Proceeding Series of the Brazilian Society of Computational and Applied Mathematics, v. 11, n. 1, 2025.

Trabalho apresentado no XLIII CNMAC, Centro de Convenções do Armação Resort - Porto de Galinhas - PE, 2024

Proceeding Series of the Brazilian Society of Computational and Applied Mathematics

Álgebras dos Quatérnios: Uma Abordagem para Códigos de Bloco Espaço-Tempo

Carina Alves[1]
IGCE/Unesp, Rio Claro-SP
Plínio Gabriel Sicuti[2]
Ibilce/Unesp, São José do Rio Preto-SP
Agnaldo José Ferrari[3]
FC/Unesp, Bauru-SP
Nicoll Vanessa Jerez Nieves [4]
IGCE/Unesp, Rio Claro-SP

No contexto da criptografia, as álgebras de divisão são exploradas no problema de aprendizado com erros (LWE - *Learning With Errors*), que é a base para muitos esquemas criptográficos seguros contra ataques de computação quântica. As álgebras de divisão contribuem para o desenvolvimento de versões mais eficientes e seguras dos esquemas baseados em LWE, proporcionando uma estrutura algébrica complexa que favorece a geração de instâncias desafiadoras do problema LWE, além de contribuir significativamente para a redução da complexidade computacional e do tamanho das chaves criptográficas, [4].

Por outro lado, na área de comunicações sem fio, à qual demos ênfase neste trabalho, a estrutura algébrica das álgebras de divisão viabiliza a construção de códigos de bloco espaço-tempo (STBC - *Space-Time Block Codes*), [7]. Diversidade máxima (isto é, maior confiabilidade do sinal) e maior determinante mínimo (isto é, maior ganho de codificação) são os dois mais importantes critérios para construir bons STBC. Os autores de [5] sugeriram que se deve usar uma ordem maximal de uma álgebra como um código reticulado, em vez da ordem natural que é amplamente utilizada, a fim de maximizar o ganho de codificação. Porém, encontrar ordens maximais dentro de uma álgebra não é uma tarefa simples e as álgebras de divisão cíclicas que produzem códigos com bom determinante mínimo são aquelas que têm como corpo base os corpos quadráticos imaginários, [8].

Diante disso, surge a seguinte questão: quais álgebras de divisão cíclicas são mais adequadas neste cenário? Consideramos neste trabalho, álgebras de divisão dos quatérnios, que são um caso especial das álgebras cíclicas, e consideramos os corpos quadráticos imaginários como corpo base. Mediante a escolha de um ideal adequado dentro de uma ordem maximal é possível construir o reticulado de maior densidade de empacotamento na dimensão 8, ou seja, o reticulado E_8.

Algumas construções do reticulado E_8 via álgebras dos quatérnios foram apresentadas em [1, 2], onde os autores consideraram como corpo base os corpos quadráticos imaginários $\mathbb{Q}(\sqrt{d})$, $d = -1, -2, -3, -7$ e os subcorpos maximais reais de corpos ciclotômicos, respectivamente.

Na tentativa de generalizar os resultados de [1] para qualquer corpo quadrático $\mathbb{F}$ cujos ideais no anel dos inteiros de $\mathbb{F}$ sejam principais, investigamos álgebras de divisão dos quatérnios $\mathcal{A} = (a, b)_{\mathbb{F}}$, para $\mathbb{F} = \mathbb{Q}(\sqrt{-11})$ e $\mathbb{F} = \mathbb{Q}(\sqrt{-19})$. Buscamos tais álgebras que se mostrassem favoráveis ao contexto de códigos espaço-tempo. Por exemplo, exigimos $|b| = 1$ para assegurar a igualdade

[1]carina.alves@unesp.br
[2]plinio.sicuti@unesp.br
[3]agnaldo.ferrari@unesp.br
[4]jerez.nieves@unesp.br

© 2025 SBMAC

da energia média transmitida por cada antena em todos os intervalos de tempo. Além disso, na tentativa de construir $\sqrt{c}E_8$, isto é, uma versão escalonada do reticulado de E_8 para algum inteiro c, exigimos que o determinante de um reticulado construído via álgebra dos quatérnios seja igual ao determinante de $\sqrt{c}E_8$.

