um ideal bilateral de $\mathbb{F}G$.

Motivação

Quais códigos de grupo twisted são códigos simplex?

Motivação

Quais códigos de grupo twisted são códigos simplex?

- $q = 2$, G cíclico $\Rightarrow$ códigos simplex são gerados por idempotentes essenciais (projetivos) em $\mathbb{F}^t G = \mathbb{F}G$.

Motivação

Quais códigos de grupo twisted são códigos simplex?

- $q = 2$, G cíclico $\Rightarrow$ códigos simplex são gerados por idempotentes essenciais (projetivos) em $\mathbb{F}^t G = \mathbb{F}G$.
- $q \neq 2$?

Pares Admissíveis

Pares Admissíveis

Seja A um grupo Abeliano finito de ordem n tal que $mdc(n, q) = 1$, e seja t um twisting de A sobre $\mathbb{F}$. Façamos

$$A_0 = \{a \in A \mid t(a, b) = t(b, a) \text{ for all } b \in A\}.$$

Pares Admissíveis

Seja A um grupo Abeliano finito de ordem n tal que $mdc(n, q) = 1$, e seja t um twisting de A sobre $\mathbb{F}$. Façamos

$$A_0 = \{a \in A \mid t(a, b) = t(b, a) \text{ for all } b \in A\}.$$

Definição

Seja H um subgrupo de A_0 e seja $\beta : H \to \mathbb{F}^*$ uma função com $\beta(h) = \beta_h$, para todo $h \in H$. Dizemos que (H, β) é um **par admissível**, *se o twisting $\mathfrak{T} = t\big|_{H \times H}$ de H sobre $\mathbb{F}$ é da forma $\mathfrak{T}(h, k) = \beta_h \beta_k \beta_{hk}^{-1}$, para todo $h, k \in H$.*

Idempotentes vindos de Subgrupos

Idempotentes vindos de Subgrupos

Se (H, β) é um par admissível, então construímos

$$\widehat{H}_\beta = \frac{1}{|H|} \sum_{h \in H} \beta_h^{-1} \bar{h}.$$

Se (H, β) é um par admissível, então construímos

$$\widehat{H}_\beta = \frac{1}{|H|} \sum_{h \in H} \beta_h^{-1} \bar{h}.$$

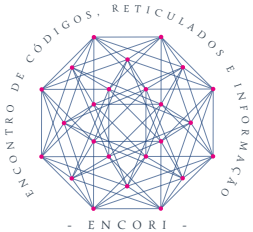
Observação

$\widehat{H}_\beta$ é um idempotente central em $\mathbb{F}\,{}^t A$.

Idempotentes Essenciais Projetivos

Definição

Seja $e \in \mathbb{F}^t A$ um idempotente central primitivo. Dizemos que e é um **idempotente essencial projetivo** *se $e\widehat{H}_\beta = 0$, para todo par admissível (H, β) com $H \neq \{1\}$.*



Códigos Simplex como Códigos de Grupo Twisted

Códigos Simplex como Códigos de Grupo Twisted

Seja $C = \langle g \rangle$ um grupo cíclico de ordem n.

Seja $C = \langle g \rangle$ um grupo cíclico de ordem n. Para $\lambda \in \mathbb{F}^*$, seja t_λ um twisting definido por:

$$t_\lambda(g^i, g^j) = \begin{cases} 1, & i + j < n \\ \lambda, & i + j \geq n. \end{cases}$$

Seja $C = \langle g \rangle$ um grupo cíclico de ordem n. Para $\lambda \in \mathbb{F}^*$, seja t_λ um twisting definido por:

$$t_\lambda(g^i, g^j) = \begin{cases} 1, & i + j < n \\ \lambda, & i + j \geq n. \end{cases}$$

Lembrando que $\varphi : \mathbb{F}^n \to \mathbb{F}^{t_\lambda} C$ definida por

$$\varphi(a_0, a_1, \ldots, a_{n-1}) = a_0\bar{1} + a_1\bar{g} + \cdots + a_{n-1}\bar{g}^{n-1}.$$

Seja $e \in \mathbb{F}^{t_\lambda} C$ um idempotente e seja $\mathcal{I} = \mathbb{F}^{t_\lambda} C\, e$ um ideal gerado por e com dimensão k.

