Banff International Research Station

for Mathematical Innovation and Discovery

Computational Complexity (10w5028)
August 1–6, 2010

MEALS

*Breakfast (Buffet): 7:00 – 9:30 am, Sally Borden Building, Monday – Friday
*****Lunch (Buffet): 11:30 am – 1:30 pm, Sally Borden Building, Monday – Friday
*****Dinner (Buffet): 5:30 – 7:30 pm, Sally Borden Building, Sunday – Thursday
Coffee Breaks: As per daily schedule, 2nd floor lounge, Corbett Hall
***Please remember to scan your meal card at the host/hostess station in the dining room for each meal.**

MEETING ROOMS

All lectures will be held in Max Bell 159 (Max Bell Building accessible by walkway on 2nd floor of Corbett Hall). LCD projector, overhead projectors and blackboards are available for presentations. *Note that the meeting space designated for BIRS is the lower level of Max Bell, Rooms 155-159. Please respect that all other space has been contracted to other Banff Centre guests, including any Food and Beverages in those areas.*

SCHEDULE

Sunday

16:00 check-in begins (Front Desk – Professional Development Centre - open 24 hours)
Lecture rooms available after 16:00 (if desired)
17:30-19:30 buffet dinner

Monday

7:00-8:40 breakfast
8:45-8:55 Introduction and Welcome by BIRS Station Manager, Max Bell 159

9:00-9:50 P. Raghavendra, *Approximating Graph Expansion: Connections, Algorithms and Reductions*
9:55-10:45 D. Moshkovitz, *Hardness of Approximately Solving Linear Equations Over Reals*

10:45-11:00 coffee break

11:05-11:55 D. Steurer, *Subexponential Algorithms for Unique Games and Related Problems*

12:00-13:00 lunch

13:05-13:55 D. van Melkebeek, *Satisfiability Allows No Nontrivial Sparsification Unless The Polynomial-Time Hierarchy Collapses*

14:00-14:50 R. Santhanam, *New and Improved Upper Bounds for Formula Satisfiability and TQBF*

14:50-15:30 coffee break

17:30-19:30 dinner

Tuesday

7:00-8:55 breakfast

9:00-9:50 S. Aaronson, *The Computational Complexity of Linear Optics*
9:55-10:30 C. Umans, P*seudorandom generators and the BQP vs. PH problem*

10:30-10:45 coffee break

10:50-11:20 Z. Dvir, *On matrix rigidity and locally self-correctable codes*
11:25-11:55 D. Wehr, *A lower bound for a restricted model of log-space computation*

12:00-13:00 lunch

13:05-13:45 L. Valiant, *Holographic Algorithms*
13:50-14:40 A. Sherstov, *Symmetrization Without Symmetries*

14:40-15:00 coffee break

15:05-15:55 V. Guruswami, *List decodability of random linear codes*

17:30-19:30 buffet dinner

Wednesday

7:00-8:55 breakfast

9:00-9:50 O. Regev, *Tight Bound for the Gap Hamming Distance Problem*
9:55-10:45 M. Braverman, *Compression, information and direct sum for communication complexity*

10:45-11:00 coffee break

11:05-11:55 A. Rao, *Recovering from Maximal Errors in Interactive Communication*

12:00-13:00 lunch

17:30-19:30 buffet dinner

Thursday

7:00-8:55 breakfast

9:00-9:50 D. Zuckerman, *Pseudorandom Generators for Polynomial Threshold Functions*
9:55-10:45 S. Lovett, P*seudorandom generators for CC0[p] and the Fourier spectrum of low-degree polynomials over finite fields*

10:45-11:00 coffee break

11:05-11:55 A. Klivans, *An Invariance Principle for Polytopes*

12:00-13:00 lunch

13:05-13:55 A. Yehudayoff, *Pseudorandom generators for regular branching programs*
14:00-14:50 P. Pudlak, *Pseudorandom Generators for Group Products*

14:50-15:30 coffee break

17:30-19:30 dinner

Friday

7:00-8:55 breakfast

9:00-9:50 E. Viola, *The complexity of distributions*
9:55-10:45 G. Kindler, *A Quantitative Proof of the Gibbard Satterthwaite Theorem*

10:45-11:00 coffee break

11:05-11:55 P. Beame, *Making RAMs Oblivious Requires Superlogarithmic Overhead*

12:00-13:30 lunch

Checkout by 12 noon.

