Twelfth Annual IEEE Conference on Computational Complexity

Proceedings

Twelfth Annual IEEE Conference on Computational Complexity

(Formerly: Structure in Complexity Theory Conference)

June 24-27, 1997
Ulm, Germany

Sponsored by

The IEEE Computer Society Technical Committee on
Mathematical Foundations of Computing

In cooperation with

ACM-SIGACT and EATCS

With support from

Ulmer Universitäts-Gesellschaft, Daimler Benz, the Sparkasse Ulm
and the Universitat Politècnica de Catalunya

IEEE
COMPUTER
SOCIETY

Los Alamitos, California
Washington • Brussels • Tokyo

The papers in this book comprise the proceedings of the meeting mentioned on the cover and title page. They reflect the authors' opinions and, in the interests of timely dissemination, are published as presented and without change. Their inclusion in this publication does not necessarily constitute endorsement by the editors, the IEEE Computer Society, or the Institute of Electrical and Electonics Engineers, Inc.

IEEE Catalog Number 97CB36072
ISBN 0-8186-7907-7 (softbound)
ISBN 0-7803-4267-4 (casebound)
ISBN 0-8186-7909-3 (microfiche)
ISSN: 1093-0159

Additional copies may be ordered from:

IEEE Computer Society
Customer Service Center
10662 Los Vaqueros Circle
P.O. Box 3014
Los Alamitos, CA 90720-1314
Tel: + 1-714-821-8380
Fax: + 1-714-821-4641
E-mail: cs.books@computer.org

IEEE Service Center
445 Hoes Lane
P.O. Box 1331
Piscataway, NJ 08855-1331
Tel: + 1-908-981-1393
Fax: + 1-908-981-9667
mis.custserv@computer.org

IEEE Computer Society
13, Avenue de l'Aquilon
B-1200 Brussels
BELGIUM
Tel: + 32-2-770-2198
Fax: + 32-2-770-8505
euro.ofc@computer.org

IEEE Computer Society
Ooshima Building
2-19-1 Minami-Aoyama
Minato-ku, Tokyo 107
JAPAN
Tel: + 81-3-3408-3118
Fax: + 81-3-3408-3553
tokyo.ofc@computer.org

Editorial production by Penny Storms

Cover art production by Joseph Daigle/Studio Productions

Printed in the United States of America by Sony Electronic Publishing Services

IEEE
COMPUTER
SOCIETY

IEEE

Proceedings

Twelfth Annual IEEE Conference on Computational Complexity

(Formerly: Structure in Complexity Theory Conference)

Foreword

This volume collects the 27 papers accepted for presentation at the Computational Complexity Conference held June 24 to 27, 1997, in Ulm, Germany. They were selected from among the 75 submissions, gathered electronically (with a single exception) after publication of the call for papers. It also contains the texts on which some of the Program Committee members (Harry Buhrman, Pierluigi Crescenzi, Georg Gottlob, and Klaus Wagner) based the survey talks that they contributed to the conference.

It must be pointed out that, whereas a few of the submissions received a substantial amount of feedback, the short time available and the large effort needed to fully referee a paper in our area imply that these texts must be considered, in general, only as extended research abstracts. We anticipate that most of them will eventually appear, in final, fully refereed form, in the customary scientific journals.

The Program Committee met in Barcelona for the selection, after conducting some brief discussion through electronic mail. In light of the experience, the Program Committee Chairman has deduced a few observations regarding electronic submissions to conferences and electronic versus presential selection committees, and will do his best to write them up.

We are thankful to those organizations that provided support for the conference. A large number of individuals merit acknowledgment for their help in various ways. Apologizing to those that we risk to omit, thanks are due to: first and foremost, all the individuals who submitted their scientific work, with or without success, for the success of the conference lies primarily on them; Sam Rebelski and Rob Schapire, who allowed for the use of their respective software systems to help with the organization of electronic submissions and with conducting preliminary e-mail discussions; Conrado Martinez, who helped to install part of the software; and the following subreferees (our apologies for the list not being, perhaps, exhaustive):

