

Report on the Dagstuhl-Seminar

“Structure and Complexity”

Organizers:

Eric Allender (Rutgers University)

Uwe Schöning (Universität Ulm)

Klaus W. Wagner (Universität Würzburg)

September 30—October 4, 1996

The seminar “Structure and Complexity” was the third Dagstuhl Seminar devoted to the structural aspects of Computational Complexity Theory. It was attended by 40 scientists who in 27 talks presented new results in this field. The following topics were among the main subjects covered by the talks: Kolmogorov complexity, isomorphism theory, resource-bounded measures, relativizations, randomness, leaf language characterizations, circuit theory, logical characterizations of complexity classes, interactive proof systems, one-way functions, and computational models.

PROGRAM

Farid Ablayev

On the Power of Randomized Branching Programs

Eric Allender

Recent Progress on the Isomorphism Conjecture

José L. Balcázar

Kolmogorov-Easy Circuit Expressions

Bernd Borchert

Looking for an Analogue of Rice's Theorem in Complexity Theory

Harry Buhrman

Six Hypotheses

Stephen Fenner

A Variant of Immunity, Btt-Reductions, and Minimal Programs

Lance Fortnow

Two Queries

Judy Goldsmith

The Complexity of Deterministically Observable Finite-Horizon Markov Decision Processes

Montserrat Hermo

Compressibility of Infinite Binary Sequences

Ulrich Hertrampf

The Shapes of Trees

Klaus-Jörn Lange

Mangrove Deforestation: Algorithms for Unambiguous Logspace Classes

Jack H. Lutz

Equivalence of Measures of Complexity Classes

Pierre McKenzie

Nondeterministic NC¹ Computation

Rüdiger Reischuk

Interactive Proofs with Public Coins and Small Space Bounds

Jörg Rothe

Characterizations of the Existence of Partial and Total One-Way Permutations

James Royer

Complexity at Higher Types

Miklos Santha

A Decision Procedure for Unitary Linear Quantum Cellular Automata

Rainer Schuler

Is Testing More Complex Than Querying?

Thomas Schwentick

Algebraic and Logical Characterizations of Deterministic Linear Time Classes

Martin Strauss

An Information-Theoretic Treatment of Random-Self-Reducibility

Denis Thérien

The Crane Beach Conjecture

Thomas Thierauf

The Isomorphism Problem for One-Time-Only Branching Programs and Arithmetic Circuits

Nicolai Vereshchagin

Boolean Decision Trees and Structure of Relativized Complexity Classes

Heribert Vollmer

Lindström Quantifiers in Complexity Theory

Jie Wang

Random Isomorphisms

Osamu Watanabe

**Some Combinatorial Problem from the Study of Locally Random
Reducibility**

Gerd Wechsung

Query Order

ABSTRACTS

On the Power of Randomized Branching Programs

Farid Ablayev

Kazan University

(joint work with Marek Karpinski, Universität Bonn)

We define a notion of randomized branching programs in a natural way similar to the notion of randomized circuits. We present two explicit boolean functions $f_n : \{0, 1\}^{4n} \rightarrow \{0, 1\}$ and $g_n : \{0, 1\}^n \rightarrow \{0, 1\}$ such that:

1. f_n can be computed by a randomized ordered read-once branching program of size polynomial in n and with a small (constant) error,
2. any nondeterministic ordered read- k -times branching program that computes f_n needs exponential size (the size is $\Omega(\exp(n/(2k - 1)))$),
3. g_n can be computed by a nondeterministic read-once branching program of size polynomial in n , and
4. any randomized ordered read-once branching program that computes g_n with a constant error ϵ has size no less than $\exp(c(\epsilon)n/\log n)$.

Recent Progress on the Isomorphism Conjecture

Eric Allender

Rutgers University

<http://www.cs.rutgers.edu/~allender>

(joint work with Manindra Agrawal and Steven Rudich)

In this talk I will discuss recent progress by Manindra Agrawal, Steven Rudich, and myself, showing unexpected similarities in the structure of complete sets. We show that for any complexity class \mathcal{C} closed under many-one

reductions computable in uniform TC^0 , the following are true:

Gap: The sets that are complete for \mathcal{C} under AC^0 and NC^0 reducibility coincide.