** 5-day workshop participants are welcome to use BIRS facilities (2nd Floor Lounge, Max Bell Meeting Rooms, Reading Room) until 3 pm on Friday, although participants are still required to checkout of the guest rooms by 12 noon. **

Banff International Research Station

for Mathematical Innovation and Discovery

Name of 2010 5-day Workshop
Date of 2010 5-day Workshop

ABSTRACTS

(in alphabetic order by speaker surname)

S. Aaronson *The Computational Complexity of Linear Optics*

We propose a linear-optics experiment that might be feasible with current technology, and argue that, if the experiment succeeded, it would provide evidence that at least some nontrivial quantum computation is possible in nature. The experiment involves generating reliable single-photon states, sending the photons through a random linear-optical network, and then reliably measuring the photon number in each mode. The resources that we consider are not known or believed to be universal for quantum computation; nevertheless, we show that they would allow the solution of certain sampling and relational problems that appear to be intractable for classical computers.

Our first result says that, if there exists a polynomial-time classical algorithm that samples from the same probability distribution as our optical experiment, then P^#P=BPP^NP, and hence the polynomial hierarchy collapses to the third level. Unfortunately, this assumes an extremely reliable experiment. While that could in principle be arranged using quantum error correction, the question arises of whether a noisy experiment would already have interesting complexity consequences.

To address this question, we formulate a so-called "Permanent-of-Gaussians Conjecture" (PGC), which says that it is #P-hard to approximate the permanent of a matrix A of independent N(0,1) Gaussian entries, with high probability over A; as well as a "Permanent Anti-Concentration Conjecture" (PACC), which says that |Per(A)|>=sqrt(n!)/poly(n) with high probability over A. We then show that, assuming both the PGC and the PACC, polynomial-time classical simulation even of noisy linear-optics experiments would imply a collapse of the polynomial hierarchy.

Joint work with Alex Arkhipov

(Note: The ideas have been fleshed out enormously since my first talk

about this at Oberwolfach.)

P. Beame *Making RAMs Oblivious Requires Superlogarithmic Overhead*

We prove a time-space tradeoff lower bound of T=Omega(n log(n/S) loglog(n/S)) for randomized oblivious branching programs to compute 1GAP, also known as the pointer jumping problem, a problem for which there is a simple deterministic time n and space O(log n) RAM (random access machine) algorithm.

In a recent STOC paper, Ajtai derived simulations of general RAMs by randomized oblivious RAMs with only a polylogarithmic factor increase in time and space. Our lower bound implies that a superlogarithmic factor increase is indeed necessary in any such simulation.

Joint work with Widad Machmouchi.

M. Braverman *Compression, information and direct sum for communication complexity*

We will present a tight three-way connection between three types of results related to the randomized two-party communication complexity of a problem:

(1) Direct sum theorems, relating the communication complexity of computing many copies of a function to the complexity of computing one copy;

(2) The information complexity of a problem, which is the smallest amount of information (as opposed to communication) the parties need to exchange to solve the problem; and

(3) Compression theorems, which show how to convert two party communication protocols closer to the information-theoretically optimal bounds.

We will then use these connections along with new compression schemes to derive new results in communication complexity.

Based on two joint works, one with [Boaz Barak, Xi Chen, and Anup Rao], and the second one with [Anup Rao].

