1011-68-177 **Satyanarayana V. Lokam*** (satyalv@eecs.umich.edu), One Microsoft Way, Redmond, WA 98052. *Quadratic Lower Bounds on Matrix Rigidity.*

The rigidity of a matrix A with respect to the rank bound r is the minimum number of entries of A that must be changed to reduce the rank of A to or below r. It is a major unsolved problem (Valiant, 1977) to construct "explicit" families of $n \times n$ matrices of rigidity $n^{1+\delta}$ for $r = \epsilon n$ where ϵ and δ are positive constants. In fact, no superlinear lower bounds are known for explicit families of matrices for rank bound $r = \Omega(n)$.

In this paper we give the first optimal, $\Omega(n^2)$, lower bound on the rigidity of two "somewhat explicit" families of matrices with respect to the rank bound $r = cn$, where c is an absolute positive constant. The entries of these matrix families are (i) square roots of the first n^2 primes and (ii) primitive roots of unity of prime orders for the first n^2 primes. Our proofs use an algebraic dimension concept introduced by Shoup and Smolensky (1997) and a generalization of that concept. We note that square roots of primes have been used by Chen and Kao (1997) to reduce the number of random bits used in randomized algorithms for polynomial identity testing. (Received August 25, 2005)