

Previous Research

Shlomo Hoory

November 16, 2005

In general I am interested in real world problems that can be attacked with mathematical tools. For example, I ask the following question: Is the secure mode of Internet browsers really secure? The underlying cryptographic standard is DES. Therefore, the natural interpretation of the problem is to ask whether there exists a polynomial time algorithm for breaking DES-like constructions. However, proving such a statement involves separating P from NP . Instead of confronting this fundamental open question, I reformulated the problem as an information theoretic question, and obtained concrete results using the well developed machinery of Markov chains.

My past research has direct applications to cryptography, coding, proof systems, and complexity, using tools from graph theory, especially Markov chains and expander graphs.

- **The spectral properties and girth of irregular graphs**

A fundamental problem in extremal graph theory is obtaining a good lower bound on the size of a d -regular graph of a specified girth. Although much effort has been directed towards this problem in the past forty years, virtually no improvement has been achieved over the trivial graph theoretic Moore bound. A major part of my Ph.D. thesis [2, 8, 1, 6] is concerned with this problem.

One of my achievements is the generalization of the Moore bound to irregular graphs [1]. Our proof gives an affirmative answer to a long standing open problem asked by Bollobás in the 70's, appearing in his classical book "Extremal Graph Theory". I later extended this result to bipartite graphs, to show that the known bounds for girth 6 and 8 (due to Reiman, de Caen and Székely and to Neuwirth) can be generalized to an arbitrary girth, [6]. These bounds were found to be of interest for the error correcting codes community, since in the belief-propagation decoding algorithm, non-regular graphs with a specified degree sequence and high girth are of interest.

Building upon the techniques of [1, 6], I considered in [7] the extremal spectral properties of irregular graphs. I proved that the spectral radius of the universal cover of any graph with average degree $d \geq 2$ is at least $2\sqrt{d-1}$. As a consequence, I obtained a generalization of the well known Alon-Boppana lower bound to irregular graphs.

- **Mixing times and cryptographic applications**

A problem occurring naturally in cryptography, when considering block ciphers such as DES and AES, is how well the composition of permutations drawn from a simple distribution resembles a random permutation. In [10, 4], we consider the measure of closeness to k -wise independence: How many random permutations drawn from a small, explicit and simple family of permutations on the n -dimensional binary cube need be composed to achieve a permutation that is nearly k -wise independent. We obtained an upper bound that nearly matches the trivial lower bound for the problem, significantly improving upon previous result by Gowers 1996. Additionally, we introduce the new and stronger notion of closeness to k -wise independence against adaptive adversaries and show that the constructed permutation has the stronger property as well. The problem, which is essentially about the mixing time of a certain Markov chain, involves constructing good multicommodity flows, and comparing the log-Sobolev constants of two Markov chains.

- **Error correcting codes**

In [3], the problem of easily decodable, asymptotically good, error correcting codes was considered. We generalized the previous constructions and decoding algorithms for low density parity check (LDPC) codes given by Sipser and Spielman 1996, and Zemor 2001. Specifically, we defined the notion of an expanding hypergraph and employed it to construct a family of LDPC codes together with a belief-propagation decoding algorithm. This led to improvements over the above papers.

- **The power of geometric proof systems**

For many prominent NP-hard problems, the best known solutions are obtained using beautiful applications of semi-definite programming. Therefore, it is interesting to understand the limitations of such techniques. In [5], we considered the effectiveness of certain geometric proof

systems, such as the Lovász-Schrijver (LS) lift and project method, for proving the unsatisfiability of several prominent CNF formulas. Namely, we obtained tight linear lower bounds on the number of LS-rounds needed for random k -CNF formulas and for the Tseitin tautologies on expanding graphs. In addition, we proved that for the maxSAT optimization problem, even a linear number of LS-rounds does not suffice to reduce the integrality gap. One can view the later result as a way to improve upon PCP inapproximability results for specific proof systems.

- **Monotone circuits for the majority**

The complexity of monotone circuits for the majority function is a fascinating problem in theoretical computer science. Without the monotonicity restriction, majority can be solved by a simple linear-size circuits of depth $O(\log n)$, where the best known constant of the O is 4.95, Paterson et al. 1992. There are two fundamental constructions achieving logarithmic depth monotone circuits for the majority. The first is an elegant random formula, Valiant 1984, of depth $5.3 \log n + O(1)$ and size $O(n^{5.3})$. The second is derived from the sorting network of Ajtai, Komlós, and Szemerédi 1983. Although this circuit achieves depth $O(\log n)$ and size $O(n \log n)$, the best known constant of the O is 5000, Paterson 1990, which is too big for practical applications.

In [11], we suggest a simple method to reduce the size of Valiant’s construction, to $O(n^3)$, while maintaining its depth, and to $O(n^{2.42})$ at the expense of doubling the depth. The basic idea, that can be considered as a technique for partial derandomization, is to replace the notion of probabilistic amplification, used for Valiant’s analysis, by deterministic amplification. As part of the construction, we obtain optimal-depth linear-size monotone circuits for the promise version of the problem, where the number of 1’s in the input is promised to be either less than one third, or greater than two thirds. Furthermore, using results of Burshtein and Miller 2001 on belief propagation decoding, we show how to make the later circuit explicit, given a family of sufficiently expanding graphs. However, explicit construction of such graphs is not known yet.