Isomorphism: The sets complete for \mathcal{C} under AC^0 reductions are all isomorphic under isomorphisms computable and invertible by AC^0 circuits of depth three.

Our Gap Theorem does not hold for strongly uniform reductions: we show that there are Dlogtime-uniform AC^0 -complete sets for NC^1 that are not Dlogtime-uniform NC^0 -complete.

An important open problem is the question of whether there is any natural complexity class such that the sets complete under polynomial-time (or more powerful) reductions are *not* already complete under NC^0 reductions.

(This work extends the paper by Agrawal and myself in the 1996 Computational Complexity conference. A full paper is available at <http://www.cs.rutgers.edu/~allender/publications>.)

Kolmogorov-Easy Circuit Expressions

José L. Balcázar

Universitat Politècnica de Catalunya, Barcelona

<http://www-lsi.upc.es/~balqui>

(joint work with Harry Buhrman and Montserrat Hermo)

Circuit expressions were introduced to provide a natural link between Computational Learning and certain aspects of Structural Complexity. Upper and lower bounds on the learnability of circuit expressions are known. We study here the case in which the circuit expressions are of low (time-bounded) Kolmogorov complexity. We show that these are polynomial-time learnable if and only if accepting computations of accepting nondeterministic exponential-time machines can be found deterministically in exponential time. We also exactly characterize, in terms of advice classes and of doubly tally polynomial-time degrees, the sets that have such easy circuit expressions, and obtain consequences regarding their lowness.

(A full paper is available at <http://www-lsi.upc.es/~balqui/postscript/q-charact.ps>.)

Looking for an Analogue of Rice's Theorem in Complexity Theory

Bernd Borchert

Universität Heidelberg

<http://math.uni-heidelberg.de/logic/bb/bb.html>

(joint work with Frank Stephan, Universität Heidelberg)

Rice's Theorem says that every nontrivial semantical property of programs is undecidable. In this spirit we show the following: Every nontrivial absolute (gap, relative) counting property of circuits is UP-hard with respect to polynomial-time Turing reductions.

(A full paper is available at

<http://math.uni-heidelberg.de/logic/bb/papers/Rice.ps>.)

Six Hypotheses

Harry Buhrman

CWI Amsterdam

(joint work with Lance Fortnow, University of Chicago)

We consider the following six hypotheses:

- (1) $P = NP$,
- (2) $SAT \leq_{tt}^p PSEL$,
- (3) $SAT \leq_{tt}^p K\text{-APPROX}$,
- (4) SAT is $\mathcal{O}(\log n)$ -APPROX,
- (5) $FP^{NP[\log]} = FP_{||}^{NP}$, and
- (6) $(1SAT, SAT) \in P$.

It is known that (1) \implies (2) \implies (3) \implies [(4)&(5)] \implies (6).

We show the following:

1. If $\mu(\text{NP}) \neq 0$, then (1)—(5) are false.
2. If $\mu(\text{NP}) \neq 0$ and symmetry of information w.r.t. polynomial-time CD^{poly} holds (i.e., $(\forall x, y) [\text{CD}^p(xy) = \text{CD}^p(x) + \text{CD}^p(y|x) + \mathcal{O}(\log n)]$), then (1)—(6) are false.
3. Symmetry of information alone implies (1) \iff (5).
4. Consider the conjecture that there exists a hierarchy theorem for compressibility: For each polynomial p_1 there exists a polynomial p_2 such that for every n there exists a string x of length n satisfying

$$\text{CD}^{p_2}(x) \leq \mathcal{O}(\log n) \quad \& \quad \text{CD}^{p_1}(x) \geq n - \mathcal{O}(\log n).$$

The conjecture implies that

- (a) $\text{R} \subseteq \text{P}$ and
- (b) (1) \iff (6).

The proofs use essentially an upper bound lemma for CD complexity and a construction of Zuckerman.

A Variant of Immunity, Btt-Reductions, and Minimal Programs

Stephen Fenner

University of Southern Maine

We work with a generalization of immunity called k -immunity ($k \geq 1$). It is shown that if a set A is k -immune, then $K \not\leq_{k\text{-}tt} A$, where K is the halting problem. It is also shown that MIN, the set of minimal indices for partial computable functions, is k -immune for all k , and hence $K \not\leq_{btt} \text{MIN}$ ($\text{MIN} \stackrel{\text{df}}{=} \{e \mid (\forall i < e) [\phi_i \neq \phi_e]\}$). A short history of MIN is given, and it is mentioned that MIN is not regressive, all regressive sets are either computably enumerable or k -immune for all k , and every computably enumerable non-computable T-degree contains a k -immune, non- $(k+1)$ -immune set, for all k .

