Pesos e empacotamentos generalizados de códigos lineares

Makson Miller A. Ribeiro

m226079@dac.unicamp.br

Encontro de Códigos, Reticulados e Informação

16 de Junho de 2023

Histórico

1. Em Teoria de códigos há alguns parâmetros de interesse como o comprimento n, a dimensão k e a distância mínima d, .
2. Victor K. Wei em 1991 introduziu, para um código linear $\mathcal{C}$, o que chamamos de $r-$ésima distância mínima de Hamming $d_r(\mathcal{C})$.
3. Tsfasman e Vladut fizeram uma releitura dos pesos generalizados com uma abordagem geométrica.
4. Os pesos mínimos para cada $r \leq k$ são capazes de determinar o código ?

Definições

Consideremos $\mathcal{C}$ um $[n, k, d]$-código sobre $\mathbb{F}_q^n$ com q primo. A distância de Hamming computa a diferença em cada entrada das palavras códigos de $\mathcal{C}$, então define-se a distância mínima como sendo

$$d_H(\mathcal{C}) = \min_{c_1, c_2 \in \mathcal{C}} d_H(c_1, c_2) = \min_{0 \neq c \in \mathcal{C}} \omega(c).$$

Pesos Generalizados e suas propriedades

Considerando c $\in \mathbb{F}_q^n$, define-se o suporte da palavra código c, como sendo

$$Supp(\mathbf{x}) = \{j | x_j \neq 0\}.$$

Teorema

Dado um $[n, k, d]_q$ código $\mathcal{C}$ com matriz geradora $G = [c_1 \dots c_k]$, então $Supp(\mathcal{C}) = \bigcup_{i=1}^{k} Supp(c_i)$.

Obs: $\omega(c) = |Supp(c)|$.

r-ésima distância generalizada

- Para todo natural (fixo) $r \leq k$, consideraremos todos os subcódigos de $\mathcal{C}$ de dimensão r.

r-ésima distância de Hamming

$d_r(\mathcal{C}) = \min\{|Supp(D)| : D \subset \mathcal{C} \text{ e } \dim D = r\}$.

Exemplo

Consideremos dois códigos $\mathcal{C}_1$ e $\mathcal{C}_2$ em $\mathbb{F}_2^4$.
$\mathcal{C}_1 =< (1,0,0,0),(0,1,0,0) >$ e $\mathcal{C}_2 =< (1,0,0,0),(1,1,1,1) >$.

- $d_1(\mathcal{C}_1) = d_1(\mathcal{C}_2)$;
- $\mathcal{C}_1$ e $\mathcal{C}_2$ corrigem até um erro se este ocorrer nas posições 3 ou 4;
- $\mathcal{C}_1$ não é capaz de corrigir se o erro estiver nas posições 1 ou 2;
- $\mathcal{C}_2$ Corrige se o erro for na posição 2;
- $2 = d_2(\mathcal{C}_1) < d_2(\mathcal{C}_2) = 4$.

Hierarquia de pesos do código $\mathcal{C}$

1. Para a sequência $(d_r(\mathcal{C}))_{r=1}^{k}$ nomea-se como a hierarquia de pesos.

Desigualdade estrita

$d(\mathcal{C}) = d_1(C) < \ldots < d_k(\mathcal{C}) = |Supp(\mathcal{C})|.$

[Wei]

Seja C um $[n, k, d_1, \ldots, d_q]_q$ Código linear. Então

$$r \leq d_r \leq n - k + r.$$

Se para algum $r < k$ acontecer de $d_r(\mathcal{C}) = n - k + r$. Então vale

$$d_r + 1 \leq d_{r+1} \leq n - k + (r + 1)$$

$$n - k + r + 1 \leq d_{r+1} \leq n - k + (r + 1) \longleftrightarrow d_{r+1} = n - k + (r + 1).$$

- Induz um código s-MDS para $s \in \{r, \ldots, k\}$
- Wei mostra que um código dual de um $1-$MDS é também um $1-$MDS

Espectro

Definição

Dado um código $\mathcal{C}$ em $\mathbb{F}_q^n$, o espectro de $\mathcal{C}$ é dado pela matriz $Spec(\mathcal{C}) = \left[A_i^j\right]_{k\times n}$, em que

$$A_i^j = |\{D \subset \mathcal{C} : \dim(D) = \text{i } |\text{Supp(D)}|\text{=j}\}|.$$

Calculando Espectros - Primeira linha da matriz

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

$$\mathcal{C} = \{11010, 00111, 00010, 00000, 11101, 00101, 11000, 11111\}$$

1. Temos 1 palavra de peso 1;
2. Temos 2 palavras de peso 2;
3. Temos 2 palavras de peso 3;
4. Temos 1 palavra de peso 4;
5. Temos 1 palavra de peso 5;

Subcódigos de dimensão 2 e segunda linha da matriz

O número q- binomial fornece quantos subespaços de dimensão r têm sobre o espaço $\mathbb{F}_q^n$.

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

$$\begin{bmatrix} 3 \\ 2 \end{bmatrix}_2 = \frac{(2^3-1)(2^3-2)}{(2^2-1)(2^2-2)} = 7$$

- Subcódigos com suporte 3 $\{< 11010, 00010 >, < 00111, 00010 > \}$;
- Subcódigo com suporte 4 $< 11101, 00101 >$;
- Subcódigos com suporte 5 $\{< 00010, 11101 >, < 11010, 00101 >, < 11010, 00111 >, < 00111, 11000 >\}$.

