GABOR PATAKI, UNC Chapel Hill

Basis Reduction, and the Complexity of Branch-and-Bound

Branch-and-bound is a classical method to solve integer programming feasibility problems. On the theoretical side, it is considered inefficient: it can provably take an exponential number of nodes to prove the infeasibility of a simple integer program. In this work we show that branch-and-bound is theoretically efficient, if we apply a simple transformation in advance to the constraint matrix of the problem which makes the columns short and near orthogonal. We analyze two such reformulation methods, called the rangespace and the nullspace methods. We prove that if the coefficients of the problem are drawn from $\{1, \ldots, M\}$ for a sufficiently large M, then for almost all such instances the number of subproblems that need to be enumerated by branch-and-bound is at most one. Besides giving an analysis of branch-and-bound, our main result generalizes results of Lagarias and Odlyzko, Frieze, and Furst and Kannan on the solvability of subset sum problems to bounded integer programs.

We give some numerical values of M which make sure that 99 percent of the reformulated problems solve at the rootnode. These values turned out to be surprisingly small for moderate values of n (the number of variables), and m (the number of constraints).

We also report the results of a computational study showing that branch-and-bound can efficiently solve subset sum problems with huge coefficients, that arise from cryptographic applications.

Joint work with Mustafa Tural at IMA, and Erick B. Wong at UBC.