Seja $e \in \mathbb{F}^{t_\lambda} C$ um idempotente e seja $\mathcal{I} = \mathbb{F}^{t_\lambda} C\, e$ um ideal gerado por e com dimensão k.

Teorema

Suponha que $\mathcal{C} = \varphi^{-1}(\mathcal{I})$. Então $\mathcal{C}$ é um código simplex se e somente se $\mathcal{I}$ é gerado por um idempotente essencial projetivo.

Seja $e \in \mathbb{F}^{t_\lambda} C$ um idempotente e seja $\mathcal{I} = \mathbb{F}^{t_\lambda} C\, e$ um ideal gerado por e com dimensão k.

Teorema

Suponha que $\mathcal{C} = \varphi^{-1}(\mathcal{I})$. Então $\mathcal{C}$ é um código simplex se e somente se $\mathcal{I}$ é gerado por um idempotente essencial projetivo.

Corolário

Para qualquer grupo cíclico C de ordem $(q^k - 1)/(q - 1)$, existe $\lambda \in \mathbb{F}^*$ tal que $\mathbb{F}^{t_\lambda} C$ contém um idempotente essencial projetivo.

Teorema de Existência

Seja $n = \prod_{i=1}^{r} p_i^{n_i}$ a decomposição do inteiro positivo n em fatores primos.

Teorema de Existência

Seja $n = \prod_{i=1}^{r} p_i^{n_i}$ a decomposição do inteiro positivo n em fatores primos.

Teorema

Sejam C um grupo cíclico de ordem n e $\lambda \in \mathbb{F}^*$ de ordem multiplicativa ν. Uma álgebra grupo twisted $\mathbb{F}^{t_\lambda} C$ contém um idempotente essencial projetivo se e somente se p_i não divide $(q-1)/\nu$, para todo $i = 1, \ldots, r$.

Exemplo 1

Considere o caso $\mathbb{F} = \mathbb{F}_5$, $C = C_3 = \langle x \rangle$ e $t(x^i, x^j) = 1$. Como $p = 3$ não divide $(q-1) = 4$, temos que $\mathbb{F}\,{}^t A = \mathbb{F}A$ contém um (único) idempotente essencial projetivo.

Exemplo 2

Para $\mathbb{F} = \mathbb{F}_9$, $C = C_4$ e $\lambda = -1$, temos que $q - 1/e = 8/2 = 4$ e $n = 2^2$. Como $2|4$, segue que $\mathbb{F}^{t-1}C$ não contém idempotente essencial projetivo.

Example 3

Seja $\mathbb{F}$ o corpo $\mathbb{F}_7$, $C = C_8 = \langle g \rangle$ e seja t_3 o twisting de C sobre $\mathbb{F}$ definido por

$$t_3(g^i, g^j) = \begin{cases} 1, & i + j < n \\ 3, & i + j \geq n. \end{cases}$$

Como $X^8 - 3$, $X^4 - 3$ e $X^2 - 3$ não possuem raízes em $\mathbb{F}$, segue que não existe par admissível (H, β) com $H \neq \{1\}$, e assim todo idempotente central primitivo de $\mathbb{F}^{t_3} C$ é um idempotente essencial projetivo.

Agradecimentos

Ao Prof. César Polcino Milies (orientador do doutorado), Prof. André Leroy (Université D'Artois) e Prof. Raul Antonio Ferraz (supervisor pós-doc) pelo apoio e sugestões que muito contribuíram para melhorar a profundidade e a clareza da investigação.

Referências

- A. Duarte, Projective Essential Idempotents, TechRxiv, Preprint, (2023) https://doi.org/10.36227/techrxiv.23184410.v1.
- A. Duarte, A. Pereira and C. Polcino, Nilpotent Group Codes, *Journal of Algebra and Its Applications*, https://doi.org/10.1142/S0219498824500609 (2022).
- A. G. Chalom , R. A. Ferraz e C. Polcino Milies. Essential Idempotents and Simplex Codes, Algebra Comb. Discrete Appl. 4.2 (2017), 181-188.