Terceira Linha da matriz

- Como o código é gerado pelas três colunas de G, o suporte do código será dado pelo suporte do espaço gerado das colunas, ou seja, $|Supp(\mathcal{C})| = 5$.

Terceira Linha da matriz

- Como o código é gerado pelas três colunas de G, o suporte do código será dado pelo suporte do espaço gerado das colunas, ou seja, $|Supp(\mathcal{C})| = 5$.

$$Spec(\mathcal{C}) = \begin{bmatrix} 1 & 2 & 2 & 1 & 1 \\ 0 & 0 & 2 & 1 & 4 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

Código equivalente a $\mathcal{C}$

Definição

Dois códigos lineares $\mathcal{C}$ e $\mathcal{C}'$ em $\mathbb{F}_q^n$ são equivalentes se existe uma permutação $\sigma \in \mathcal{S}_n$ tal que $\sigma(\mathcal{C}) = \mathcal{C}'$.

Considere $G' = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}$, então

$C' = \{00000, 11111, 10010, 10111, 11010, 01101, 01000, 00101\}$

Neste caso, obtemos que $Spec(C') = Spec(C)$.

Códigos equivalentes e espectros

Teorema

Dado dois códigos binários equivalentes, eles possuem o mesmo espectro.

Esquema da prova

Sendo C_1 e C_2 dois códigos equivalentes, existe portanto $\sigma \in \mathcal{S}_n$, tal que $\sigma(C_1) = C_2$. Para qualaquer subcódigo $D \leq C_1 \rightarrow \sigma(D) \leq C_2$, também temos $D' \leq C_2 \rightarrow \sigma^{-1}(D') \leq C_1$. Ainda preserva-se os suportes de cada um dos subcódigos, ou seja, $|Supp(D)| = |Supp(\sigma(D))|$ e $|Supp(D')| = |Supp(\sigma(D'))|$ fornecendo portanto uma bijeção entre os subespaços induzida por σ, logo $Spec(C_1) = Spec(C_2)$.

Conjectura com a recíproca

Dois códigos binários são equivalentes se, e somente se, têm o mesmo espectro.

1. No trabalho[4] tem uma checagem computacional (por exaustão) em que para todos os $[n, k]_2$-códigos com mesmo espectros e com $n \leq 11$ a recíproca é verificada.
2. (Resultado Parcial) Para dois códigos binários k-dimensionais com mesmo espectro, estes são equivalentes para $k = 1$, $k = 2$, $k = n - 1$ e $k = n - 2$.

Alternativa para a prova

Um sistema projetivo $\mathcal{P}$ é uma família de pontos (não ordenados) no espaço projetivo $\mathbb{P} = \mathbb{P}(V)$ sobre $\mathbb{F}_q$ que não pertencem a qualquer hiperplano Π.

- $n = |\mathcal{P}|$;
- $k = dim\mathbb{P} + 1$;
- $d = n - \max_{\Pi} |\mathcal{P} \cap \Pi| \geq 1$

Dois sistemas projetivos $\mathcal{P} \subset \mathbb{P}$ e $\mathcal{P}' \subset \mathbb{P}'$ são equivalentes se existe um isomorfismo (projetivo) que leva $\mathcal{P}$ em $\mathcal{P}'$.

Alternativa para a prova

Teorema

Sejam $k \geq 1$ e $d \geq 1$. Há uma bijeção entre o conjunto das classes de equivalência de $[n, k, d]_q$-códigos lineares e o conjunto $[n, k, d]_q$-sistemas projetivos.

- $d_r = d_r(\mathcal{P})$, $n - d_r = \max\{|\mathcal{P} \cap H| : codim(H) = r\}$;
- $A_i^r = |\{\Pi \subset \mathbb{P} : codim(\Pi) = r, |\Pi \cap \mathcal{P}| = n - i\}|$.

Há uma bijeção entre o conjunto das classes de equivalência de sistemas projetivos não degenerados e o conjunto das classes de equivalências de códigos lineares não degenerados. **A correspondência preserva os parâmetros** $n, k, d_1, \ldots, d_k, A_i^r$.

Perspectivas Futuras

- Códigos equivalentes em baixa dimensão estão associados a sistemas projetivos equivalentes, espectros iguais de sistemas projetivos levam a sistemas equivalentes;
- Usar aprendizado de máquina através dos resultados de [4];
- Analizar a capacidade de correção com pesos generalizados não usuais, com $r = \lfloor \frac{d_r(\mathcal{C}) - 1}{2} \rfloor$;
- Surgiu a ideia de observar como se comporta o "empacotamento" de reticulados construídos via Construção A, utilizando raios intermediários ($r_{pack} < r < r_{cover}$) e o desempenho de decodificação.

Referências I

[1] Victor K. Wei. *Generalized Hamming weights for linear codes*. IEEE Transac- tions on information theory 37.5 (1991), pp. 1412–1418.

[2] Michael A Tsfasman e Serge G Vladut *eometric approach to higher weights*. IEEE Transactions on Information Theory 41.6 (1995), pp. 1564–1588.

[3] Tor Helleseth, Torleiv Klove e Øyvind Ytrehus. *Generalized Hamming weights of li- near codes*. IEEE transactions on information theory 38.3 (1992), pp. 1133–1140.

[4] Darwin Gregorio Villar Salinas. *On linear block codes: classification and estimation of bounds for weight hierarchy of codes*. Tese de Doutorado- Imecc- Unicamp (2022).

OBRIGADO!