(Current sources are two technical reports found on the WWW at <http://www.cs.usm.maine.edu>.)

Two Queries

Lance Fortnow

CWI, Amsterdam, and The University of Chicago

<http://www.cs.uchicago.edu/~fortnow>

(joint work with Harry Buhrman at CWI)

Hemaspaandra, Hemaspaandra and Hempel showed that for $k > 2$, if $P_{tt}^{\Sigma_k^p[2]} = P^{\Sigma_k^p[1]}$ then $\Sigma_k^p = \Pi_k^p$. We extend their techniques to show that if $P_{tt}^{\Sigma_2^p[2]} = P^{\Sigma_2^p[1]}$ then $\Sigma_2^p = \Pi_2^p$.

However, the techniques cannot be pushed down to $k = 1$. We show a relativized world where $P_{tt}^{\text{NP}[2]} = P^{\text{NP}[1]}$ but $\text{NP} \neq \text{coNP}$.

What does happen when $P_{tt}^{\text{NP}[2]} = P^{\text{NP}[1]}$? Kadin shows that $\text{NP} \subseteq \text{coNP}/poly$ and thus $\text{PH} \subseteq \Sigma_3^p$ (Yap). Beigel, Chang and Ogihara building on Chang and Kadin improve this to show that every language in the polynomial-time hierarchy can be solved by an NP query and an Σ_2^p query.

Building on the techniques of the above papers we show several new collapses if $P_{tt}^{\text{NP}[2]} = P^{\text{NP}[1]}$ including:

- Locally either $\text{NP} = \text{coNP}$ or NP has polynomial-size circuits.
- $P^{\text{NP}} = P^{\text{NP}[1]}$.
- $\Sigma_2^p = \text{UP}^{\text{NP}[1]} \cap \text{RP}^{\text{NP}[1]}$.
- $\text{PH} = \text{BPP}^{\text{NP}[1]}$.

(The paper can be found at
<http://www.cs.uchicago.edu/~fortnow/papers.>)

The Complexity of Deterministically Observable Finite-Horizon Markov Decision Processes

Judy Goldsmith

University of Kentucky

<http://www.cs.engr.uky.edu/~goldsmi>

(joint work with Martin Mundhenk, Universität Trier, and Chris Lusena,
University of Kentucky)

We consider the complexity of the decision problem for different types of partially-observable Markov decision processes (MDPs): given an MDP, does there exist a policy with performance > 0 ? Lower and upper bounds on the complexity of the decision problems are shown in terms of completeness for NL, P, NP, PSPACE, EXP, NEXP or EXPSpace, dependent on the type of the Markov decision process. For several NP-complete types, we show that they are not even polynomial-time ε -approximable for any fixed ε , unless $P = NP$. These results also reveal interesting trade-offs between the power of policies, observations, and rewards.

Compressibility of Infinite Binary Sequences

Montserrat Hermo

Universität Trier

(joint work with Ricard Gavaldà and José L. Balcázar, Barcelona)

It is known that infinite binary sequences of constant Kolmogorov complexity are exactly the recursive ones. Such a kind of statement no longer holds in the presence of resource bounds. Contrary to what intuition might suggest, there are sequences of constant, polynomial-time bounded Kolmogorov complexity that are not polynomial-time computable. This motivates the study of several resource-bounded variants in search for a characterization, similar in spirit, of the polynomial-time computable sequences. We propose a definition, based on Kobayashi's notion of compressibility, and compare it to both the standard resource-bounded Kolmogorov complexity of infinite strings, and the uniform complexity introduced by Loveland. Some nontrivial coincidences and disagreements are proved. The resource-unbounded case is also considered.