Sergio De Agostino, Jean-Paul Allouche, Carme Àlvarez, Andris Ambainis, Klaus Ambos-Spies, V. Arvind, Giorgio Ausiello, Cristina Bazgan, Richard Beigel, Michael Ben-Or, Dan Boneh, Ravi Boppana, Bernd Borchert, Stéphane Boucheron, Andrea Clementi, Nadia Creignou, Antonella Cresti, Alain Denise, Bruno Durand, Christophe Dürr, Thomas Eiter, Juan Luis Esteban, Kousha Etessami, Uri Feige, Wenceslas Fernandez de la Vega, Lance Fortnow, Kim Gabarró, Péter Gács, Nicola Galesi, Ricard Gavaldà, Oded Goldreich, Judy Goldsmith, Etienne Grandjean, Fred Green, Serge Grigorieff, Vince Grolmusz, Peter Grunwald, David Guijarro, Péter Hajnal, Armin Haken, Montse Hermo, Steve Homer, Russell Impagliazzo, Sandy Irani, Birgit Jenner, Viggo Kann, Sampath Kannan, Lila Kari, Claire Kenyon, Sanjeev Khanna, Johannes Köbler, Sven Kosub, Klaus-Jörn Lange, Huong Le-Thanh, Matthew Levy, Wolfgang Lindner, Antoni Lozano, Carsten Lund, Jack Lutz, Janos Makowsky, Elvira Mayordomo, Pierre McKenzie, Peter Bro Miltersen, Angelo Monti, Martin Mundhenk, Noam Nisan, Mitsunori Ogihara, Rafail Ostrovsky, Erez Petrank, Yuri Rabinovitch, Omer Reingold, Steffen Reith, Heinz Schmitz, Uwe Schöning, Lex Schrijver, Rainer Schuler, Maria Serna, Avy Sharell, Riccardo Silvestri, Anatol Slissenko, Martin Strauss, Mario Szegedy, Gábor Tardos, Amnon Ta-Shma, Bas Terwijn, Denis Thérien, Thomas Thierauf, Jacobo Torán, Leen Torenvliet, Luca Trevisan, John Tromp, Wim van Dam, Peter van Emde Boas, Dieter van Melkebeek, Helmut Veith, Paul Vitanyi, Heribert Vollmer, Osamu Watanabe, Chris Wilson, and Fatos Xhafa.

José Balcázar
Program Chair

Harry Buhrman
Pierluigi Crescenzi
Georg Gottlob
Toniann Pitassi
Ran Raz
Miklós Sántha
Klaus Wagner

Committees

Conference Committee

Steven Homer (Chair), *Boston University*
Eric Allender, *Rutgers University*
Jin-Yi Cai, *SUNY at Buffalo*
Anne Condon, *University of Wisconsin*
Joan Feigenbaum, *AT&T Bell Laboratories*
Lance Fortnow, *University of Chicago*
Luc Longpré, *University of Texas at El Paso*
Avi Wigderson, *The Hebrew University*

Local Arrangements Chairs

Uwe Schöning, *Universität Ulm*
Jacobo Toran, *Universität Ulm*

Publicity Chair

Luc Longpré
University of Texas at El Paso

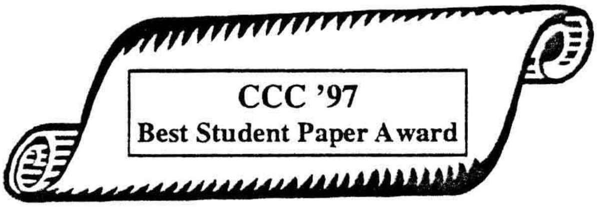
Program Committee

José Balcázar (Chair), *Universitat Politècnica de Catalunya*
Harry Buhrman, *CWI Amsterdam*
Pierluigi Crescenzi, *Università di Roma ``La Sapienza"*
Georg Gottlob, *TU Wien*
Toniann Pitassi, *University of Arizona*
Ran Raz, *Weizmann Institute of Science*
Miklós Sántha, *Université Paris-Sud*
Klaus Wagner, *Universiät Würzburg*

Acknowledgments

Our thanks to the "Ulmer Universitäts-Gesellschaft" which provided a grant for the travel expenses of three participants to the conference. The Universitat Politècnica de Catalunya provided support for the program committee meeting and for a Theory Day which proceeded it. The Universität Ulm graciously provided the space and facilities for this conference. Our thanks to both of these institutions for their generosity and support.

