COMPLEXITY ABSTRACTS 1999. Vol IX

Abstract

This is a collection of one page abstracts of recent results of interest to the Complexity community. The purpose of this document is to spread this information, not to judge the truth or interest of the results therein.

Titles of Abstracts

Connecting the Complexities of Approximating Clique and TSP
On the Complexity of Tensor Formulae
The Zero-One Law Holds for BPP
Streaming Algorithms for Distributed, Massive Data
Distributionally-Hard Languages
On the Quantum Complexity of Majority
Graph Nonisomorphism Has Subexponential Size Proofs
Derandomizing RP if Boolean Circuits are not learnable
The Boolean Hierarchy of NP-partitions
My Brain is Full: When More Memory Helps
Arithmetic Circuits and Polynomial Replacement Systems
A Lower Bound for the Shortest Path Problem
A note on the Isomorphism Conjecture and one-way
Kolmogorov Complexity-Based Ideas for
Logspace MOD classes with composite moduli
Lower Bounds for Space in Resolution
Sampling under adverse conditions

Connecting the Complexities of Approximating Clique and TSP

Richard Chang
Department of Computer Science and Electrical Engineering
University of Maryland Baltimore County
1000 Hilltop Circle
Baltimore, MD 21250, USA
Email: chang@umbc.edu

Abstract Number 99-1

This paper demonstrates a linkage between the complexity of finding approximate solutions to the MaxClique problem and that of the Traveling Salesman Problem (TSP). The main result of the paper is:

$$\text{MaxClique} \leq_{\text{m}}^{\text{P}} \text{2-approximating MaxClique} \Longrightarrow \text{TSP} \leq_{\text{m}}^{\text{P}} \text{2-approximating TSP}.$$

Previously, it was known that TSP $\leq_{\text{m}}^{\text{P}}$-reduces to $(1+n^{-\log n})$-approximating TSP under the same assumptions. The proof of the main result uses a characterization of the complexity of NP-approximation problems by nondeterministic bounded query classes. The class $\text{NPF}_b^{\text{SAT}[q(n)]}$ is the class of multi-valued functions computed by NP machines that have access to the NP-complete language SAT as an oracle. These NP machines are limited to $q(n)$ queries to the SAT oracle in the entire nondeterministic computation tree (not just a single computation path). Since finding approximate solutions to MaxClique and TSP are complete for various $\text{NPF}_b^{\text{SAT}[q(n)]}$ classes, proving the main result is equivalent to showing that

$$\text{NPF}_b^{\text{SAT}[O(\log n)]} = \text{NPF}_b^{\text{SAT}[\log\log n + O(1)]} \Longrightarrow \text{NPF}_b^{\text{SAT}[n^{O(1)}]} = \text{NPF}_b^{\text{SAT}[O(\log n)]}.$$

This improves upon the previously known result that

$$\text{NPF}_b^{\text{SAT}[O(\log n)]} = \text{NPF}_b^{\text{SAT}[\log\log n + O(1)]} \Longrightarrow \text{NPF}_b^{\text{SAT}[n^{O(1)}]} = \text{NPF}_b^{\text{SAT}[O(\log^2 n)]}.$$

A preliminary version of the paper is available at http://umbc.edu/~chang/papers/ or by email to chang@umbc.edu.

On the Complexity of Tensor Formulae

Carsten Damm, Fachbereich Informatik, Universität Trier, D-54286 Trier, Germany (damm@uni-trier.de)

Abstract Number 99-2

We consider matrix formulae on base of sum, product, and tensor product. In particular, we consider tensor formulae over the Boolean semi-ring $B = (\{0,1\}, AND, OR)$ and over the two-element field $F_2 = (\{0,1\}, +, \times)$.
The TENSOR FORMULA EVALUATION PROBLEM over a certain semi-ring $\mathcal{S}$ (denoted $TEP_{\mathcal{S}}$) is the set of tensor formulae that over $\mathcal{S}$ evaluate to 1. We prove: (1) TEP_B and TEP_{F_2}, respectively, are complete for NP and $\oplus P$, respectively, under polynomial time reductions. (2) When restricted to tensor formulae containing only small sub-formulae, these problems are complete for $LOGCFL$ and $\oplus LOGCFL$ under log-space reductions, respectively. Restriction to formulae without tensor products leads to problems that are complete for NL and $\oplus L$, respectively.
We demonstrate the strength of these characterizations by giving a unified proof for the inclusions