The Shapes of Trees

Ulrich Hertrampf
Universität Stuttgart

We investigate the influence of the types of computation trees, allowed in a leaf language description of a certain complexity class, on the computational power of this class. To this end, we introduce three potentially different classes $\text{Leaf}^p(A)$, $\text{BalLeaf}^p(A)$, and $\text{FBTLeaf}^p(A)$, the classes of sets recognized using polynomial-time machines with acceptance defined by leaf language A , and arbitrary, balanced, or full binary trees as their computation trees. For language classes \mathcal{C} , we further define $\text{Leaf}^p(\mathcal{C}) \stackrel{\text{df}}{=} \bigcup_{A \in \mathcal{C}} \text{Leaf}^p(A)$ and analogously $\text{BalLeaf}^p(\mathcal{C})$, and $\text{FBTLeaf}^p(\mathcal{C})$.

For $A \in \mathcal{N}$ (the class of languages having a so-called *neutral* letter), it is easy to see that $\text{Leaf}^p(A) = \text{BalLeaf}^p(A) = \text{FBTLeaf}^p(A)$. On the other hand, in [U. Hertrampf, H. Vollmer, K. W. Wagner, On Balanced Versus Unbalanced Computation Trees, *Mathematical Systems Theory*, 1996] it was shown that $\text{BalLeaf}^p(\text{DLOGTIME}) = \text{FBTLeaf}^p(\text{DLOGTIME}) = \text{P}$, but $\text{Leaf}^p(\text{DLOGTIME}) = \text{P}^{\text{PP}}$.

For the set REG of regular languages, it was shown that $\text{Leaf}^p(\text{REG}) = \text{BalLeaf}^p(\text{REG}) = \text{FBTLeaf}^p(\text{REG}) = \text{PSPACE}$ (cf. [U. Hertrampf et al., On the Power of Polynomial Time Bit Reductions, *Structures* 1993]).

Our main results are:

- $(\forall L \in \text{REG}) (\exists L' \in \text{REG}) [\text{Leaf}^p(L) = \text{Leaf}^p(L') = \text{BalLeaf}^p(L') = \text{FBTLeaf}^p(L')]$.
- $(\forall L \in \text{REG}) (\exists L' \in \text{REG}) [\text{BalLeaf}^p(L) = \text{BalLeaf}^p(L') = \text{FBTLeaf}^p(L')]$.

Moreover, defining $\text{LEAF}^p(\mathcal{C}) \stackrel{\text{df}}{=} \{\text{Leaf}^p(A) \mid A \in \mathcal{C}\}$, and $\text{BALLEAF}^p(\mathcal{C})$ and $\text{FBTLEAF}^p(\mathcal{C})$ analogously, we obtain the existence of sets $\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3 \subseteq \text{REG}$ such that

- $\text{FBTLEAF}^p(\mathcal{C}_1) = \text{BALLEAF}^p(\mathcal{C}_1) \subseteq \text{LEAF}^p(\mathcal{C}_1)$,
- $\text{FBTLEAF}^p(\mathcal{C}_2) \subseteq \text{LEAF}^p(\mathcal{C}_2) \subseteq \text{BALLEAF}^p(\mathcal{C}_2)$, and
- $\text{LEAF}^p(\mathcal{C}_3) \subseteq \text{BALLEAF}^p(\mathcal{C}_3) \subseteq \text{FBTLEAF}^p(\mathcal{C}_3)$.

If $\oplus\text{P} \subseteq \text{NP}$, then all these inclusions are strict.

(These results are from [U. Hertrampf, Regular Leaf Languages and (Non-) Regular Tree Shapes, TR 95-21, Universität Lübeck, 1995].)

Mangrove Deforestation: Algorithms for Unambiguous Logspace Classes

Klaus-Jörn Lange

Universität Tübingen

<http://www-fs.informatik.uni-tuebingen.de/~lange>

(joint work with Eric Allender)

There are several versions of unambiguous log-space classes. We give a complete problem for the class $\text{RUSPACE}(\log n)$, making it the first non-syntactical class with a complete set. In the time-bounded case there are relativizations excluding the existence of complete sets.

Further on, in a joint work with ERIC ALLENDER, deterministic algorithms for the membership problems of the elements in $\text{RUSPACE}(\log n)$ using $\mathcal{O}(\log^2 n / \log n) = o(\log^2 n)$ space are constructed. As a consequence we get parallel algorithms running on rather simple machine models.

(The second part has appeared as TR 96-048 at <http://www.eccc.uni-trier.de>; the first part will appear in the *Chicago Journal of Theoretical Computer Science*.)