1997 Best Student Paper Award



The program committee of the 1997 Conference on Computational Complexity is proud to present the Best Student Paper Award to Cristoph Karg of the University of Ulm. This award is given annually to the most outstanding paper written solely by one or more students. The paper selected this year by the CCC Program Committee is

LR(k) Testing is Average-Case Complete

by

Cristoph Karg

Congratulations to the winner !

Table of Contents

Twelfth Annual IEEE Conference on Computational Complexity

Session 1

Session Chair: José Balcázar

Session 2

Session Chair: Harry Buhrman

Session 3

Session Chair: Klaus Wagner

Session 4

Session Chair: Miklós Sántha

Session 5

Session Chair: Steven Homer

Session 6

Session Chair: Pierluigi Crescenzi

Session 7

Session Chair: Georg Gottlob

Session 1

Chair:
José Balcázar

Universitat Politècnica de Catalunya,
Barcelona

Six Hypotheses in Search of a Theorem

Harry Buhrman* Lance Fortnow† Leen Torenvliet‡

Sir, we are truly six special and interesting characters. Believe us. However we have gone lost.
- "Six Characters in Search of an Author."
Luigi Pirandello.

Abstract

We consider the following six hypotheses:

- $\mathbf{P} = \mathbf{NP}$.
- **SAT** is truth-table reducible to a **P**-selective set.
- **SAT** is truth-table reducible to a k-approximable set for some k.
- $\mathbf{FP}^{\mathbf{NP}}_{||} = \mathbf{FP}^{\mathbf{NP}[\log]}$
- **SAT** is $O(\log n)$-approximable.
- Solving **SAT** is in **P** on formulae with at most one assignment.

We discuss their importance and relationships among them.

1 Introduction

Complexity theorists have put considerable effort into investigating the structure and properties of sets in **NP**. This research led to various hypotheses. In this survey paper we put together, for the first time, six hypotheses that we encountered in our own research as well as in the literature. We believe that these hypotheses are important and are closely related to each other.

The first hypothesis is: "$\mathbf{P} = \mathbf{NP}$." This is the most famous and important one and does not need any further introduction.

Most sets in **NP** that arise from practice turn out to be **NP**-complete. Moreover since complete sets reflect the structure of a complexity class they receive close attention. Three of our six hypotheses concern sets that are complete or hard for **NP**.

Selman [Sel82] introduced the **P**-selective sets in analogue of recursion theory. A set is called **P**-*selective* iff there exists a polynomial time computable function that from two strings x and y selects one that (if at least one belongs to A) is in A. He investigated the possibility for **NP** to have hard sets that are **P**-selective. He showed [Sel82] that this can not be the case for many-one reductions (unless $\mathbf{P} = \mathbf{NP}$). This was later improved to $\leq^p_{1-tt}$ reductions by Buhrman and Torenvliet [BT96b]. The hypothesis we are interested in is: "**NP** has a truth-table hard set that is **P**-selective."

Beigel [Bei87a], looking at properties of bounded queries to sets (in **NP**), developed a generalization of **P**-selective sets later dubbed the approximable sets. A set A is k-approximable if there exists a polynomial time computable function that with k strings $x_1, \ldots, x_k$ as input, generates k bits $b_1, \ldots, b_k$ such that for at least 1 bit it is true that $b_i \neq \chi_A(x_i)$. That is from the 2^k possible settings of $x_1, \ldots, x_k$ one is excluded. Beigel, Kummer and Stephan [BKS95], Agrawal and Arvind [AA96], and Ogihara [Ogi95]

[*] URL: http://www.cwi.nl/cwi/people/Harry.Buhrman.html. E-mail: buhrman@cwi.nl. Partially supported by the Dutch foundation for scientific research (NWO) by SION project 612-34-002, and by the European Union through Neuro-COLT ESPRIT Working Group Nr. 8556, and HC&M grant nr. ERB4050PL93-0516. CWI, Kruislaan 413, 1098SJ Amsterdam, The Netherlands.

[†] URL: http://www.cs.uchicago.edu/~fortnow. Email: fortnow@cs.uchicago.edu. Supported in part by NSF grant CCR 92-53582, the Dutch Foundation for Scientific Research (NWO) and a Fulbright Scholar award. CWI and University of Chicago, Department of Computer Science 1100 E. 58th. St. Chicago, IL 60637, USA.

