2011 XIX congresso interno de iniciação científica

E0424

O PROBLEMA DO VETOR MAIS PRÓXIMO NOS RETICULADOS RAÍZES: UMA ABORDAGEM COMPUTACIONAL

Alan Bondesan de Maria (Bolsista PIBIC/CNPq) e Prof. Dr. Cristiano Torezzan (Orientador), Faculdade de Ciências Aplicadas da Unicamp - Limeira - FCA, UNICAMP

Apresentamos neste trabalho um estudo introdutório sobre o problema da decodificação em reticulados. A ênfase é dada nos reticulados raízes Zn, An, Dn através do estudo de suas propriedades principais como matriz geradora, matriz de Gram, densidade de empacotamento, dentre outras. Apresentamos também os principais algoritmos utilizados para resolver o problema de encontrar um ponto do reticulado mais próximo de um ponto arbitrário do R^n. Os algoritmos foram implementados e testados no software Mathematica 8 e os resultados dos testes foram comparados com os da literatura. A generalização deste problema tem forte relação com os chamados criptossistemas pós-quânticos, que pode ser um tema para trabalho futuro.

Reticulados - Teoria de Códigos - Criptografia pós-quântica