1. $NP/poly \subseteq \oplus P/poly$,
2. $LOGCFL/poly \subseteq \oplus LOGCFL/poly$, and
3. $NL/poly \subseteq \oplus L/poly$,

that were first proved using Valiant-Vazirani's Lemma and the Isolating Lemma of Vazirani, Vazirani, and Mulmuley. Our proof instead relies on randomized polynomial testing. In case of the latter two inclusions our proof uses less random bits than earlier constructions.

A paper is available by email to damm@uni-trier.de

The Zero-One Law Holds for BPP

Dieter van Melkebeek, Department of Computer Science, University of Chicago, 1100 East 58th Street, Chicago, IL 60637, USA. (dieter@cs.uchicago.edu)

Abstract Number 99-3

We show that BPP has resource-bounded measure zero in exponential time if and only if BPP differs from exponential time. This provides the first non-trivial example of a class for which Kolmogorov's zero-one law holds for resource-bounded measure: Either BPP has measure zero or it has measure one.

A preliminary version is available as technical report TR-98-07 from URL http://www.cs.uchicago.edu/publications/tech-reports.

Streaming Algorithms for Distributed, Massive Data Sets

Joan Feigenbaum, AT&T Labs – Research, 180 Park Avenue, Florham Park, NJ 07932 USA, (jf@research.att.com)
Sampath Kannan, Computer and Information Sciences, University of Pennsylvania, Philadelphia, PA 19104 USA, (kannan@central.cis.upenn.edu)
Martin Strauss, AT&T Labs – Research, 180 Park Avenue, Florham Park, NJ 07932 USA, (mstrauss@research.att.com)
Mahesh Viswanathan, Computer and Information Sciences, University of Pennsylvania, Philadelphia, PA 19104 USA, (maheshv@saul.cis.upenn.edu)

Abstract Number 99-4

Massive data sets are increasingly important in a wide range of applications, including observational sciences, product marketing, and monitoring and operations of large systems. In network operations, raw data typically arrive in *streams*, and decisions must be made by algorithms that make one pass over each stream, throw much of the raw data away, and produce "synopses" or "sketches" for further processing. Moreover, network-generated massive data sets are often *distributed*: Several different, physically separated network elements may receive or generate data streams that, together, comprise one logical data set; to be of use in operations, the streams must be analyzed locally and their synopses sent to a central operations facility. The enormous scale, distributed nature, and one-pass processing requirement on the data sets of interest must be addressed with new algorithmic techniques.

We present one fundamental new technique here: a space-efficient, one-pass algorithm for approximating the L^1 difference $\sum_i |a_i - b_i|$ between two functions, when the function values a_i and b_i are given as data streams, and their order is chosen by an adversary. Our main technical innovation, which may be of interest outside the realm of massive data stream algorithmics, is a method of constructing families $\{V_j\}$ of random variables such that most 4-tuples are independent and such that $\sum_{j=0}^{c-1} V_j(s)$ is computable in time $polylog(c)$, for all seeds s. Our L^1-difference algorithm can be viewed as a "sketching" algorithm, in the sense of [Broder, Charikar, Frieze, and Mitzenmacher, STOC '98, pp. 327-336], and our technique performs better than that of Broder *et al.* when used to approximate the symmetric difference of two sets with small symmetric difference.

A full paper is available by email to mstrauss@research.att.com.