Equivalence of Measures of Complexity Classes

Jack H. Lutz

Iowa State University

(joint work with Josef Breutzmann)

The resource-bounded measures of complexity classes are shown to be robust with respect to certain changes in the underlying probability measure. Specifically, for any real number $\delta > 0$, any uniformly polynomial-time computable sequence $\vec{\beta} = (\beta_1, \beta_2, \beta_3, \dots)$ of real numbers (biases) $\beta_i \in [\delta, 1 - \delta]$ and any complexity class \mathcal{C} (such as P, NP, BPP, P/poly, PH, PSPACE, etc.) that is closed under positive polynomial-time truth-table reductions with queries of at most linear length, it is shown that the following two conditions are equivalent:

1. \mathcal{C} has p -measure 0 (respectively, measure 0 in E , measure 0 in E_2) relative to the coin-toss probability measure given by the sequence $\overline{\beta}$.
2. \mathcal{C} has p -measure 0 (respectively, measure 0 in E , measure 0 in E_2) relative to the uniform probability measure.

The proof introduces three techniques that may be useful in other contexts, namely, (i) the transformation of an efficient martingale for one probability measure into an efficient martingale for a “nearby” probability measure; (ii) the construction of a *positive bias reduction*, a truth-table reduction that encodes a positive, efficient, approximate simulation of one bias sequence by another; and (iii) the use of such a reduction to *dilate* an efficient martingale for the simulated probability measure into an efficient martingale for the simulating probability measure.

Nondeterministic NC^{\succ} Computation

Pierre McKenzie

Université de Montréal

<http://www.iro.umontreal.ca/~mckenzie>

(joint work with Hervé Caussinus, Montreal, Denis Thérien, McGill, and Heribert Vollmer, Würzburg)

We present and extend results from our 1996 Computational Complexity Conference paper with the same title. We define the counting classes $\#\text{NC}^1$, GapNC^1 , PNC^1 , and GNC^1 . We prove that boolean circuits, algebraic circuits, programs over nondeterministic finite automata, and programs over constant integer matrices yield equivalent definitions of the latter three classes. Alternative definitions of nondeterministic NC^1 computation lead to the open question of whether evaluating log-depth $\{+, \times\}$ formulas over \mathbb{N} reduces to multiplying constant size matrices over \mathbb{N} .

Then we adapt the leaf language concept to the level of NC^1 . We show how known characterizations imply $\text{ACC}^0 \subset \text{MODPH}$ and $\text{TC}^0 \subset \text{CH}$. We then extend these techniques to prove that MODPH (resp., CH) contains languages which have no ACC^0 -type circuits (resp., TC^0 -type circuits) of

size $2^{g(n)}$, provided $g(n)$ satisfies:

$$(\exists \epsilon) (\forall \text{ polynomials } p) [p(n)^{g(p(n) \cdot g(2^{p(n)}))} = o(2^{n^\epsilon})].$$

This in effect matches Eric Allender's COCOON'96 lower bounds, but with an even simpler proof which does not require Eric's stronger form of the time hierarchy theorem; Eric's constructive COCOON'96 lower bounds can also be deduced.

Interactive Proofs with Public Coins and Small Space Bounds

Rüdiger Reischuk
 Medizinische Universität zu Lübeck
 (joint work with Maciej Liskiewicz)

We consider interactive proof systems with a bound on the space used by the verifier. While such systems with a logarithmic space bound seem to be extremely powerful if the random coin flips are kept secret, restricting to public coins one stays within \mathcal{P} . An alternative characterization can be given by Arthur-Merlin-Games, that means stochastic Turing machines that alternate between probabilistic (A) and existential (M) configurations.

Let $\text{AM}_k\text{Space}(S)$ (resp. $\text{MA}_k\text{Space}(S)$) denote the corresponding complexity classes, where the machines start in a probabilistic (resp. existential) configuration and use at most space S . We prove for the language $\text{PATTERN} \stackrel{\text{df}}{=} \{w_1\#w_2\#\dots w_m\#\#u\#\# \text{BIN}(2^l) \mid l \in \mathbb{N}, u, w_i \in \{0, 1\}^*, |u| = l \ \& \ \exists i \ u = w_i\}$ the following results:

$$\begin{aligned} \text{PATTERN} &\in \text{MA}_2\text{Space}(\log \log), \\ \text{PATTERN} &\notin \text{AM}_2\text{Space}(o(\log)), \\ \overline{\text{PATTERN}} &\notin \text{AM}_2\text{Space}(o(\log)). \end{aligned}$$

This yields the hierarchy $\text{AM}_1\text{Space}(S) \subset \text{AM}_2\text{Space}(S) \subset \text{AM}_3\text{Space}(S)$ for any sublogarithmic space bound S . At the end we discuss how this hierarchy might be extended.

