Publications

Nitin Saxena

May 28, 2008

Journal Papers

1. *Parameters of Integral Circulant Graphs and Periodic Quantum Dynamics* (with S. Severini and I. E. Shparlinski), International Journal of Quantum Information, volume 5(4), pages 1–14, 2007.

   Abstract: The intention of the paper is to move a step towards a classification of network topologies that exhibit periodic quantum dynamics. We show that the evolution of a quantum system, whose hamiltonian is identical to the adjacency matrix of a circulant graph, is periodic if and only if all eigenvalues of the graph are integers (that is, the graph is integral). Motivated by this observation, we focus on relevant properties of integral circulant graphs. Specifically, we bound the number of vertices of integral circulant graphs in terms of their degree, characterize bipartiteness and give exact bounds for their diameter. Additionally, we prove that circulant graphs with odd order do not allow perfect state transfer.

2. *Polynomial Identity Testing for Depth* 3 *Circuits* (with N. Kayal), the special issue of the journal of Computational Complexity on the 21st Conference on Computational Complexity, volume 16(2), pages 115–138, 2007.

   Abstract: We study the identity testing problem for depth 3 arithmetic circuits ($\Sigma\Pi\Sigma$ circuit). We give the first deterministic polynomial time identity test for $\Sigma\Pi\Sigma$ circuits with bounded top fanin. We also show that the *rank* of a minimal and simple $\Sigma\Pi\Sigma$ circuit with bounded top fanin, computing zero, can be unbounded. These results answer the open questions posed by Klivans-Spielman (STOC 2001) and Dvir-Shpilka (STOC 2005).

3. *Complexity of Ring Morphism Problems* (with N. Kayal), the special issue of the journal of Computational Complexity on the 20th Conference on Computational Complexity, volume 15(4), pages 342–390, 2006.

   Abstract: We study the complexity of the isomorphism and automorphism problems for finite rings. We show that both integer factorization and graph isomorphism reduce to the problem of counting automorphisms of a ring. This counting problem is shown to be in the functional version of the complexity class AM$\cap$coAM and hence is not NP-complete unless the polynomial hierarchy collapses. As a "positive" result we show that deciding whether a given ring has a non-trivial automorphism can be done in deterministic polynomial time. Finding such an automorphism is, however, shown to be randomly equivalent to integer factorization.

4. *PRIMES is in P* (with M. Agrawal and N. Kayal), Annals of Mathematics, volume 160(2), pages 781–793, 2004. Awarded the Gödel Prize and the Fulkerson Prize for the year 2006.

   Abstract: We present an unconditional deterministic polynomial-time algorithm that determines whether an input number is prime or composite.

Refereed Conference Papers

1. *Diagonal Circuit Identity Testing and Lower Bounds*, in proceedings of the 35th International Colloquium on Automata, Languages and Programming, 2008, LNCS 5125, pp 60–71.

Abstract: Suppose we are given a depth-4 circuit (over any field $\mathbb{F}$) of the form:

$$C(x_1, \ldots, x_n) := \sum_{i=1}^{k} L_{i,1}^{e_{i,1}} \cdots L_{i,s}^{e_{i,s}}$$

where, each $L_{i,j}$ is a sum of univariate polynomials in $\mathbb{F}[x_1, \ldots, x_n]$. We can test whether C is zero deterministically in $poly(size(C), max_i\{(1 + e_{i,1}) \cdots (1 + e_{i,s})\})$ field operations. We also show exponential lower bounds for determinant and permanent for circuits of the above form.

2. *Polynomial Identity Testing for Depth* 3 *Circuits* (with N. Kayal), in proceedings of the 21st IEEE Computational Complexity Conference, 2006, pp 9–17. Awarded both the Best Paper Award and the Ronald V. Book Best Student Paper Award. Invited to the Special Issue of the journal Computational Complexity.

3. *Equivalence of $\mathbb{F}$-algebras and cubic forms* (with M. Agrawal), in proceedings of the 23rd Symposium on Theoretical Aspects of Computer Science, 2006, LNCS 3884, pp 115–126.

   Abstract: We study the isomorphism problem of two "natural" algebraic structures – $\mathbb{F}$-algebras and cubic forms. We prove that the $\mathbb{F}$-algebra isomorphism problem reduces in polynomial time to the cubic forms equivalence problem. For finite fields of the form $3 \not| (\#\mathbb{F} - 1)$, this result implies that the two problems are infact equivalent. This result yields the following "nice" relation: Graph Isomorphism $\leq_m^P$ $\mathbb{F}$-algebra Isomorphism $\leq_m^P$ Cubic Form Equivalence.

4. *Automorphisms of Finite Rings and Applications to Complexity of Problems* (with M. Agrawal), *invited talk*, in proceedings of the 22nd Symposium on Theoretical Aspects of Computer Science, 2005, LNCS 3404, pp 1–17.

   Abstract: A number of algebraic problems in computer science efficiently reduce to questions about automorphisms and isomorphisms of finite rings. In this paper, we collect several examples of this from the literature as well as providing some new and interesting connections. Specifically, we show that Graph Isomorphism can be reduced to cubic form equivalence. This explains, at least partly, why cubic forms have been hard to analyze.

5. *On the Ring Isomorphism & Automorphism Problems* (with N. Kayal), in the proceedings of the 20th IEEE Conference on Computational Complexity, 2005, pp 2–12. Invited to the Special Issue of the journal of Computational Complexity.

Manuscripts

1. *Schemes for Deterministic Polynomial Factoring* (with Gábor Ivanyos and Marek Karpinski), 2008, submitted.

   Abstract: In this work we relate the deterministic complexity of factoring polynomials (over finite fields) to certain combinatorial objects we call m-schemes. We extend the known conditional deterministic subexponential time polynomial factoring algorithm for finite fields to get an underlying m-scheme. We demonstrate how the properties of m-schemes relate to improvements in the deterministic complexity of factoring polynomials over finite fields assuming the generalized Riemann Hypothesis (GRH). In particular, we give the first deterministic polynomial time algorithm (assuming GRH) to find a nontrivial factor of a polynomial of prime degree n where $(n - 1)$ is a smooth number.

2. *On the Complexity of Cubic Forms* (with M. Agrawal), 2006, to be submitted.

   Abstract: We study the equivalence problem of cubic forms. We lower bound its complexity by that of $\mathbb{F}$-algebra isomorphism problem and hence by the graph isomorphism problem (for all fields $\mathbb{F}$). For finite fields we upper bound the complexity of cubic forms by NP$\cap$coAM. We also study the cubic forms obtained from $\mathbb{F}$-algebras and show that they are regular and indecomposable.

3. *Morphisms of Rings and Applications to Complexity*, PhD Thesis, Indian Institute of Technology, Kanpur, India, 2006.