Diante disso, para o corpo base $\mathbb{F} = \mathbb{Q}(\sqrt{-11})$ encontramos ideais $\mathcal{I}_1$ e $\mathcal{I}_2$ com norma absoluta 3 e 11, respectivamente. Para o corpo base $\mathbb{F} = \mathbb{Q}(\sqrt{-19})$ encontramos ideais $\mathcal{I}_1$ e $\mathcal{I}_2$ com norma absoluta 7 e 19, respectivamente. Além disso, discutimos a propriedade do bom arredondamento de tais reticulados, segundo [3].

A motivação para considerar símbolos de informação em outros anéis de inteiros de corpos quadráticos imaginários, ao invés de $\mathbb{Q}(i)$ e $\mathbb{Q}(\zeta_3)$, frequentemente empregados na maioria dos problemas de comunicação, reside nos estudos da última década. Esses trabalhos exploram os símbolos de informação no anel de inteiros algébricos de corpos quadráticos imaginários de forma mais ampla, conforme apresentado em [6].

Agradecimentos

Esta pesquisa é financiada pela FAPESP Proc. 2023/15735-8, 2019/20800-8 e CNPq 405842/2023-6. As opiniões, hipóteses e conclusões ou recomendações expressas neste material são de responsabilidade dos autores e não necessariamente refletem a visão da FAPESP e do CNPq.

Referências

[1] C. Alves e J.-C. Belfiore. "Lattices from maximal orders into quaternion algebras". Em: **Journal of Pure Applied Algebra** 4 (2015), pp. 687–702. DOI: 10.1016/j.jpaa.2014.04.025.

[2] C. W. O. Benedito, C. Alves, N. G. Brasil Jr e S. I. R. Costa. "Algebraic construction of lattices via maximal quaternion orders". Em: **Journal of Pure and Applied Algebra** 5 (2020), p. 106221. ISSN: 0022-4049. DOI: 10.1016/j.jpaa.2019.106221.

[3] L. Fukshansky e K. Petersen. "On well-rounded ideal lattices". Em: **International Journal of Number Theory** 1 (2012), pp. 189–206. DOI: 10.1142/S179304211250011X.

[4] C. Grover, A. Mendelsohn, C. Ling e R. Vehkalahti. "Non-commutative Ring Learning with Errors from Cyclic Algebras". Em: **Journal of Cryptology** 3 (2022). DOI: 10.1007/s00145-022-09430-6.

[5] C. Hollanti e J. Lahtonen. "A New Tool: Constructing STBCs from Maximal Orders in Central Simple Algebras". Em: **2006 IEEE Information Theory Workshop - ITW '06 Punta del Este**. 2006, pp. 322–326. DOI: 10.1109/ITW.2006.1633838.

[6] Y.-C. Huang, K. R. Narayanan e P.-C. Wang. "Lattices over algebraic integers with an application to compute-and-forward". Em: **IEEE Transactions on Information Theory** 10 (2018), pp. 6863–6877. DOI: 10.1109/TIT.2018.2848277.

[7] F. E. Oggier, J.-C. Belfiore e E. Viterbo. "Cyclic Division Algebras: A Tool for Space-Time Coding". Em: **Foundations and Trends in Communications and Information Theory** (2007), pp. 1–95. DOI: 10.1561/0100000016.

[8] R. Vehkalahti, C. Hollanti e J. Lahtonen. "On the Densest MIMO Lattices from Cyclic Division Algebras". Em: **IEEE Transactions on Information Theory** (2009). Aceito. DOI: 10.1109/TIT.2009.2023713.

© 2025 SBMAC