Distributionally-Hard Languages

Lance Fortnow, Department of Computer Science, University of Chicago, 1100 East 58th Street, Chicago, IL 60637 (fortnow@cs.uchicago.edu)
A. Pavan, Department of Computer Science and Engineering, University at Buffalo, Buffalo, NY 14260 (aduri@cse.buffalo.edu)
Alan L. Selman, Department of Computer Science and Engineering, University at Buffalo, Buffalo, NY 14260 (selman@cse.buffalo.edu)

Abstract Number 99-5

Define a set L to be *distributionally-hard to recognize* if for every polynomial-time computable distribution μ with infinite support, L is not recognizable in polynomial time on the μ-average. Cai and Selman defined a modification of Levin's notion of average polynomial time and proved that every P-bi-immune language is distributionally-hard. Pavan and Selman proved that there exist distributionally-hard sets that are not P-bi-immune if and only P contains P-printable-immune sets. We extend this characterizion to include assertions about several traditional questions about immunity, about finding witnesses for NP-machines, and about existence of one-way functions. Similarly, we address the question of whether NP contains sets that are distributionally hard. Several of our results are implications for which we cannot prove whether or not their converse holds. In nearly all such cases we provide oracles relative to which the converse fails. The central theorem is that the following assertions are equivalent:

1. There exists a distributionally-hard set that is not P-bi-immune.
2. There exists a P-printable-bi-immune set that is not P-bi-immune.
3. P contains a P-printable-immune set.
4. NP contains a P-printable-immune set.
5. There is an infinite set S in NE and an NE-machine M that accepts S such that no E-machine correctly computes infinitely many accepting computations of M.
6. There is an infinite tally language L in NP and an NP-machine M that accepts L such that no P-machine correctly computes infinitely many accepting computations of M.
7. There is an infinite set S in NP and an NP-machine M that accepts S such that no P-machine computes infinitely many accepting computations of M.
8. Almost-always one-way functions exist.

A full paper will be available at http://www.ncstrl.org.

On the Quantum Complexity of Majority

Thomas Hayes, Department of Computer Science, University of Chicago, 1100 East 58th Street, Chicago, IL 60637, USA, (hayest@cs.uchicago.edu)
Samuel Kutin, Department of Computer Science, University of Chicago, 1100 East 58th Street, Chicago, IL 60637, USA, (kutin@cs.uchicago.edu)
Dieter van Melkebeek, Department of Computer Science, University of Chicago, 1100 East 58th Street, Chicago, IL 60637, USA. (dieter@cs.uchicago.edu)

Abstract Number 99-6

We construct a quantum black-box algorithm that computes the majority of N bits exactly using $N + 1 - w(N)$ queries, where $w(N)$ denotes the number of ones in the binary expansion of N. We establish a matching lower bound in a generalized classical decision tree model in which the equivalent of our quantum algorithm is optimal. We also provide an exact quantum algorithm that almost surely makes no more than $\frac{N}{\sqrt{2}} + O((N \log N)^{\frac{2}{3}})$ queries.

A preliminary version is available as technical report TR-98-11 from URL http://www.cs.uchicago.edu/publications/tech-reports.

Graph Nonisomorphism Has Subexponential Size Proofs Unless The Polynomial-Time Hierarchy Collapses

Adam Klivans, Department of Mathematics, MIT, Cambridge, MA 02139, USA, (klivans@math.mit.edu)
Dieter van Melkebeek, Department of Computer Science, University of Chicago, 1100 East 58th Street, Chicago, IL 60637, USA. (dieter@cs.uchicago.edu)

Abstract Number 99-7

We establish hardness versus randomness trade-offs for a broad class of randomized procedures. In particular, we create efficient nondeterministic simulations of bounded round Arthur-Merlin games using a language in exponential time that cannot be decided by polynomial size oracle circuits with access to satisfiability. We show that every language with a bounded round Arthur-Merlin game has subexponential size membership proofs for infinitely many input lengths unless exponential time coincides with the third level of the polynomial-time hierarchy (and hence the polynomial-time hierarchy collapses). This provides the first strong evidence that graph nonisomorphism has subexponential size proofs.