Characterizations of the Existence of Partial and Total One-Way Permutations

Jörg Rothe

Friedrich-Schiller-Universität Jena

<http://www.minet.uni-jena.de/~rothe>

(joint work with Lane A. Hemaspaandra, University of Rochester)

We study the easy certificate classes introduced by Hemaspaandra, Rothe, and Wechsung (cf. “Easy Sets and Hard Certificate Schemes,” to appear in *Acta Informatica*), with regard to the question of whether or not surjective one-way functions exist. This is an important open question in cryptology. We show that the existence of partial one-way permutations can be characterized by separating P from the class of UP sets that, for all unambiguous polynomial-time Turing machines accepting them, always have easy (i.e., polynomial-time computable) certificates. Similar results characterizing certain types of poly-one one-way functions are given.

This extends the work of Grollmann and Selman (“Complexity Measures for Public-Key Cryptosystems,” *SIAM Journal of Computing*, 1988) and Allender (“The Complexity of Sparse Sets in P,” *Structures* 1986). By Grädel’s recent results about one-way functions (“Definability on Finite Structures and the Existence of One-Way Functions,” *Methods of Logic in Computer Science*, 1994), this is also linked to statements in finite model theory.

Finally, we establish a condition necessary and sufficient for the existence of total one-way permutations.

Complexity at Higher Types

James Royer

Syracuse University

<http://top.cis.syr.edu/people/royer/royer.html>

Constable, in 1973, posed the problem of working out a computational complexity theory for functionals and operators of type-2 and higher. In particular, he wanted a good type-2 analogue of polynomial-time. Progress

on these questions has been slow in coming. In large part this is because understanding the dynamic complexity of type-2 computations is surprisingly tricky. In 1991 Kapron and Cook proved a machine characterization of BFF_2 , a particular type-2 analogue of polynomial-time and in the process introduced several lovely ideas that have been central to recent progress on Constable's problems. I will survey this work, focusing on the recent results of myself and others. I will also illustrate why sorting out complexity at type-3 and above will be an even trickier enterprise.

A Decision Procedure for Unitary Linear Quantum Cellular Automata

Miklos Santha
Université Paris-Sud

Linear quantum cellular automata were introduced recently as one of the models of quantum computing. A basic postulate of quantum mechanics imposes a strong constraint on any quantum machine: it has to be *unitary*, that is its time evolution operator has to be a unitary transformation. In this paper we give an efficient algorithm to decide if a linear quantum cellular automaton is unitary. The complexity of the algorithm is $\mathcal{O}(n^{\frac{4r\Gamma_3}{r+1}}) = \mathcal{O}(n^4)$ if the automaton has a continuous neighborhood of size r .

Is Testing More Complex Than Querying?

Rainer Schuler
Universität Ulm

In this talk we consider the complexity of generating instances of NP search problems with one of its solutions under some pre-chosen distribution. In particular, if the distribution is sufficiently natural, i.e., polynomial-time samplable, then generating only instances (asking questions) is “easy” for every problem. We observe that for every problem in \mathbb{R} (random polynomial

time), generating instances with solutions is easy for polynomial-time samplable distributions. It turns out that every problem that allows generating instances with solutions (certified instances) is contained in co-AM, where AM is the class of Arthur-Merlin games introduced by Babai. This shows that it is unlikely that every NP search problem allows generating certified instances. Nevertheless, it is still possible that natural problems not known to be in P, like graph isomorphism, fall into this class.

Algebraic and Logical Characterizations of Deterministic Linear Time Classes

Thomas Schwentick
Universität Mainz

<http://www.informatik.uni-mainz.de/PERSONEN/Schwentick.eng.html>

An algebraic characterization of the class DLIN of functions that can be computed in linear time by a deterministic RAM using only numbers of linear size is given. This class was introduced by Grandjean, who showed that it is robust and contains most computational problems that are usually considered to be solvable in deterministic linear time.

