Proceeding Series of the Brazilian Society of Computational and Applied Mathematics, v. 6, n. 2, 2018.

Trabalho apresentado no XXXVIII CNMAC, Campinas - SP, 2018.

Proceeding Series of the Brazilian Society of Computational and Applied Mathematics

Códigos de Grupo n-shot via Isomorfismo entre Espaços Projetivos e Reticulados de Grupos Multiplicativos de Corpos Finitos

Leandro Bezerra de Lima[1]
CPAq - Campus de Aquidauana, UFMS, Aquidauana, MS
Reginaldo Palazzo Júnior[2]
FEEC - Faculdade de Engenharia Elétrica e Computação, Unicamp, Campinas, SP

RESUMO

O objetivo deste trabalho é apresentar uma proposta de construção de códigos de subespaço de grupos n-shot, [1], através do uso do isomorfismo existente entre o reticulado de um grupo abeliano, este consistindo do produto direto de grupos abelianos finitos multiplicativos das unidades de $\mathbb{F}_p$, e o diagrama de Hasse de espaços projetivos $\mathbb{P}(\mathbb{F}_p^m)$. O modelo de canal sendo considerado é o canal matricial multiplicativo q-ário, $Y = AX$, onde $X \in \mathbb{F}_q^{n\times l}$ é a matriz cujas linhas são os n pacotes injetados na rede pelo nó fonte, $Y \in \mathbb{F}_q^{m\times l}$ é a matriz cujas linhas são os m pacotes coletados pelo nó destino e $G \in \mathbb{F}_q^{m\times n}$ é a matriz de transferência de X para Y, [2]. Este canal justifica a viabilidade de comunicação via subespaços, onde a informação é enviada através da escolha do subespaço gerado pelas linhas da matriz de entrada. Sabendo que o espaço vetorial $\mathbb{F}_q^m$ é isomorfo a $\mathbb{F}_{q^m}$, onde q é um primo ou potência de primo e m é um inteiro positivo, temos as seguintes definições,

Definição 1. *O **espaço projetivo** consiste do conjunto de todos os subespaços vetoriais de $\mathbb{F}_q^m$ e será denotado por $\mathbb{P}(\mathbb{F}_q^m)$. Além disso, o conjunto de todos os subespaços com uma dada dimensão k é chamado **Grassmanniana** e será denotada por $\mathcal{G}(\mathbb{F}_q^m, k)$. Note que $\mathbb{P}(\mathbb{F}_q^m) = \bigcup_{k=0}^m \mathcal{G}(\mathbb{F}_q^m, k)$.*

Definição 2. *Um **código de subespaço** $\mathcal{C}$ é um conjunto não vazio de $\mathbb{P}(\mathbb{F}_q^m)$. No caso do código de subespaço pertencer a uma Grassmanniana de ordem k, $\mathcal{G}(\mathbb{F}_q^m, k) = \{V \in \mathbb{P}(\mathbb{F}_q^m) : dimV = k\}$, todas as palavras-código têm a mesma dimensão. Este código é chamado **código de subespaço de dimensão constante**. A distância mínima de $\mathcal{C}$ será denotada por d.*

Definição 3. *A **distância de subespaço** entre U e V é definida como: $d(U,V) = dim(U) + dim(V) - 2dim(U \cap V)$, onde $+$ e $\cap$ denotam, respectivamente, a soma e a interseção de subespaços.*

[1]leandro.lima@ufms.br
[2]palazzojr@gmail.com

Definição 4. *Os* ***parâmetros*** *do código de subespaço* $\mathcal{C} \subset \mathbb{P}(\mathbb{F}_q^m)$*, são denotados por* (m, M, d)*, onde* m *é a dimensão do espaço projetivo,* M *é a cardinalidade, e* d *é a distância mínima. Se* $\mathcal{C}$ *pertence a uma Grassmanniana de dimensão* k*, os correspondentes parâmetros são* (m, M, d, k)*.*