We set up a general framework for derandomization which encompasses more than the traditional model of randomized computation. For a randomized procedure to fit within this framework, we only require that for any fixed input the complexity of checking whether the procedure succeeds on a given random bit sequence is not too high. We then apply our derandomization technique to the following complexity theoretic constructions, assuming in each case a sufficiently strong worst-case hardness condition:

- The Valiant-Vazirani random hashing technique which prunes the number of satisfying assignments of a Boolean formula to one, and related procedures like computing satisfying assignments to Boolean formulas *non-adaptively* given access to an oracle for satisfiability.
- The algorithm of Bshouty et al. for learning Boolean circuits.
- Constructing matrices with high rigidity.
- Constructing polynomial-size universal traversal sequences.

We also show that if linear space requires exponential size circuits, then space bounded randomized computations can be simulated deterministically with only a constant factor overhead in space.

A full version is available as technical report TR-98-12 from URL http://www.cs.uchicago.edu/publications/tech-reports.

Derandomizing RP if Boolean Circuits are not learnable

Johannes Köbler, Wolfgang Lindner, Rainer Schuler, Abt. Theoretische Informatik, Universität Ulm, 89081 Ulm, Germany (lindner@informatik.uni-ulm.de)

Abstract Number 99-8

We show that every language in RP has subexponential-time approximations for infinitely many input lengths if Boolean Circuits are not polynomial-time pac-learnable with membership queries under the uniform distribution.
We also consider the weak model of learning as introduced by Kearns and Valiant. As an intermediate step towards the derandomization of RP, we show that with respect to the uniform distribution, weak and strong learning of boolean circuits are equivalent. Recall that unlike in the distribution independent model, a weak learning algorithm that is successful on a specific distribution does not necessarily imply the existence of a strong learning algorithm that is successful on the same distribution.

A full paper is available by email to lindner@informatik.uni-ulm.de. (See also http://theorie.informatik.uni-ulm.de/papers/)

The Boolean Hierarchy of NP-partitions

Sven Kosub and Klaus W. Wagner, Lehrstuhl für Theoretische Informatik, Julius-Maximilians-Universität Würzburg, Am Exerzierplatz 3, D-97072 Würzburg, GERMANY. ({kosub, wagner}@informatik.uni-wuerzburg.de)

Abstract Number 99-9

Classical computational complexity theory is primarely investigating the complexity of sets, i.e., the complexity of partitioning a basic set into two parts. By this work, a (first?) step is made towards the study of computational complexity of partitioning a ground set into k parts. For that, the definition of the classes of the boolean hierarchy of sets is generalized in the way that to any function $f : \{0,1\}^m \to \{1,2,\ldots,k\}$, a class
$\mathrm{NP}(f)$ of k-partitions is associated. While in the classical case ($k = 2$) each such class coincides with one of well-known classes $\mathrm{NP}(n)$ or $\mathrm{coNP}(n)$, in the case of $k \geq 3$ the situation is much more complicated.
It is given a sufficient criterion for the truth of the inclusion $\mathrm{NP}(f) \subseteq \mathrm{NP}(g)$ when functions $f, g : \{0,1\}^m \to \{1,2,\ldots,k\}$ are considered, and it is conjectured that this criterion is also necessary (assuming the polynomial hierarchy does not collapse to any level). In order to prove the underlying equivalence which is called *Embedding Conjecture*, we examine the emerging hierarchy of partition classes over NP. To this purpose, technical tools are developed in terms of alternative characterizations of such classes by means of finite labeled lattices and inclusion-preserving relations between them.

A full paper is soon available by email to kosub@informatik.uni-wuerzburg.de.

