Proceeding Series of the Brazilian Society of Applied and Computational Mathematics, Vol. 5, N. 1, 2017.

Trabalho apresentado no CNMAC, Gramado - RS, 2016.

Proceeding Series of the Brazilian Society of Computational and Applied Mathematics

---

Construção do Reticulado E_8 via Corpos de Números Abelianos

Eliton Mendonça Moro[1]
Departamento de Matemática, UNESP, São José do Rio Preto, SP
Carina Alves[2]
Departamento de Matemática, UNESP, Rio Claro, SP
Antonio Aparecido de Andrade[3]
Departamento de Matemática, UNESP, São José do Rio Preto, SP

1 Introdução

Constelações de sinais tendo estrutura de reticulados são usadas para a transmissão de sinais, pois a estrutura linear e simétrica dos reticulados facilita a tarefa de decodificação.

Um dos principais objetivos na teoria dos reticulados é encontrar reticulados com alta densidade de empacotamento. Os reticulados mais densos são conhecidos somente em dimensão $n = 1, \cdots, 8$ e em dimensão 24 [2].

Reticulados algébricos são reticulados obtidos via o anel dos inteiros $\mathcal{O}_{\mathbb{F}}$, de um corpo de números $\mathbb{F}$. Eles podem ser construídos considerando representações geométricas de ideais em $\mathcal{O}_{\mathbb{F}}$ [2]. Este último método foi usado por Craig [4] para construir o reticulado de Leech a partir de um ideal $\mathcal{I}$ devidamente escolhido em $\mathbb{Z}[\zeta_{39}]$, o anel dos inteiros do corpo ciclotômico $\mathbb{F} = \mathbb{Q}(\zeta_{39})$.

Além do reticulado de Leech, Craig [3] mostrou que os reticulados D_4, E_8, K_{12}, e Λ_{16} podem ser obtidos via ideais devidamente escolhidos nos anéis dos inteiros dos corpos ciclotômicos. Em [1], Bayer-Fluckiger mostrou que E_8 pode ser obtido via um ideal $\mathcal{I}$ em $\mathcal{O}_{\mathbb{F}}$, $\mathbb{F} = \mathbb{Q}(\zeta_{15})$, $\mathbb{Q}(\zeta_{20})$, $\mathbb{Q}(\zeta_{24})$.

Neste trabalho focamos na construção do reticulado E_8. Nosso objetivo é construir o reticulado E_8 via infinitos corpos de números abelianos.

2 A Construção

Para a construção do reticulado E_8, consideramos p e q primos ímpares distintos de modo que

$$ord\, q_p \equiv ord\, p_q \equiv 1 (mod\, 2). \tag{1}$$

[1] elitonmoro@hotmail.com
[2] carina@rc.unesp.br
[3] andrade@ibilce.unesp.br

O diagrama abaixo mostra as extensões de corpos que usamos, em que $M/\mathbb{Q}$ é Galois e $\mathcal{G} = Gal(M/\mathbb{Q})$ é abeliano.

$$
\begin{tikzcd}
 & \mathbb{Q}(\zeta_{pq}) \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\mathbb{Q}(\zeta_p) \arrow[d, dash] & M = K_1K_2 \arrow[dl, dash] \arrow[dr, dash] & \mathbb{Q}(\zeta_q) \arrow[d, dash] \\
K_1 \arrow[dr, dash] & & K_2 \arrow[dl, dash] \\
 & \mathbb{Q} &
\end{tikzcd}
$$

Usamos o fato de que a densidade de centro de E_8 é $\delta = 1/16$ e que se $p \equiv 1 (mod\, 4)$ existem infinitos primos q satisfazendo (1) para mostrar, a partir das ideias de [5], que é possível construir o reticulado E_8 via infinitos corpos de números abelianos.

3 Conclusões

Através da construção apresentada é possível construir o reticulado E_8 via corpos abelianos em geral e não somente via corpos ciclotômicos. Este é um trabalho em andamento, e a perspectiva é construir, via este método, outros reticulados de maior densidade de empacotamento. Ainda há muitos resultados envolvendo construções de reticulados e teoria dos números algébricos a serem descobertos e que fornecerão um aprimoramento na teoria da informação e na criptografia.

Referências

[1] E. Bayer-Fluckiger, Lattices and number fields, *Contemp. Math.*, 241:69-84, 1999.

[2] J.H. Conway, N.J.A Sloane. *Sphere Packing, Lattices and Groups.* Springer-Verlag, New York, 1999.

[3] M. Craig, Extreme forms and cyclotomic, *Mathematika*, 25:44-56, 1978b.

[4] M. Craig, A cyclotomic construction for Leech lattice, *Mathematika*, 25:236-241, 1978a.

[5] A. L. Flores, J. C. Interlando, T. P. da N. Neto, and A. L. Contiero, A new number field construction of the lattice E_8, *Beitr. Algebra Geom.*, 2012. DOI 10.1007/s13366-012-0095-5.