Z. Dvir *On matrix rigidity and locally self-correctable codes*

We describe a new approach for the problem of finding rigid matrices, as posed by Valiant [Val77], by connecting it to the, seemingly unrelated, problem of proving lower bounds for locally self-correctable codes. This approach, if successful, could lead to a non-natural property (in the sense of Razborov and Rudich [RR97]) implying super-linear lower bounds for linear functions in the model of logarithmic-depth arithmetic circuits.

Our results are based on a lemma saying that, if the generating matrix of a locally decodable code is not rigid, then it defines a locally self-correctable code with rate close to one. Thus, showing that such codes cannot exist will prove that the generating matrix of any locally decodable code (and in particular Reed Muller codes) is rigid.

V. Guruswami *List decodability of random linear codes*

For every fixed finite field F_q, $0 < p < 1-1/q$, and $\text{epsilon} > 0$, we prove that with high probability a random subspace C of F_q^n of dimension $(1-h_q(p)-\text{epsilon})n$ has the property that every Hamming ball of radius pn has at most $O(1/\text{epsilon})$ elements of C. (Here $h_q(x)$ is the q-ary entropy function.)

This answers a basic open question concerning the list-decodability of linear codes, showing that a list size of $O(1/\text{epsilon})$ suffices to have rate within epsilon of the information-theoretic limit $1-h_q(p)$. This matches up to constant factors the list-size achieved by general (non-linear) random codes, and gives an exponential improvement over the best previously known list-size bound of $q^{O(1/\text{epsilon})}$.

The main technical ingredient in our proof is a strong upper bound on the probability that m random vectors chosen from a Hamming ball centered at the origin have too many (more than O(m)) vectors from their linear span also belong to the ball.

The talk will be self-contained and not assume any coding theory background.

Joint work with Johan Hastad (KTH) and Swastik Kopparty (MIT).

G. Kindler *A Quantitative Proof of the Gibbard-Satterthwaite Theorem*

A social choice function f with n voters and q alternatives, takes as input a tuple of n full rankinds of the alternatives, supposedly corresponding to the preferences of the voters, and outputs the winner alternative. We say that f is manipulable at a given voting profile if a voter who knows the rankings given by the others can change her own ranking in a way that does not reflect her true preferences, but which leads to a winner that is more favorable to her.

Gibbard and Satterthwaite proved that any social choice function which attains three or more values, and which is not a dictatorship, must be manipulable. We show a quantitative version of the theorem in the case where f is neutral, showing that f must be manipulable at a uniformly chosen voting profile with probability bounded below by (the inverse of) a polynomial in n and q. Our results also imply that manipulations cannot be completely hidden by making them computationally hard to find: a voter can randomly try different permutations and find a useful manipulation with non-negligible probability.

Out results extend those of Friedgut, Kalai and Nisan, which worked only for the case of 3 alternatives. The methods we use are quite different though, using a canonical-paths style geometric argument.

A. Klivans *An Invariance Principle for Polytopes*

Let X be randomly chosen from {-1,1}^n, and let Y be randomly chosen from a standard n-variate Gaussian. For any polytope P formed by the intersection of k halfspaces, we prove that | Pr [X \in P] - Pr [Y \in P] | \leq polylog(k) * \Delta, where \Delta is a parameter that is small for polytopes formed by the intersection of ``regular'' halfspaces (i.e., halfspaces with low influence). The novelty of our invariance principle is the polylogarithmic dependence on k. Previously, only bounds that were at least linear in k were known.

We give two important applications of our main result:

1) A bound of polylog(k) * \eps^{O(1)} on the noise sensitivity of intersections of k regular halfspaces (previous work gave bounds linear in k). This gives the first quasipolynomial-time algorithm for learning intersections of regular halfspaces.

2) The first pseudorandom generators (with polylogarithmic seed length) for regular polytopes. This gives an algorithm for approximately counting the number of solutions to a broad class of integer programs (including dense covering programs and contingency tables).

This is joint work with Prahladh Harsha and Raghu Meka.