[‡] URL: http://turing.wins.uva.nl/~leen/. E-mail: leen@wins.uva.nl. University of Amsterdam, Department of Computer Science, Plantage Muidergracht 24, 1018TV Amsterdam, The Netherlands.

showed that **NP** can not have $\leq^p_{btt}$ -hard sets that are k-approximable for some k (unless **P** = **NP**). Since **P**-selective sets are in fact 2-approximable sets this result also improves the bound for **P**-selective sets. The hypothesis related to this work is: "**NP** has a truth-table hard set that is k-approximable for some k."

Ogihara [Ogi95] working on the hypothesis that **NP** has a truth-table hard **P**-selective set, took it one step further and considered $f(n)$-approximable sets for non-constant functions $f(n)$. He showed that if **SAT** is not $a\log(n)$-approximable for $a < 1$ unless **P** = **NP**. This result subsumes the results on truth-table reductions to k-approximable sets (see Section 3). The hypothesis connected to this work is: "**SAT** is $O(\log(n))$-approximable."

The next hypothesis states that it is possible to compute **SAT** in polynomial time when we only consider formulae with at most *one* satisfying assignment. It is possible to phrase this in terms of sets as: "**Unique-SAT** ∈ **P**" (see Section 2). Valiant and Vazirani [VV86] showed that this set problem for **SAT** is hard for **NP** under randomized reductions.

The last hypothesis deals with functions that are computable in polynomial time relative to some set in **NP**. There are essentially three different ways to define this. The most unrestricted way is that the polynomial time computable function has unrestricted access to an **NP** oracle and is called $\mathbf{FP^{NP}}$. The next restriction to the oracle mechanism is that the queries have to be non-adaptive: $\mathbf{FP^{NP}_{||}}$. The last and most restrictive version is that only $O(\log(n))$ queries are allowed on inputs of length n: $\mathbf{FP^{NP[\log]}}$. The last hypothesis can now be stated as: $\mathbf{FP^{NP[\log]}} = \mathbf{FP^{NP}_{||}}$.

These are the main characters of our paper. We show that these hypotheses are closely related to each other and in Section 3 we show which of these hypotheses implies any of the others. Furthermore we give background information on each of them individually and we indicate which problems are still open. The main open question however is to show that any two of these six hypotheses are equivalent.

We should note that probably all of the six hypotheses are false since all of them imply that **NP** ⊆ **P**/*poly* and this on its turn implies that the polynomial time hierarchy collapses to its second level [KL80].

Until recently no oracles were known that showed that any of these hypotheses are different from each other. However recent progress has been made in this direction (see Section 7).

2 Preliminaries

We assume the reader familiar with basic notions of computation and complexity theory as can be found e.g. in [HU79, BDG88, BDG90, GJ79] and many other textbooks.

Central to the six hypotheses in this paper however are the following notions, which we will highlight here by separately defining them.

Definition 2.1 *A set A is called* **P***-selective iff there exists a polynomial time computable function f (called p-selector function) such that for any two strings x and y, $f(x,y) \in \{x,y\}$ and if x or y is in A then $f(x,y)$ is in A.*

For a set A we will identify A with its characteristic function. Hence for a string x, $A(x) \in \{0,1\}$ and $A(x) = 1$ iff $x \in A$. For two strings x and y and a **P**-selective set A, a p-selector excludes one of the four possibilities for the string $A(x)A(y)$ (either 01 or 10 is impossible). A generalization extends this exclusion to one of the possible settings for the string $A(x_1)\ldots A(x_k)$ for some function $k(n)$. For constant k, this notion was called "approximability" of sets (see Beigel et al. [BKS95]).

Definition 2.2 *A function g is called an f-approximator for a set A if for every $x_1,\ldots,x_m$ with $m \geq f(\max\{|x_1|,\ldots,|x_m|\})$,*

$$g(x_1,\ldots,x_m) \in \{0,1\}^m$$
and
$$(A(x_1),\ldots,A(x_m)) \neq g(x_1,\ldots,x_m)$$

A set A is then called f-approximable if it has an f-approximator. A is bounded-approximable, *or $A \in$* **bAPP** *if A is k-approximable for some constant k.*

The notion f-approximability was called f-membership comparability by Ogihara [Ogi95] who was the first to consider this notion for nonconstant functions. Beigel [Bei87a] uses the term "approximable" to represent **bAPP**. Sets which are not in **bAPP** Beigel calls superterse.

