

1048-49-264

Gábor Pataki (gabor@unc.edu), Dept. of Statistics and Operations Research, CB #3260, Hanes Hall, UNC Chapel Hill, Chapel Hill, NC 27599, and **Mustafa Kemal Tural*** (tural@email.unc.edu), Dept. of Statistics and Operations Research, CB #3260, Hanes Hall, UNC Chapel Hill, Chapel Hill, NC 27599. *On sublattice determinants in reduced bases.*

A basis reduction algorithm computes a reduced basis of a lattice consisting of “short” and “nearly orthogonal” vectors. The polynomial time LLL basis reduction algorithm was introduced in 1982 by Lenstra, Lenstra and Lovász; and has since been used in numerous applications in computational mathematics and computer science starting with factoring polynomials with rational coefficients and solving the integer linear programming problem in polynomial time in fixed dimensions.

As shown by Lenstra, Lenstra, and Lovász, in an LLL-reduced basis of a lattice L , the norm of the first vector is bounded by a function of the norm of a nonzero shortest vector of L , and also by a function of the determinant of L . We prove several inequalities on the determinants of sublattices in LLL-reduced bases generalizing these fundamental inequalities, and show that LLL-reduction finds not only a short vector, but also sublattices with small determinants.

We also prove new inequalities on the product of the norms of the first few basis vectors. (Received February 09, 2009)