S. Lovett *Pseudorandom generators for CC0[p] and the Fourier spectrum of low-degree polynomials over finite fields*

In this paper we give the first construction of a pseudorandom generator with seed length O(log n), for CC0[p], the class of constant-depth circuits with unbounded fan-in MODp gates, for some prime p. More accurately, the seed length of our generator is O(log n) for any constant error epsilon>0. In fact, we obtain our generator by fooling distributions generated by low degree polynomials, over Fp, when evaluated on the Boolean cube. This result significantly extends previous constructions that either required a long seed [LVW93] or that could only fool the distribution generated by linear functions over Fp, when evaluated on the Boolean cube [LRTV09, MZ09].

Enroute of constructing our PRG, we prove two structural results for low degree polynomials over finite fields that can be of independent interest:

1. Let f be an n-variate degree d polynomial over Fp. Then, for every epsilon>0 there exists a subset S of variables of size depending only on d and epsilon, such that the total weight of the Fourier coefficients that do not involve any variable from S is at most epsilon.

2. Let f be an n-variate degree d polynomial over Fp. If the distribution of f when applied to uniform zero-one bits is epsilon-far (in statistical distance) from its distribution when applied to biased bits, then for every delta>0, f can be approximated over zero-one bits, up to error delta, by a function of a small number (depending only on epsilon, delta and d) of lower degree polynomials.

Joint work with Partha Mukhopadhyay and Amir Shpilka.

D. van Melkebeek *Satisfiability Allows No Nontrivial Sparsification Unless The Polynomial-Time Hierarchy Collapses*

Consider the following two-player communication process to decide a language L: The first player holds the entire input x but is polynomially bounded; the second player is computationally unbounded but does not know any part of x; their goal is to cooperatively decide whether x belongs to L at small cost, where the cost measure is the number of bits of communication from the first player to the second player.

For any integer d>=3 and positive real epsilon we show that if satisfiability for n-variable d-CNF formulas has a protocol of cost O(n^{d-epsilon}) then coNP is in NP/poly, which implies that the polynomial-time hierarchy collapses to the third level. The result even holds for conondeterministic protocols, and is tight as there exists a trivial deterministic protocol for epsilon = 0. Under the

hypothesis that coNP is not in NP/poly, our result implies tight lower bounds for parameters of interest in several areas, including sparsification, probabilistically checkable proofs, instance compression, and kernelization in parameterized complexity.

By reduction similar results holds for other NP-complete problems. For the vertex-cover problem on n-vertex d-regular hypergraphs the above statement holds for any integer d>=2. The case d=2 implies that no nontrivial parameterized vertex deletion problem on standard graphs can have kernels consisting of O(k^{2-epsilon}) edges unless coNP is in NP/poly. Kernels consisting of O(k^2) edges are known for several problems in the class, including vertex cover, bounded-degree deletion, and feedback vertex set.

Our approach refines the framework developed in recent papers showing that certain parameterized languages do not have protocols of cost bounded by any polynomial in the parameter unless coNP is in NP/poly. We study parameterized problems that do have protocols of polynomial cost, and show that no polynomial cost of lower degree than the current best is achievable unless coNP is in NP/poly. In order to obtain our tight bounds we exploit a result from additive combinatorics, namely the existence of high-density subsets of the integers without nontrivial arithmetic progressions of length three.

Joint work with Holger Dell.

D. Moshkovitz *Hardness of Approximately Solving Linear Equations Over Reals*

We consider the problem of approximately solving a system of homogeneous linear equations over reals, where each equation contains at most three variables.

Since the all-zero assignment always satisfies all the equations exactly, we restrict the assignments to be ``non-trivial". Here is an informal statement of our result: it is NP-hard to distinguish whether there is a non-trivial assignment that satisfies 1-\delta fraction of the equations or every non-trivial assignment fails to satisfy a constant fraction of the equations with a ``margin" of \Omega(\sqrt{\delta}).