Amir, Beigel and Gasarch [ABG90] show that every **bAPP** language is in **P**/poly. Ogihara [Ogi95] notices that their proof generalizes.

Theorem 2.3 (Amir-Beigel-Gasarch-Ogihara) *If A is $f(n)$-approximable for any polynomial $f(n)$ then A is in* **P***/poly.*

We use the function $\mathbf{F_{SAT}}$ which on input $\phi_1,\ldots,\phi_n$ returns a string $x \in \{0,1\}^n$, where $x_i = 1$ iff $\phi_i \in$ **SAT**. We will also need classes of functions that are computable by queries to **SAT**. Depending on the number of queries and the type of oracle access these are defined as follows.

Definition 2.4 *A function f is in* $\mathbf{FP}^{\mathbf{NP}}_{||}$ *if there exists a polynomial time bounded oracle machine M that computes f with non-adaptive queries to some language in* **NP**.

Note that $\mathbf{F_{SAT}}$ is $\mathbf{FP}^{\mathbf{NP}}_{||}$ complete. A set is sparse if there exists a polynomial p such that for each length n it contains at most $p(n)$ strings. Let **SPARSE** denote the class of all sparse sets.

A truth-table reduction from A to B is disjunctive ($A \leq^p_{dtt} B$) if it accepts iff one of it queries is in B.

Definition 2.5 *A function f is in* $\mathbf{FP}^{\mathbf{NP}[\log]}$ *if there is a polynomial time bounded oracle machine that computes f using $O(\log n)$ (adaptive) queries to some language in* **NP**.

Definition 2.6 *Let Q denote a boolean predicate. we define the set* Unique-$\mathbf{SAT}_Q$ *as follows.*

For any formula x

$$\textit{Unique-}\mathbf{SAT}_Q(x) = \begin{cases} 0 & \textit{if } x \notin \mathbf{SAT} \\ 1 & \textit{if } x \textit{ has 1} \\ & \textit{satisfying assignment} \\ Q(x) & \textit{Otherwise} \end{cases}$$

*If there exists a predicate Q such that Unique-$\mathbf{SAT}_Q$ is polynomial time computable then we will say "Unique-***SAT** $\in$ *P."*

The notion of bounded nondeterminism was introduced by Kintala and Fischer in [KF80].

Definition 2.7 *Let f be any function. We define* $\mathbf{NP}(f(n)) = \{L \mid L \subseteq \{0,1\}^*$ *and there is a constant c such that L is accepted by a polynomial time bounded Turing machine making at most $f(n)$ c-ary nondeterministic moves*$\}$

Kintala and Fischer denote $\mathbf{NP}(f(n))$ as $\mathcal{P}_{f(n)}$.

Definition 2.8 *A function $f(x)$ is $h(n)$-enumerable iff there exists a polynomial-time computable function $g(x) = \{y_1, \ldots, y_{h(n)}\}$ such that for every x, $f(x) \in g(x)$. A function $f(x)$ is poly-enumerable $f(x)$ is n^c enumerable for some c.*

There is a very useful connection between $\mathbf{FP}^{\mathbf{NP}}_{||} = \mathbf{FP}^{\mathbf{NP}[\log]}$ and the enumerability of $\mathbf{F_{SAT}}$ [Bei87a].

Lemma 2.9 (Beigel) $\mathbf{FP}^{\mathbf{NP}}_{||} = \mathbf{FP}^{\mathbf{NP}[\log]}$ *if and only if* $\mathbf{F_{SAT}}$ *is poly-enumerable.*

Proof:
($\mathbf{FP}^{\mathbf{NP}}_{||} = \mathbf{FP}^{\mathbf{NP}} \Rightarrow \mathbf{F_{SAT}}$ is poly-enumerable)
$\mathbf{F_{SAT}} \in \mathbf{FP}^{\mathbf{NP}}_{||}$, so by assumption it is in $\mathbf{FP}^{\mathbf{NP}[\log]}$. There are polynomially possible answers for the oracle queries of the $\mathbf{FP}^{\mathbf{NP}[\log]}$ machine. Cycling through them yields an enumeration of $\mathbf{F_{SAT}}$.
($\mathbf{F_{SAT}}$ is polynomial enumerable $\Rightarrow \mathbf{FP}^{\mathbf{NP}}_{||} = \mathbf{FP}^{\mathbf{NP}}$)
On input $\phi_1, \ldots, \phi_l$ each of size at most n one can enumerate n^c vectors $b_1, \ldots b_{n^c}$ such that $b_i = \mathbf{F_{SAT}}$ for some i. Next one can use binary search to some suitable oracle in **NP** to find b_i, using $\log(n^c) + 1$ queries. □

