Proceeding Series of the Brazilian Society of Applied and Computational Mathematics, Vol. 3, N. 1, 2015.
Trabalho apresentado no XXXV CNMAC, Natal-RN, 2014.

Códigos lineares sobre corpos finitos através da métrica de Lee

Antonio Aparecido de Andrade **Robson Ricardo de Araujo***
Departamento de Matemática, IBILCE, UNESP,
15054-000, São José do Rio Preto, SP
E-mail: andrade@ibilce.unesp.br, dearaujorobsonricardo@gmail.com

RESUMO

A Teoria dos Códigos Corretores de Erros foi inaugurada por Claude Shannon em meados do século XX. Desde então, vários estudos começaram a ser desenvolvidos nessa área e contribuíram para que os dados passassem a ser transmitidos por meio dos mais diversos canais de comunicações de maneira mais segura. Usualmente, os códigos são tratados sobre a métrica de Hamming. Ao atravessar um canal, uma mensagem pode sofrer erros. Na métrica de Hamming, cada erro é a mudança de uma *coordenada* entre a palavra do código e a palavra recebida. Como alternativa a essa métrica para códigos não binários, foi desenvolvida a métrica de Lee, na qual cada erro é definido como mudança de uma *unidade* entre a palavra do código e a palavra recebida. Códigos sob a métrica de Lee começaram a ser estudados em 1957 por W. Ulrich e em 1958 por C. Y. Lee. Esse tipo de erro é encontrado em canais ruidosos que usam modulação PSK e em canais que são suscetíveis à sincronização de erros.

Seja $a \in \mathbb{Z}_q$ (anel dos inteiros módulo q), para algum $q \in \mathbb{Z}_+^*$. O valor de Lee de a, denotado por $|a|$, é definido como a, se $0 \leq a \leq q/2$, ou $q-a$, se $q/2 < a \leq q-1$. Dados dois vetores $c = (c_1, c_2, \ldots, c_n)$ e $d = (d_1, d_2, \ldots, d_n)$ sobre $\mathbb{Z}_q$, o peso de Lee de c é $w_L(c) = \sum_{j=1}^{n} |c_i|$ e a distância de Lee entre eles é definida como $d_L(c, d) = w_L(c - d)$, que é uma métrica. Seja $C \subset \mathbb{Z}_q^n$ um conjunto. A distância de Lee mínima de C é definida como a menor das distâncias mínimas entre todos os vetores de C e é denotado por $d_L(C)$. Comparando as duas métricas comentadas (Hamming e Lee), sabe-se que sobre $\mathbb{Z}_2$ e $\mathbb{Z}_3$, a distância de Lee e a distância de Hamming entre dois vetores coincidem; mas, se $q > 3$, a distância de Lee é superior à de Hamming.

Se C é um código linear, isto é, um $\mathbb{Z}_q$-submódulo de $\mathbb{Z}_q^n$, então $d_L(C)$ é o menor dos pesos entre todos os vetores de C. Seja ainda $c \in C$ uma palavra transmitida para um canal de comunicação e $y \in \mathbb{Z}_q^n$ o vetor recebido depois da transmissão. Assim, $e = y - c$ é chamado de vetor erro da transmissão e o número de erros de Lee é dado por $w_L(e)$. Se $C \subset \mathbb{Z}_q^n$ é um código linear cuja distância mínima é d, então C pode corrigir até $(d-1)/2$ erros de Lee. Como consequência deste fato, concluímos que para corrigir vetores que sofram até t erros de Lee, é necessário usar um código com distância mínima de Lee maior ou igual a $2t + 1$.

Na métrica de Hamming, os chamados códigos BCH (lineares) são conhecidos por serem bons corretores de erros. Com base nisso, em [1] os autores buscaram e encontraram limites inferiores para a distância mínima de Lee em códigos BCH. Além disso, um código corretor de erros só pode ser considerado bom (e útil) quando é fornecido um eficiente algoritmo de decodificação de uma palavra recebida do canal de comunicação. Utilizando-se do Algoritmo Euclidiano da divisão, em [1] os autores também fornecem um algoritmo de decodificação para códigos BCH. Neste trabalho, desenvolvemos o estudo de códigos BCH sob a métrica de Lee, onde expomos o Teorema do Limite Inferior, descrevemos Algoritmo de Decodificação fazendo uso do Algoritmo Euclidiano e concluímos com um exemplo aplicado dessa

*Bolsista de Mestrado CAPES

teoria.