My Brain is Full: When More Memory Helps

Christopher Lusena, Computer Science Dept., University of Kentucky, Lexington, Kentucky, 40506, USA, (lusena@cs.uky.edu)
Tong Li, Computer Science Dept., University of Kentucky, Lexington, Kentucky, 40506, USA, (tongli@cs.uky.edu)
Shelia Sittinger, Computer Science Dept., University of Kentucky, Lexington, Kentucky, 40506, USA, (smsitt0@cs.uky.edu)
Chris Wells, Computer Science Dept., University of Kentucky, Lexington, Kentucky, 40506, USA, (chrisw@cs.uky.edu)
Judy Goldsmith, Computer Science Dept., University of Kentucky, Lexington, Kentucky, 40506, USA, (goldsmit@cs.uky.edu)

Abstract Number 99-10

We consider the problem of finding good finite-horizon policies for POMDPs under the expected reward metric. The policies considered are free finite-memory policies with limited memory; a policy is a mapping from the space of action-memory pairs to the space of action-memory pairs (the policy updates the memory as it goes), and the number of possible memory states is a parameter of the input to the policy-finding algorithms. The algorithms considered here are search heuristics: local search, simulated annealing, and genetic algorithms. We compare their outcomes to each other and to the optimal policies for each instance. We compare run times of each policy and of a dynamic programming algorithm for POMDPs developed by Hansen that iteratively improves a finite-state controller — the previous state of the art for finite memory policies. The value of the best policy can only improve as the amount of memory increases, up to the amount needed for an optimal finite-memory policy. Our most surprising finding is that more memory helps in another way: *given more memory than is needed for an optimal policy, the algorithms are more likely to converge to optimal-valued policies.*

To appear in the fifteenth conference on Uncertainty in Artificial Intelligence (1999). A full paper is available by email from lusena@cs.uky.edu .

Arithmetic Circuits and Polynomial Replacement Systems

Pierre McKenzie, Informatique et recherche opérationnelle, Université de Montréal, C.P. 6128, Succ. Centre-Ville, Montréal (Québec), H3C 3J7 Canada,
(mckenzie@iro.umontreal.ca),
Heribert Vollmer and Klaus W. Wagner, Theoretische Informatik, Universität Würzburg, Am Exerzierplatz 3, 97072 Würzburg, Germany,
((vollmer|wagner)@informatik.uni-wuerzburg.de).

Abstract Number 99-11

This paper addresses the problems of counting proof trees (as introduced by Venkateswaran and Tompa) and counting proof circuits, a related but seemingly more natural question. These problems lead to a common generalization of straight-line programs which we call polynomial replacement systems. We contribute a classification of these systems and we investigate their complexity. Diverse problems falling in the scope of this study include, for example, counting proof circuits, and evaluating $\{\cup, +\}$-circuits over the natural numbers. The former is shown #P-complete, the latter PSPACE-complete, and other complexity results are obtained.

A full paper is available by email to vollmer@informatik.uni-wuerzburg.de.

A Lower Bound for the Shortest Path Problem

Ketan Mulmuley, Department of Computer Science, University of Chicago, 1100 East 58th Street, Chicago, IL 60637 (mulmuley@cs.uchicago.edu)
Pradyut Shah, Department of Computer Science, University of Chicago, 1100 East 58th Street, Chicago, IL 60637 (pradyut@cs.uchicago.edu)

Abstract Number 99-12

We show that the SHORTEST PATHS PROBLEM cannot be solved in $o(\log n)$ time on an unbounded fan-in PRAM without bit operations using poly(n) processors even when the bit-lengths of the weights on the edges are restricted to be of size $O(\log^3 n)$. This shows that the matrix-based *repeated squaring* algorithm for the SHORTEST PATHS PROBLEM is optimal in the unbounded fan-in PRAM model without bit operations.

A full paper is available at http://www.cs.uchicago.edu/~pradyut/papers/path.ps.

A note on the Isomorphism Conjecture and one-way functions

John D. Rogers, School of CTI, DePaul University, 243 S. Wabash, Chicago IL 60604 (jrogers@cs.depaul.edu)

Abstract Number 99-13

Fenner, Fortnow, and Kurtz [FFK92] created an oracle relative to which the Isomorphism Conjecture (IC) is true. Rogers [Rogers95] used this oracle to create one relative to which the IC is true and one-way functions exist. These oracles arise from difficult and technical constructions.