We will need the following definition of the dimension of a family of sets, called Vapnik-Chervonenkis dimension [VC71]:

Definition 2.10 *Given a family of sets $\mathcal{F}$ the Vapnik-Chervonenkis dimension of $\mathcal{F}$ or VC-dimension is the largest number d such that there exists a set A with $\|A\| = d$ and $\|\{A \cap F \mid F \in \mathcal{F}\}\| = 2^d$. If such a d does not exist the VC-dimension of $\mathcal{F}$ is ∞.*

Sauer [Sau72] and independently Shelah [She72] proved the following lemma. Sauer notes that Paul Erdös originally posed this as a question.

Lemma 2.11 *If $\mathcal{F}$ is a family of sets with VC-dimension at most d then for any set A with $\|A\| = n$:*

$$\|\{A \cap F \mid F \in \mathcal{F}\}\| \leq \sum_{i=0}^{d} \binom{n}{i}$$

For $n \geq d \geq 1$, $\sum_{i=0}^{d} \binom{n}{i}$ is bounded by $n^d + 1$. Moreover the proof of Lemma 2.11 is constructible: Suppose we have a polynomial-time algorithm that on $S = x_1, \ldots, x_{d+1}$ computes a subset of S that is not in $\{A \cap F \mid F \in \mathcal{F}\}$. Lemma 2.11 gives us a polynomial-time algorithm to compute $\{A \cap F \mid F \in \mathcal{F}\}$ in time polynomial in n and the sizes of the elements of A.

3 Relations

In this section we will show which of the six hypotheses implies any of the others. The relations are given in Figure 1.

Theorem 3.1 $\mathbf{P} = \mathbf{NP} \Rightarrow \mathbf{SAT} \leq^p_{tt} \mathbf{Psel}$.

Proof: If $\mathbf{P} = \mathbf{NP}$ then **SAT** is in **P** and reduces to any set. □

$$\begin{tikzcd}
\mathbf{P} = \mathbf{NP} \arrow[d, Rightarrow] & \\
\mathbf{SAT} \leq^p_{tt} \mathbf{Psel} \arrow[d, Rightarrow] & \\
\mathbf{SAT} \leq^p_{tt} \mathbf{bAPP} \arrow[d, Rightarrow] & \mathbf{SAT} \text{ is } O(\log n) \text{ approximable} \\
\mathbf{FP}^{\mathbf{NP}}_{||} = \mathbf{FP}^{\mathbf{NP}[\log]} \arrow[ur, Rightarrow] \arrow[dr, Rightarrow] & \\
& \text{Unique-}\mathbf{SAT} \text{ in } \mathbf{P}
\end{tikzcd}$$

Figure 1: Relations

Theorem 3.2 $\mathbf{SAT} \leq^p_{tt} \mathbf{Psel} \Rightarrow \mathbf{SAT} \leq^p_{tt} \mathbf{bAPP}$

Proof: Note that every **P**-selective set is 2-approximable. □

Theorem 3.3 $\mathbf{SAT} \leq^p_{tt} \mathbf{bAPP} \Rightarrow \mathbf{FP}^{\mathbf{NP}}_{||} = \mathbf{FP}^{\mathbf{NP}[\log]}$.

We first prove the following lemma due to Beigel [Bei87a, Bei87b].

Lemma 3.4 (Beigel) *If A is k-approximable then there exists a function f which computes for any n numbers $x_1, \dots, x_n$ a set of at most $\sum_{i=0}^{k-1} \binom{n}{i}$ vectors from $\{0,1\}^n$ which contains $\mathbf{F}^A_n(x_1, \dots, x_n)$. Moreover f runs in time polynomial in n and the size of the largest string in $x_1, \dots, x_n$.*

Proof: Let g be the function that k-approximates A. Define the following family of sets:

$$\mathcal{F} = \{B \mid g \text{ is a } k\text{-approximator for } B\}$$

It follows that the VC-dimension of $\mathcal{F}$ is at most $k - 1$. We then apply the constructible version of Lemma 2.11. □