Especificamente, um código BCH de tamanho n sobre $\mathbb{Z}_p$, onde p é um primo, é um código linear $C(n, r, \alpha; p) \subset \mathbb{Z}_p^n$ cujos elementos $c \in C$ são tais que $Hc^T = 0$, onde r é um inteiro positivo, $\alpha = (\alpha_1, \ldots, \alpha_n)$ é o *vetor localizador do código* e pertence a $GF(p^m)$ (o menor corpo finito de cuja ordem é maior do que n) e $H = [\alpha_j^{i-1}]_{r \times n}$ é a matriz teste de paridade do código. Se $m = 1$, $C(n, r, \alpha; p)$ é chamado código sobre o corpo base. No caso em que $n = p^m - 1$, o código $C(n, r, \alpha; p)$ é chamado código primitivo.

O Teorema do Limite Inferior para códigos BCH nos diz que a distância mínima de Lee $d_L(n, r, \alpha; p)$ do código BCH $C(n, r, \alpha; p)$ satisfaz

$$d_L(n, r, \alpha; p) \geq \begin{cases} 2r & se\ r \leq \frac{p-1}{2} \\ p & se\ \frac{p+1}{2} \leq r < p. \end{cases}$$

Se $C(n, r, \alpha; p)$ é um código sobre o corpo base, podemos ignorar a condição $r \leq \frac{p-1}{2}$, isto é, $d_L(n, r, \alpha; p) \geq 2r$ para todo $r \leq n \leq p - 1$. Se $C = C(p - 1, \alpha, r; p)$ é um código BCH primitivo sobre o corpo base com dimensão $k \neq 0$ ($k = p - 1 - r$), então $d_L(C) \geq (p^2 - k^2)/(4k)$, que é uma cota inferior para C melhor do que $2r$ se $r \geq 6p/7$.

O Algoritmo de Decodificação de Códigos BCH sob a métrica de Lee que comentamos anteriormente pode ser aplicado quando $r \leq (p - 1)/2$ ou $r \leq n \leq p$, pois nesse caso o código $C(n, r, \alpha; p)$ tem distância mínima de Lee $d_L \geq 2r$ e, portanto, é capaz de corrigir $r - 1$ erros de Lee.

Pode-se também tratar de códigos BCH sobre $\mathbb{Z}$ (e não mais sobre $GF(q)$), que são chamados códigos inteiros. Neste caso, pode-se estender as definições de valores de Lee, distância mínima de Lee e de códigos BCH sob essa métrica em $\mathbb{Z}^n$. Dessa forma, consegue-se associar um código inteiro BCH a um reticulado integral $L_q(C)$ via a chamada Construção A. Os autores em [2] desenvolvem esta teoria e fornecem um algoritmo de decodificação para esse reticulado via métrica de Lee.

Por fim, citamos que houve a tentativa de generalizar as ideias aplicadas nesse estudo para desenvolver uma teoria mais geral para código Alternantes ou códigos de Goppa. Porém, não obtivemos resultados satisfatórios até o momento. Em nosso plano futuro, pretendemos nos dedicar ao estudo da Teoria Algébrica dos Número aplicada à Teoria dos Códigos Corretores de Erros, dos quais podem surgir novas contribuições à teoria apresentada neste trabalho.

Palavras-chave: *Métrica de Lee, Códigos BCH, Códigos Corretores de Erros*

Referências

[1] Roth, R., Siegel, P. *Lee-Metric BCH Codes and their Application to Constrained and Partial-Response Channels*. IEEE Transactions on Information Theory, vol. 40, no. 4, 1994.

[2] Campello, A., Jorge, G., Costa, S. *Decoding q-ary lattices in the Lee metric*. ArXiv e-prints, Cornell University, 2011.

[3] Blahut, R. *Theory and Practice of Error Control Codes*. Addison-Wesley Publishing Company, 1984, London.

[4] Rodrigues, J., Carvalho, D. *Compactificação de Informação via Métrica de Lee*. In: IV Congresso Internacional de Matemática Aplicada e Computacional, 2008, Lambayeque.

[5] Roth, R. *Introduction to Coding Theory*. Cambridge University Press, 2006.

[6] MacWilliams, F., Sloane, N. *The Theory of Error-Correcting Codes*. North-Holland, 1988.