In 1997, Beigel, Buhrman, and Fortnow [BBF97] found a much simpler oracle relative to which the IC is true. Using this oracle and the techniques developed in [Rogers95], we demonstrate the existence of a simple oracle relative to which the IC is true but one-way functions exist.

A full paper is available from http://www.depaul.edu/~jrogers/.

Kolmogorov Complexity-Based Ideas for Locating Text in Web Images

Martin Schmidt, Vladik Kreinovich, and Luc Longpré,
Department of Computer Science, University of Texas at El Paso, El Paso, TX 79968, USA ({mschmidt,vladik,longpre}@cs.utep.edu)

Abstract Number 99-14

Practical problem. The gaining popularity of the World Wide Web also means increasing security risks. While numerous web search tools can be used to automatically monitor plain text in web pages, search for text in graphical images is still a considerable challenge.

Idea. An image is, typically, more complicated (= more difficult to compress) than plain text. Therefore, such an image in which several pixels are replaced by text has a smaller Kolmogorov complexity $K(x)$ than the original image. So, if we start with an image which is "uniformly complex" in the sense that every part of the image has "similar" complexity, and we replace a piece of this image by text, then we can, in principle, detect where exactly this text is – because a part x' with a text t will have smaller complexity than a part x'' of same size but without the text: $K(x') < K(x'')$. The larger t, the smaller $K(x')$; so, by the value of $K(x')$, we can determine the size of the intersection $t \cap x'$. In other words, if we can use Kolmogorov complexity as an oracle, we have the following problem:

Algorithmic problem. We have: a *string* $I : \{1, \ldots, n\} (= N_n) \to \mathcal{A}$ (for some alphabet $\mathcal{A}$) in which an (unknown) subset $T \subseteq N_n$ of size L is pre-selected, and an *oracle* which, given a subset $S \subseteq N_n$, returns the number of elements in the intersection $S \cap T$. How can we use this oracle to locate T?

1D solution. In a 1D image, a "text" T is a substring of L consecutive pixels. There are $n - L$ possible locations of T. Our first result is that *for $L > 1$, we can locate T in $O(\log(n))$ oracle calls.*

2D solution. If a text is linearly aligned in a 2D image, and we store pixels row-by-row, the text's letter locations T form an arithmetic progression $a + bi$, $1 \le i \le L$, with unknown a and b. In this case, *we can locate T (i.e., find a and b) with $O(\log(n))$ calls to an oracle.*

Approximate oracles. Kolmogorov complexity $K(x)$ is not computable, so we must use a computable approximation to $K(x)$ instead. As a result, instead of the exact number of elements in $T \cap S$, we get an approximation to this number. We analyze the computational complexity of locating T for the situation when we only have an approximate oracle.

Open problem: Our algorithms work on "uniformly complex" images. We started to look for a characterization of a class of images for which such an algorithm can work.

This research was supported by the National Security Agency Grant MDA904-98-1-0564. A full paper will be available shortly.

Logspace MOD classes with composite moduli

Robert Szelepcsényi, The University of Chicago, Department of Computer Science, 1100 East 58-th Street, Chicago, IL 60637, (robert@cs.uchicago.edu)

Abstract Number 99-15

We continue the study of logspace MOD classes introduced by Buntrock, Damm, Hertrampf and Meinel who proved that MOD_kL classes are closed under NC_1 reductions when k is a prime (power of prime) and showed that all the standard problems of linear algebra over finite fields Z_k are complete for MOD_kL under logspace reductions. Closely related work was later done by Allender, Beals and Ogihara who introduced and investigated the exact counting logspace class $C_=L$. They proved that $NC_1(C_=L) = L(C_=L)$ and characterised the complexity of many standard problems of linear algebra over Z in terms of $C_=L$.

We extend the study of logspace MOD classes with composite moduli. Buntrock et al showed that MOD_kL is closed under union for arbitrary $k \geq 2$. We prove that MOD_kL is also closed under disjunctive truthtable reductions. Moreover, we show that closure of MOD_kL under complement, intersection and conjunctive truth table reductions are equivalent.

