Pesos Generalizados de códigos lineares

Makson Miller A. Ribeiro & Marcelo Firer

Universidade Estadual de Campinas

m226079@dac.unicamp.br

Resumo

Os pesos generalizados de um código $\mathcal{C}$ os quais foram introduzidos por Wei [4], buscam essencialmente encontrar pesos mínimos de subcódigos $\mathcal{D} \subset \mathcal{C}$. Sabe-se que para um código linear, que são os códigos do escopo deste trabalho, tais pesos coincidem com a $r-$distância mínima de $\mathcal{C}$, $d_r(\mathcal{C})$. O papel e desempenho destes pesos generalizados ($r > 1$) ainda não têm sido explorados no contexto de eficiência. Foram Tsfasman e Vladut [3] que trouxeram uma abordagem mais geométrica para estes pesos e ainda exploraram o caso q-ário no espaço projetivo finito sobre $\mathbb{F}_q^n$, também fizeram releituras dos principais parâmetros relacionados a códigos neste espaço. Já em [1] alguns limitantes são encontrados para os pesos generalizados, estes limitantes são úteis visto que ao elevarmos a dimensão do código o problema se torna combinatorialmente difícil. Desta maneira, apresentamos neste trabalho um contexto em que como espectro de peso m, que é obtido atráves de um subcódigo $\mathcal{D} \subset \mathcal{C}$ com dimensão r nos intrigou, pois há caminhos que indicam que a hierarquia de pesos e os espectros são capazes de determinar a equivalência entre códigos.

Conceitos preliminares

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

Definição 2. A r-ésima distância de Hamming $d_r(\mathcal{C}) = \min\{|Supp(D)| : D \subset \mathcal{C} \ e \ \dim D = r\}$.

Teorema 1. Para um código linear $\mathcal{C}$ em $\mathbb{F}_q^n$ de parâmetros $[n, k, d_1, \dots, d_k]$ temos $1 \leq d_1(\mathcal{C}) < d_2(\mathcal{C}) < \dots < d_k(\mathcal{C}) \leq n$.

Demonstração. Considere os códigos $\mathcal{D}_{r-1}$ e $\mathcal{D}_r$ com dimensões $r-1$ e r respectivamente. Assumindo que $d_{r-1}(\mathcal{C}) = \|\mathcal{D}_{r-1}\|_{Supp}$ e $d_r(\mathcal{C}) = \|\mathcal{D}_r\|_{Supp}$. Note que se $\|\mathcal{D}_{r-1}\|_{Supp} > \|\mathcal{D}_r\|_{Supp}$ para qualquer subcódigo $\mathcal{S}_{r-1} \subset \mathcal{D}_r$, teríamos $\|\mathcal{S}_{r-1}\|_{Supp} \leq \|\mathcal{D}_r\|_{Supp} < \|\mathcal{D}_{r-1}\|_{Supp}$, contrariando a minimalidade de $d_{r-1}(\mathcal{C})$. Para mostrar as desigualdades estritas basta observar que para r fixo e um subcódigo $\mathcal{S} \subset \mathcal{C}$ em que $\|\mathcal{S}\|_{Supp} = d_r(\mathcal{C})$, tomando $i \in Supp(\mathcal{S})$ e definindo $\mathcal{S}_i = \{c \in \mathcal{S} : c_i = 0\}$, então $\mathcal{S}_i$ é um subcódigo de dimensão $r-1$, mais ainda, vale que

$$d_{r-1}(\mathcal{C}) \leq \|\mathcal{S}_i\|_{Supp} \leq \|S\|_{Supp} - 1 = d_r(\mathcal{C}) - 1.$$

□

Definição 3.(Espectro) 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 $A_i^j = |\{D \subset \mathcal{C} : \dim(D) = i \ e \ \ |Supp(D)| = j\}|$.

Exemplo.

Considerando a matriz geradora $G = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 0 \end{bmatrix}$

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

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

Definição 4. 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 $Spec(C') = Spec(C)$.

Definição 5. (Códigos binários com base preservado o espectro) Dado os códigos binários $\mathcal{C}_1$ e $\mathcal{C}_2$, ambos com dimensão k e comprimento n. Eles admitem espectro preservando a base se para qualquer base $\mathcal{B} = \{c_1, \dots, c_k\}$ existe $\mathcal{B}' = \{c'_1, \dots, c'_k\}$ tal que $\omega(c_j) = \omega(c'_j)$ para qualquer $j \in \{1, 2, \dots, k\}$.

Teorema 2. Dados os códigos Binários $\mathcal{C}_1$ e $\mathcal{C}_2$ com comprimento n e dimensão k. Eles admitem base preservando o espectro se, e somente se, $Spec(\mathcal{C}_1) = Spec(\mathcal{C}_2)$.

Resultados

• ***Teorema 3.*** Dado dois códigos binários equivalentes, eles possuem o mesmo espectro.

Demonstração. (Ideia) 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 $D' \leq C_2 \rightarrow \sigma^{-1}(D') \leq C_1$. Além disso preserva-se os suportes de cada um dos subcódigos, ou seja, $|Supp(D)| = |Supp(\sigma(D))|$ e ainda $|Supp(D')| = |Supp(\sigma(D'))|$ fornecendo portanto uma bijeção induzida por σ, entre os subespaços logo $Spec(C_1) = Spec(C_2)$. □

• Em baixas dimensões bem como suas respectivas codimensão é possível concluir que para dois códigos binários k-dimensionais com mesmo espectro, estes códigos são equivalentes para $k = 1$, $k = 2$, $k = n-1$ e $k = n-2$.

• Conjectura. (Com a recíproca do **Teorema 3**) Dois códigos binários são equivalentes se, e somente se, têm o mesmo espectro.

Conclusão e perspectivas futuras

Com a conjecutra verificada poderemos incluir o espectro como um importante invariante para códigos lineares. O espectro também poderá ser uma ferramenta últil para análise entre códigos cuja primeira distância mínima se iguala. Até dimensão $n = 11$ temos resultados positivos sobre a validação da conjectura .

Buscamos apresentar neste trabalho, que faz parte da tese de doutorado em andamento, um novo parâmetro para avaliar códigos e suas respectivas capacidade de correção para cada r escolhido. Ainda temos uma segunda alternativa utilizando os pesos generalizados que é observar a relevância com o raio de empacotamento determinado pelo peso generalizado, isto é , considerar o raio $r = \left\lfloor \frac{d_r(\mathcal{C})-1}{2} \right\rfloor$.

Referências

[1] Tor Helleseth, Torleiv Klove, and Øyvind Ytrehus. Generalized hamming weights of linear codes. *IEEE transactions on information theory*, 38(3):1133–1140, 1992.

[2] Darwin Gregorio Villar Salinas. *On linear block codes: classification and estimation of bounds for weight hierarchy of codes*. PhD thesis, [sn], 2022.

[3] Michael A Tsfasman and Serge G Vladut. Geometric approach to higher weights. *IEEE Transactions on Information Theory*, 41(6):1564–1588, 1995.

[4] Victor K Wei. Generalized hamming weights for linear codes. *IEEE Transactions on information theory*, 37(5):1412–1418, 1991.