Programa Institucional de Bolsas de Iniciação Científica
24 a 26 outubro de 2012
Pró-Reitoria de Pesquisa - Pibic/CNPq
Pró-Reitoria de Graduação - SAE/ Unicamp
XX congresso interno de iniciação científica da unicamp 2012

E0734

TEORIA DE RETICULADOS

Paulo Henrique Perin Facini (Bolsista ProFIS/CNPq) e Prof. Dr. João Eloir Strapasson (Orientador), Faculdade de Ciências Aplicadas da Unicamp - Limeira - FCA, UNICAMP

Um reticulado é um subconjunto de todas as combinações lineares inteiras de vetores linearmente independentes, o espaço vetorial suporte é o espaço euclidiano n-dimensional. Várias propriedades desta teoria tem relação com a álgebra linear clássica, entretanto a restrição aos inteiros promovem novas propriedades. Essencialmente os reticulados são grupos abelianos munidos de uma métrica euclidiana e os problemas complexos associados à métrica jogam um papel fundamental na criptografia, por outro lado problemas de natureza simples envolvendo a métrica contribuem com a teoria de códigos. Portanto, a teoria dos reticulados tem diversas aplicações, em especial na teoria de códigos (teoria que consiste em transformar informações em entes matemáticos e consequentemente usufruir das propriedades associadas) e da criptografia (a criptografia consiste em proteger informações). Os principais objetivos são promover, divulgar e ilustrar mais a teoria dos reticulados, já que esta é uma teoria altamente aplicável, com muitos resultados em trabalhos internacionais e ainda muito restrito no Brasil. O nosso trabalho está na fase inicial e apresentaremos uma introdução a teoria dos reticulados com a perspectiva de aplicação a teoria dos códigos ou a criptografia.

Reticulados - Códigos - Criptografia