- **Satisfiability of k -CNF formulas**

The satisfiability problem for k -CNF formulas is a fundamental NP-

complete problem. However, the satisfiability problem can be solved in many instances encountered in practice. It is therefore, of great interest to study simple restrictions that make the satisfiability problem easy. In [13, 12] we consider a problem regarding (k, s) -CNF formulas. Namely, formulas where each clause has exactly k literals and every variable occurs at most s times. Kratochvíl et al. 1993 proved that there exists a function $f(k)$ such that $(k, f(k))$ -CNF is always satisfiable, but the restriction of the SAT problem to $(k, f(k) + 1)$ -CNF formulas is already NP-complete. However, the exact values of $f(k)$ are not known for $k \geq 5$ and it is open whether $f(k)$ is computable. In [13] we introduce a computable function f_1 bounding f from above. By means of a calculus of integer sequences we determine $f_1(k)$ for $k \leq 9$, thus improving upon the known bounds on f for $k \in \{5, 6, 7, 8, 9\}$.

In [12] we focused on the asymptotic behavior of f_1 . Previously known asymptotic bounds on f were (i) a lower bound $f(k) \geq \Omega(2^k/k)$ due to Kratochvíl et al. 1993 and (ii) an upper bound $f(k) \leq O(2^k/k^{0.26})$ due to Savický and Sgall 2000. In [12], we exhibit an unsatisfiable family of k -CNF formulas where each variable has a small number of occurrences. This implies an improved bound, $f(k) \leq O(2^k \cdot \log k/k)$, which is tight up to a $\log k$ factor.

- **Topological obstructions to graph colorings**

There are not many known methods to lower bound the chromatic number of a graph. In 1978 Lovász solved the Knezer conjecture by showing that the Borsuk-Ulam Theorem prohibits coloring the Knezer graph with few colors. Since then, the idea of finding topological obstructions to graph colorings has been extensively studied (Babson and Kozlov 2003). In particular, Björner and Lovász have attempted to generalize the concept of a topological obstruction by conjecturing that any two graphs G, H for which the coloring complex $\text{Hom}(G, H)$ is k -connected, must satisfy $\chi(H) \geq \chi(G) + k + 1$. However, in [9], we refuted this conjecture by exhibiting an explicit graph G with chromatic number 5, such that $\text{Hom}(G, K_5)$ is 0-connected.

References

- [1] Noga Alon, Shlomo Hoory, and Nathan Linial. The Moore bound for irregular graphs. *Graphs and Combinatorics*, 18(1):53–57, 2002.
- [2] Alon Amit, Shlomo Hoory, and Nathan Linial. A continuous analogue of the girth problem. *Journal of Combinatorial Theory. Series B*, 84(2):340–363, 2002.
- [3] Yonatan Bilu and Shlomo Hoory. On codes from hypergraphs. *European Journal of Combinatorics*, 25(3):339–354, 2004.
- [4] Alex Brodsky and Shlomo Hoory. Simple permutation mix even better. Arxiv math.CO/0411098, submitted to Random Structures and Algorithms, 2005.
- [5] Joshua Buresh-Oppenheim, Nicola Galesi, Shlomo Hoory, Avner Magen, and Toniann Pitassi. Rank bounds and integrality gaps for cutting planes procedures. *IEEE Symposium on Foundations of Computer Science (FOCS)*, 2003.
- [6] Shlomo Hoory. The size of bipartite graphs with a given girth. *Journal of Combinatorial Theory. Series B*, 86(2):215–220, 2002.
- [7] Shlomo Hoory. A lower bound on the spectral radius of the universal cover of a graph. *J. Combin. Theory Ser. B*, 93(1):33–43, 2005.
- [8] Shlomo Hoory and Nathan Linial. Colorings of the d -regular infinite tree. *Journal of Combinatorial Theory. Series B*, 91(2):161–167, 2004.
- [9] Shlomo Hoory and Nathan Linial. A counterexample to a conjecture of björner and lovász on the χ -coloring complex. *Journal of Combinatorial Theory. Series B*, 95(2):346–349, 2005.
- [10] Shlomo Hoory, Avner Magen, Steve Myers, and Charles Rackoff. Simple permutations mix well. In *The 31st International Colloquium on Automata, Languages and Programming (ICALP)*, 2004.
- [11] Shlomo Hoory, Avner Magen, and Toniann Pitassi. Monotone circuits for the majority function. submitted to CCC 2006, 2005.
- [12] Shlomo Hoory and Stefan Szeider. Families of unsatisfiable k-cnf formulas with few occurrences per variable. Arxiv math.CO/0411167, submitted to *SIAM Journal on Discrete Mathematics*, 2004.

- [13] Shlomo Hoory and Stefan Szeider. Computing unsatisfiable k -SAT instances with few occurrences per variable. *Theoret. Comput. Sci.*, 337(1-3):347–359, 2005. Also in SAT 2004.