Next we evaluate the power of circuit reductions to MOD_kL. We adapt methods by Allender et al. developed for class $C_=L$. $AC^0(MOD_kL)$ turns out to capture the oracle tape hierarchy based on MOD_kL in the same way as in the case of $C_=L$ and many other logspace classes. We provide a uniform proof that $NC_1(MOD_kL) = L(MOD_kL)$ for arbitrary moduli $k \geq 2$. This implies that the oracle hierarchy based on MOD_kL collapses down to $L(MOD_kL)$.

All these results allows us to conclude that MOD_kL as defined by Buntrock et al. is closed under NC^1 reductions iff it is closed under all other operations under consideration, i.e. AC^0 reductions, logspace truth-table reductions, complement, conjunctive truth-table reductions and intersection. The oracle hierarchy based on MOD_kL collapses down to MOD_kL iff MOD_kL is closed under any of these operations.

Similarly to previous work done for prime moduli and $C_=L$ we also seek to classify the complexity of important problems of linear algebra over finite rings. Buntrock et al. already showed that several important problems of linear algebra over finite rings Z_k are complete for $\overline{MOD_kL}$. These include inversion of matrices, powering of matrices, computation of characteristic polynomials. Newly proven closure properties allow us to use methods by Allender et al. to classify the complexity of additional problems. The problem of verifying whether the rank of a matrix is smaller than a given value is complete for $\overline{MOD_kL}$ and the problem of verifying whether the rank of a matrix is equal to a given value is complete for $MOD_kL \cap \overline{MOD_kL}$ under logspace reductions.

A preliminary version of the paper is available at http://www.cs.uchicago.edu/ robert

Lower Bounds for Space in Resolution

Jacobo Torán, Abt. Theoretische Informatik, Universität Ulm, Oberer Esselsberg, 89069 Ulm, GERMANY, (toran@informatik.uni-ulm.de)

Abstract Number 99-16

Resolution space measures the maximum number of clauses that need to be simultaneously active in a resolution refutation. This complexity measure was defined by Kleine Büning and Lettmann and slightly modified recently to make it suitable for comparisons with other measures. Since its definition, only trivial lower bound for the resolution space, measured in terms of the number of initial clauses were known. In this paper we prove optimal lower bounds for the space needed in the resolution refutation of two important families of formulas. We show that Tseitin formulas associated to expander graphs of n nodes need resolution space $n-1$. Measured on the number of clauses, this result is best possible since the mentioned formulas have $O(n)$ clauses, and the number of clauses is an upper bound for the resolution space. We also show that the formulas expressing the general Pigeonhole Principle with n holes and more than n pigeons, need space $n+1$ independently of the number of pigeons. Since a matching space upper bound of $n+1$ for these formulas exist, the obtained bound is exact. These results point to a connection between resolution space and resolution width, another measure for the complexity of resolution refutations.

A full paper is available by email to toran@informatik.uni-ulm.de

Sampling under adverse conditions

Marius Zimand, School of Computer and Information Science, Georgia Southwestern State University, Americus, GA 31709 , (zimand@canes.gsw.edu)

Abstract Number 99-17

Sampling can be viewed as a game in which one player, the adversary, chooses a function f defined on a large domain, say $\{0,1\}^m$, and the other player, the sampler, chooses D random points in the domain. In the traditional setting, the adversary moves first, the sampler moves second, and the sampler wins the (γ, ϵ)-game if with probability at least $1-\gamma$ on the choice of the sample points, the sample average is within ϵ from the real average of f. We show that even if the order of the moves is inversed, the sampler can still win the game with $D = poly(m)$, $\epsilon = 1/poly(m)$, and $\gamma = 1/poly(m)$, provided that the adversary is restricted to choose a function f computable by a polynomial-size circuit.

The paper is available from http://www.gsw.edu/~mzimand.