Unlike the well-studied case of linear equations over finite fields, for equations over reals, the best approximation algorithm known (SDP-based) is the same no matter whether the number of variables per equation is two or three.

Our result is motivated by the following potential approach to proving The Unique Games Conjecture:

1. Prove the NP-hardness of solving approximate linear equations over reals, for the case of three variables per equation (we prove this result).

2. Prove the NP-hardness of the problem for the case of two variables per equation, possibly via a

reduction from the three variable case.

3. Prove the Unique Games Conjecture.

An interesting feature of our result is that it shows NP-hardness result that matches the performance of a non-trivial SDP-algorithm. Indeed, the Unique Games Conjecture predicts that an SDP-based algorithm is optimal for a huge class of problems (e.g. all CSPs by Raghavendra's result).

Joint work with Subhash Khot

P. Pudlak *Pseudorandom Generators for Group Products*

We will show that the pseudorandom generator introduced in \cite{INW94} fools group products of a given finite group. The seed length is $O(\log n\log\frac 1{\epsilon})$, where n the length of the word and ϵ is the precision. The result is equivalent to the statement that the pseudorandom generator fools read-once permutation branching programs of constant width.

Joint work with Michal Koucky and Prajakta Nimbhorkar.

A. Rao *Recovering from Maximal Errors in Interactive Communication*

We show that it is possible to encode any communication protocol between two parties so that the protocol succeeds even if a (1/4 - \epsilon) fraction of all symbols transmitted by the parties are corrupted adversarially, at a cost of increasing the communication in the protocol by a constant factor (the constant depends on epsilon). No encoding can tolerate a 1/4 fraction of errors in the interactive setting, if the communication is to remain bounded in terms of the original communication of the protocol. This improves on an earlier result of Schulman, who showed how to recover when the fraction of errors is at most 1/240.

Joint work with M. Braverman

P. Raghavendra *Approximating Graph Expansion: Connections, Algorithms and Reductions*

Approximating edge expansion, equivalently finding sparse cuts in graphs is a fundamental problem in combinatorial optimization that has received considerable attention in both theory and practice. Yet, the complexity of approximating edge expansion in graphs is poorly understood.

Particularly, worse is the understanding of the approximability of the expansion of small sets in graphs. More formally, current algorithmic or hardness results do not settle the approximability of the following problem: Given a regular graph G and a very small constant c, find a set S of cn vertices in the graph such that minimum number of edges cross the set S.

Recently it was shown that the complexity of this problem is closely tied to the Unique Games Conjecture. Furthermore, we show that the hardness of this problem is a natural assumption that generalizes the unique games conjecture, and yields hardness for problems like Balanced Separator and Minimum Linear arrangement.

O. Regev *Tight Bound for the Gap Hamming Distance Problem*

We consider the Gap Hamming Distance problem in communication complexity. Here, Alice receives an n-bit string x, and Bob receives an n-bit string y. They are promised that the Hamming distance between x and y is either at least $n/2+\sqrt{n}$ or at most $n/2-\sqrt{n}$, and their goal is to decide which is the case.

The naive protocol requires n bits of communication and it was an open question whether this is optimal. This was shown in several special cases, e.g., when the communication is deterministic [Woodruff'07] or when the number of rounds of communication is limited [Indyk-Woodruff'03, Jayram-Kumar-Sivakumar'07, Brody-Chakrabarti'09, Brody-Chakrabarti-R-Vidick-deWolf'09].

Here we settle this question by showing a tight lower bound of \Omega(n) on the randomized communication complexity of the problem. The bound is based on a new geometric statement regarding correlations in Gaussian space, related to a result of C. Borell from 1985, which is proven using properties of projections of sets in Gaussian space.
Partly based on a joint paper with Amit Chakrabarti.