The characterization is in terms of a recursion scheme for unary functions. A variation of this recursion scheme characterizes the class DLINEAR, which allows polynomially large numbers. A second variation defines a class that still contains $\text{DTIME}(n)$, the class of functions that are computable in linear time on a Turing machine.

From these algebraic characterizations logical characterizations of DLIN and DLINEAR as well as complete problems for these classes (under $\text{DTIME}(n)$ reductions) are derived.

An Information-Theoretic Treatment of Random-Self-Reducibility

Martin Strauss

Iowa State University

<http://www.cs.iastate.edu/~mstrauss/homepage.html>

(joint work with Joan Feigenbaum, AT&T Labs)

Informally, a function f is *random-self-reducible* if the evaluation of f at any given instance x can be reduced in polynomial time to the evaluation of f at one or more *random* instances y_i , each one of which is uncorrelated with x .

Random-self-reducible functions have many applications, including average-case complexity, lower bounds, cryptography, interactive proof systems, and program checkers, self-testers, and self-correctors.

In this paper, we initiate the study of random-self-reducibility from an information-theoretic point of view. Specifically, we formally define the notion of a random-self-reduction that, with respect to a given ensemble of distributions, leaks a limited number of bits, *i.e.*, produces y_i 's in such a manner that each has a limited amount of mutual information with x . We argue that this notion is useful in studying the relationships between random-self-reducibility and other properties of interest, including self-correctability and NP-hardness. In the case of self-correctability, we show that the information-theoretic definition of random-self-reducibility leads to somewhat different conclusions from those drawn by Feigenbaum, Fortnow, Laplante, and Naik [2], who used the standard definition. In the case of NP-hardness, we use the information-theoretic definition to strengthen the result of Feigenbaum and Fortnow [1], who proved, using the standard definition, that the polynomial hierarchy collapses if an NP-hard set is random-self-reducible.

(The full paper can be found at

<http://www.research.att.com/library/trs/TRs/96/96.13/96.13.1.body.ps>.)

References

- [1] J. Feigenbaum and L. Fortnow. Random-self-reducibility of complete sets. *SIAM Journal on Computing*, 22:994–1005, 1993.

- [2] J. Feigenbaum, L. Fortnow, S. Laplante, and A. Naik. On coherence, random-self-reducibility, and self-correction. In *Proc. 11th Conference on Computational Complexity*, pages 59–67. IEEE Computer Society Press, Los Alamitos, 1996.

The Crane Beach Conjecture

Denis Thérien
McGill University, Montreal

Let $L \subseteq \Sigma^*$, $e \in \Sigma$; e is *neutral* for L if and only if, for all $u, v \in \Sigma^*$, uv is in L if and only if uev is in L . The Crane Beach Conjecture says the following: If L is a language with a neutral letter, then L is in AC^0 if and only if L is a regular $*$ -free set. In logical terms, this means that, assuming the presence of a neutral letter, any language definable by a first-order sentence using arbitrary numerical predicates can also be represented by a first-order formula using $<$ only. Using the Furst-Saxe-Sipser/Ajtai circuit lower bound for PARITY, we know the conjecture to be true under the additional assumption that the language is regular. On the other hand, an independent proof of the Crane Beach Conjecture would imply the circuit lower bound.

The Isomorphism Problem for One-Time-Only Branching Programs and Arithmetic Circuits

Thomas Thierauf
Universität Ulm

We investigate the computational complexity of the isomorphism problem for one-time-only branching programs (1-BPI): On input of two such programs, B_0 and B_1 , decide whether there exists a permutation of the variables of B_1 such that it becomes equivalent to B_0 .

We show that 1-BPI cannot be NP-hard, unless the polynomial hierarchy collapses to the second level. The result is extended to the isomorphism problem for arithmetic circuits over large enough fields.