Definição 5. *O* n***-ésimo produto cartesiano*** *do espaço projetivo* $\mathbb{P}(\mathbb{F}_q^m)$ *será denotado por* $\mathbb{P}(\mathbb{F}_q^m)^n$*. Assim, os elementos de* $\mathbb{P}(\mathbb{F}_q^m)^n$ *são t-uplas tendo como componentes os subespaços do espaço projetivo original* $\mathbb{P}(\mathbb{F}_q^m)$*, onde* $2 \leq t \leq n$*.*

Definição 6. *A* ***distância de subespaço*** *entre* $\boldsymbol{U} = (U_1, U_2, ..., U_n)$ *e* $\boldsymbol{V} = (V_1, V_2, ..., V_n)$ *pertencentes a* $\mathbb{P}(\mathbb{F}_q^m)^n$ *é definida como:* $d(\boldsymbol{U}, \boldsymbol{V}) = \sum_{i=1}^{n} d(U_i, V_i)$*, onde* $d(U_i, V_i) = dim(U_i) + dim(V_i) - 2dim(U_i \cap V_i)$ *para* $i \in \{1, 2, ..., n\}$*. Então,* $1 \leq d(\boldsymbol{U}, \boldsymbol{V}) \leq m.n$*.*

Consequentemente, $(\mathbb{P}(\mathbb{F}_q^m)^n, d)$ é um espaço métrico. Um **código de bloco de subespaço** é um subconjunto não vazio $\boldsymbol{\mathcal{C}} \subset \mathbb{P}(\mathbb{F}_q^m)^n$ chamado **código de subespaço** $\boldsymbol{n}$**-shot**. Assim, os **parâmetros** do código $\boldsymbol{\mathcal{C}} \subset \mathbb{P}(\mathbb{F}_q^m)^n$ são denotados por $(m.n, M^n, d)$, onde $m.n$ é a dimensão do espaço projetivo, M^n é a cardinalidade do código, e d é a distância mínima. Se $\boldsymbol{\mathcal{C}}$ pertence a uma Grassmanniana de dimensão $k.n$ os parâmetros do código são $(m.n, M^n, d, k.n)$.

Neste trabalho, mostraremos a existência de um isomorfismo (função bijetora isótona com inversa isótona) entre uma classe de espaços projetivos $\mathbb{P}(\mathbb{F}_p^m)$ e uma estrutura algébrica consistindo do produto direto de grupo das unidades do corpo finito $\mathbb{F}_p$, ver [3] e [4]. A importância deste isomorfismo reside no fato de que será possível explicitar a estrutura algébrica inerente tanto a cada subespaço (palavra-código) como do código de subespaço de grupo, além claro, dos subcódigos em sua cadeia de decomposição. Adicionalmente, poderá resultar em uma proposta alternativa de decodificação de tais códigos.

Palavras-chave. Espaços Projetivos, Códigos de Subespaços, Reticulados de Grupo, Códigos de Grupo.

Referências

[1] R. Nóbrega and B. Uchôa-Filho, Multishot Codes for Network Coding: Bounds and a Multilevel Construction, *in Proceedings of the 2009 IEEE International Symposium on Information Theory - ISIT-09*, Seoul, South Korea, Jun. 2009.

[2] D. Silva and F. R. Kschischang and R. Köetter, Communication over finite-field matrix channels, *IEEE Transactions on Information Theory*, vol. 56, n.º2, pp. 1296-1305, 2010.

[3] L. B. de Lima. Contribuições em codificação no espaço projetivo e proposta de códigos quânticos de subespaços na grassmanniana, *Tese(Doutorado em Engenharia Elétrica)* -Faculdade de Engenharia Elétrica e de Computação-Unicamp. Campinas, 2017.

[4] L. B. Lima and R. Palazzo Junior, Geometrically uniform n-shot subspace codes, *Electronic Notes in Discrete Mathematics*, vol. 57, pp. 47-54, 2017.