R. Santhanam *New and Improved Upper Bounds for Formula Satisfiability and TQBF*

I will describe what appears to be a new technique for bounding the running time of algorithms for satisfiability, based on proving concentration versions of results about random restrictions. I will show how this gives a running time upper bound of 2^{n - \Omega(n)} for a simple and natural algorithm for formula satisfiability on formulae of linear length, and explain how the technique also gives a strong average-case lower bound for Parity against linear-size formulae. I will pose some questions relevant to extending this line of research to satisfiability and lower bounds for polynomial-size constant-depth circuits. If time permits, I will also mention a memoization-based technique that beats brute force search for QBF satisfiability on formulae with a bounded number of variable occurrences.

A. Sherstov *Symmetrization Without Symmetries*

We prove that the intersection of two halfspaces on the n-cube cannot be sign-represented by a polynomial of degree less than Theta(n), which matches the trivial upper bound and solves an open problem due to Klivans (2002). This result shows that intersections of halfspaces are not amenable to learning by perceptron-based techniques, which have been successful in other cases (halfspaces, DNF formulas, read-once formulas). A mostly complete proof will be presented with emphasis on a key technical component, a method for symmetrizing a Boolean function f without any symmetries by averaging f over suitable sections over the n-cube.

D. Steurer *Subexponential Algorithms for Unique Games and Related Problems*

We give a subexponential time approximation algorithm for the Unique Games problem: Given a Unique Games instance with optimal value 1-epsilon^6 and alphabet size k, our algorithm finds in time exp(k*n^epsilon) a solution of value 1-epsilon.

We also obtain subexponential algorithms with similar approximation guarantees for Small-Set Expansion and Multi Cut. For Max Cut, Sparsest Cut and Vertex Cover, our techniques lead to subexponential algorithms with improved approximation guarantees on subclasses of instances.

Khot's Unique Games Conjecture (UGC) states that it is NP-hard to achieve approximation guarantees such as ours for Unique Games. While our result stops short of refuting the UGC, it does suggest that Unique Games is significantly easier than NP-hard problems such as Max 3-SAT, Label Cover and more, that are believed not to have subexponential algorithms achieving a non-trivial approximation ratio.

The main component in our algorithms is a new kind of graph decomposition that may have other applications: We show that by changing an epsilon fraction of its edges, any regular graph on n vertices can be broken into disjoint parts such that the stochastic adjacency matrix of each part has at most n^epsilon eigenvalues larger than 1-epsilon^6.

Joint work with Sanjeev Arora and Boaz Barak.

C. Umans *Pseudorandom generators and the BQP vs. PH problem*

It is a longstanding open problem to devise an oracle relative to which BQP does not lie in the Polynomial-Time Hierarchy (PH). We advance a natural conjecture about the capacity of the Nisan-Wigderson pseudorandom generator [NW94] to fool AC0, with MAJORITY as its hard function. Our conjecture is essentially that the loss due to the hybrid argument (which is a component of the standard proof from [NW94]) can be avoided in this setting. This is a question that has been asked previously in the pseudorandomness literature [BSW03]. We then show that our conjecture implies the existence of an oracle relative to which BQP is not in the PH. This entails giving an explicit construction of unitary matrices, realizable by small quantum circuits, whose row-supports are nearly-disjoint. Our framework generalizes the setting of [Aar09], and remains a viable approach to resolving the BQP vs. PH problem after the recent proof [Aar10] that the Generalized Linial-Nisan Conjecture of [Aar09] is false.

Joint work with Bill Fefferman.

L. Valiant *Holographic Algorithms*

First we briefly review some recent dichotomy results, including some that strictly generalize constraint satisfaction problems, that showcase the power of the holographic method.

We go on to define the notion of diversity for families of finite functions, and express the limitations of a class of holographic algorithms in terms of limitations on diversity. In particular, we show, by a new but very classical looking combination of counting and algebraic methods, that the class of elementary holographic algorithms, which has yielded novel polynomial time algorithms for such problems as special cases of Boolean Satisfiability, is insufficient for expressing general Boolean Satisfiability. We suggest that the question of how far this lower bound argument can be extended is of some general interest.

