Approximation Algorithms
June 12–14, 2006

Hardness of approximating the Shortest Vector Problem

Subhash Khot
khot@cc.gatech.edu
College of Computing
Georgia Institute of Technology
801 *Atlantic Drive*
Atlanta, GA 30332
USA

Abstract

In this talk, I will present a result showing that the *Shortest Vector Problem* in n-dimensional lattices is hard to approximate within factor (roughly) $2^{\sqrt{\log n}}$. The result holds for any l_p norm with $p > 1$. We first give a new (randomized) reduction from *Closest Vector Problem* (CVP) to SVP that achieves some constant factor hardness. The reduction is based on BCH codes. Its advantage is that the SVP instances produced by the reduction behave well under the augmented tensor product, a new variant of tensor product that we introduce. This enables us to boost the hardness factor to (roughly) $2^{\sqrt{\log n}}$. The paper appeared in FOCS'04.