Boolean Decision Trees and Structure of Relativized Complexity Classes

Nicolai Vereshchagin
Moscow State University

We define analogs of the complexity classes P, NP, AM, and IP for the Boolean decision trees model. The analogs are denoted respectively by P_{dt} , NP_{dt} , AM_{dt} , and IP_{dt} . It is known that $P_{dt} \neq NP_{dt}$, but $NP_{dt} \cap coNP_{dt} = P_{dt} = BPP_{dt}$ and even $IP_{dt} \cap coIP_{dt} = P_{dt}$. The open problem is whether $IP_{dt} = NP_{dt}$ or not. Trying to prove that $IP_{dt} \neq NP_{dt}$, we define two classes \mathcal{C}_1 and \mathcal{C}_2 both containing all of IP_{dt} for which we managed to prove that $NP_{dt} \neq \mathcal{C}_1$ and $NP_{dt} \neq \mathcal{C}_2$ and even $MA_{dt} \neq \mathcal{C}_1$ and $MA_{dt} \neq \mathcal{C}_2$.

Lindström Quantifiers in Complexity Theory

Heribert Vollmer
Universität Würzburg

<http://haegar.informatik.uni-wuerzburg.de/person/mitarbeiter/vollmer>
(joint work with Hans-Jörg Burtschick, Technische Universität Berlin)

We show that examinations of the expressive power of logical formulae enriched by Lindström quantifiers over ordered finite structures have a well-studied complexity-theoretic counterpart: the leaf language approach to define complexity classes. Model classes of formulae with Lindström quantifiers are nothing else than leaf language definable sets. Along the way we tighten the best up to now known leaf language characterization of the classes of the polynomial time hierarchy and give a new model-theoretic characterization of PSPACE.

Random Isomorphisms

Jie Wang

University of North Carolina at Greensboro

We extend the NP-isomorphism theory of Berman and Hartmanis in the setting of randomized reductions for distributional NP problems. Early results on isomorphisms of average-case NP-complete problems are obtained w.r.t. deterministic reductions. We define, in a standard way, what it means for two distributional NP problems to be isomorphic under randomized reductions. We then show that all the known average-case NP-complete problems, whether they are complete under deterministic or randomized reductions, are all “randomly” isomorphic, and so these problems, regardless their origins, are “random encodings” of each other.

Some Combinatorial Problem from the Study of Locally Random Reducibility

Osamu Watanabe

Tokyo Institute of Technology

<http://watanabe-www.cs.titech.ac.jp/~watanabe/myhome/intro-e.html>

Abadi, Feigenbaum, and Kilian (in M. Abadi, J. Feigenbaum, and J. Kilian, On Hiding Information from an Oracle, *Journal of Computer and Systems Sciences*, Vol. 39, (1989), 21–50) formally defined the notion of “locally random reducibility” and studied it from a complexity theoretic point of view. Since then, it has been open whether every function is k -locally reducible to some k functions, even for some constant $k \geq 2$. Based on the idea of Yao, Fortnow and Szegedy showed that there is a Boolean function that is 2-locally reducible to no pair of Boolean functions, but their argument does not seem to work for the question whether there is a Boolean function that is 2-locally reducible to no pair of functions whose range is $\{0, 1, 2\}$. Here I asked one combinatorial question, which seems to be a key for solving this problem.

Query Order

Gerd Wechsung

Friedrich-Schiller-Universität Jena

<http://www.minet.uni-jena.de/~wechsung>

(joint work with Lane A. Hemaspaandra and Harald Hempel)

Let $P^{C[1]:D[1]}$ be the class of all sets accepted by a polynomial-time oracle Turing machine asking one query to some oracle $C \in \mathcal{C}$ followed by one query to some oracle $D \in \mathcal{D}$. We ask: Does query order matter, i.e. does

$$P^{C[1]:D[1]} = P^{D[1]:C[1]}$$

hold?

We show for \mathcal{C}, \mathcal{D} from the Boolean hierarchy over NP

$$P^{BH_i[1]:BH_j[1]} = \begin{cases} R_{(i+2j-1)-tt}^p(\text{NP}) & \text{if } i \equiv 0(2) \wedge j \equiv 1(2) \\ R_{(i+2j)-tt}^p(\text{NP}) & \text{otherwise.} \end{cases}$$

From this it follows that the only nontrivial case for

$$P^{BH_i[1]:BH_j[1]} = P^{BH_j[1]:BH_i[1]}$$

is i even and $j = i + 1$, provided that $i \leq j$. In all remaining cases we have nonequality, unless the BH, and thus also the PH, collapse.

We similarly characterize oracle classes with a tree like query structure and oracles from the BH.