We go on to explore the power of nonelementary polynomial time holographic algorithms by describing such algorithms for certain parity problems for which no polynomial time algorithms were previously known. These algorithms compute the parity of the following quantities for degree three planar undirected graphs: the number of 3-colorings up to permutation of colors, the number of connected vertex covers, and the number of induced forests or feedback vertex sets. These holographic algorithms, besides being nonelementary, use bases of more than two components and thereby potentially evade the Cai-Lu Collapse Theorem.

E. Viola *The complexity of distributions*

Complexity theory typically studies the complexity of computing a function h(x) : {0,1}^m -> {0,1}^n of a given input x. We advocate the study of the complexity of generating the distribution h(x) for uniform x, given random bits.

We discuss recent work in this direction. This includes lower and upper bounds for various computational models (NC^0, decision trees, and AC^0) and the consequences of these bounds for succinct data structures and pseudorandom generators.

We expect the talk to be based on two papers "The complexity of distributions" and "Bounded-depth circuits cannot sample good codes," the latter co-authored with Shachar Lovett.

D. Wehr *A lower bound for a restricted model of log-space computation*

I'll show how to solve a problem posed in [Gal,Koucky,McKenzie "Incremental branching programs" 2006] regarding a restricted model of small-space computation, tailored for solving the P-complete GEN problem. They define two variants of incremental branching programs, the syntactic variant defined by a restriction on the graph-theoretic paths in the program, and the more-general semantic variant in which the same restriction is enforced only on the consistent paths (those that are followed by at least one input). They used a lower bound for monotone circuits to show that exponential size is required for the syntactic variant, but left open the problem of superpolynomial lower bounds for the semantic variant. I'll give the main part of the proof of an exponential lower bound for the semantic variant; it is a generalization of a lower bound argument for a similar restricted model of computation tailored for solving the Tree Evaluation Problem, which appeared in [Braverman, Cook, McKenzie, Santhanam, Wehr "Fractional pebbling and thrifty branching programs" 09].

A. Yehudayoff *Pseudorandom generators for regular branching programs*

We give new pseudorandom generators for \emph{regular} read-once branching programs of small width. A branching program is regular if the in-degree of every vertex in it is (0 or) 2. For every width d and length n, our pseudorandom generator uses a seed of length O((log(d) + loglog(n) + log(1/epsilon)) log(n)) to produce n bits that cannot be distinguished from a uniformly random string by any regular width d length n read-once branching program, except with probability epsilon.

We also give a result for general read-once branching programs, in the case that there are no vertices that are reached with small probability. We show that if a (possibly non-regular) branching program of length n and width d has the property that every vertex in the program is traversed with probability at least p on a uniformly random input, then the error of the generator above is at most 2 epsilon / p^2 .

Joint work with Mark Braverman, Anup Rao, and Ran Raz.

D. Zuckerman *Pseudorandom Generators for Polynomial Threshold Functions*

We study the natural question of constructing pseudorandom generators (PRGs) for low-degree polynomial threshold functions (PTFs). We give a PRG with seed-length log n/eps^{O(d)} fooling degree d PTFs with error at most eps. Previously, no nontrivial constructions were known even for quadratic threshold functions and constant error eps. For the class of degree 1 threshold functions or halfspaces, we construct PRGs with much better dependence on the error parameter eps and obtain the following results. 1) A PRG with seed length O(log n log(1/eps)) for eps > 1/poly(n). 2) A PRG with seed length O(log n) for eps > 1/poly(log n). Previously, only PRGs with seed length O(log n log^2(1/eps)/eps^2) were known for halfspaces. We also obtain PRGs with similar seed lengths for fooling halfspaces over the n-dimensional unit sphere. The main theme of our constructions and analysis is the use of invariance principles to construct pseudorandom generators. We also introduce the notion of monotone read-once branching programs, which is key to improving the dependence on the error rate eps for halfspaces. These techniques may be of independent interest.

Joint work with R. Meka.