We now give the proof of Theorem 3.3.
Proof: Let M witness the fact that **SAT** truth-table reduces to a k-approximable set A. let $f \in \mathbf{FP}^{\mathbf{NP}}_{||}$ via machine M_f. On input x, M_f computes the following queries $q_1, \dots, q_l$ to **SAT**, for l some polynomial. Next reduce each of these queries to A with M, yielding a set of queries $q'_1, \dots, q'_{l'}$, for l' a polynomial. Next we apply Lemma 3.4 to generate l'^k many different vectors, containing $\mathbf{F}^A_{l'}(q'_1, \dots, q'_{l'})$. From these vectors one can generate l'^k many vectors containing $\mathbf{F}^{\mathbf{SAT}}_l(q_1, \dots, q_l)$. $\mathbf{FP}^{\mathbf{NP}}_{||} = \mathbf{FP}^{\mathbf{NP}[\log]}$ follows from Lemma 2.9. □

The following theorem is implicit in [Bei88, Tod91b]

Theorem 3.5 (Beigel-Toda)
$\mathbf{FP}^{\mathbf{NP}}_{||} = \mathbf{FP}^{\mathbf{NP}[\log]} \Rightarrow$ *Unique-***SAT** *is in* **P**

Proof: We have to show that there is a polynomial time algorithm that tells formulae with exactly one satisfying assignment apart from ones that are unsatisfiable. Consider the function $f(\phi)$ that on input ϕ with variables $x_1, \dots, x_k$ returns $b_1 \dots b_k$ such that $b_i = 1$ iff there is a satisfying assignment to ϕ with $x_i = 1$. This function is in $\mathbf{FP}^{\mathbf{NP}}_{||}$ and hence, by assumption in $\mathbf{FP}^{\mathbf{NP}[\log]}$. Suppose we are given a formula ϕ with exactly 1 satisfying assignment. Then f will return exactly this assignment. Since there are only polynomial many possible answers to the $\log(n)$ queries to **SAT**, one can enumerate all the possible values of f in **P**. We can check that one of the generated values is indeed a satisfying assignment to ϕ. On the other hand if ϕ was unsatisfiable we would not have generated a satisfying assignment, since none exists. □

Theorem 3.6 $\mathbf{FP}^{\mathbf{NP}}_{||} = \mathbf{FP}^{\mathbf{NP}[\log]} \Rightarrow \mathbf{SAT}$ *is $O(\log(n))$-approximable.*

Proof: By Lemma 2.9 we have that $\mathbf{F_{SAT}}$ is m^c enumerable for some c where m is the input length of $\mathbf{F_{SAT}}$. Given any $2c\log(n)$ formulae $\phi_1, \dots, \phi_{2c\log(n)}$ each of size at most n. The size of these $2c\log(n)$ formulae is bounded by $2c\log(n) \times n$ and thus $\mathbf{F}_{SAT}(\phi_1, \dots, \phi_{2c\log(n)})$ is $2^{c\log(2c\log(n)\times n)} < n^{c+1}$ enumerable. Thus one of the n^{2c} vectors for $\mathbf{F_{SAT}}$ has not been enumerated. □

4 Selective and Approximable

The question whether sets that have simple structure could be hard for **NP** dates back to the Berman-Hartmanis conjecture [BH77] and subsequent work by Mahaney for sparse sets [Mah82]. Following sparse sets, the first sets of simple structure to be considered were the **P**-selective sets introduced by [Sel79].

P-selective sets, though of arbitrary complexity, are structurally simple sets. The p-selector function induces an ordering that reduces the number of possible "membership configurations" of two strings. For a **P**-selective set A and two strings x and y either $x \in A \land y \notin A$ or $y \in A \land x \notin A$ is ruled out by the p-selector. This property makes **P**-selective sets structurally as simple as being Turing equivalent to tally sets [Sel82]. Generalizing the structural restriction: "Not all 2^n membership configurations of n strings are possible" has induced many related notions. Among the many notions that pertain to this idea are: **P**-selective sets [Sel79, HHN+95], near-testable sets [GHJY91], k-approximable sets (see below), $(a, b)_p$-recursive sets [KS91], Easily countable sets [HN93], Cheatable sets [Bei87a, BGGO93], $(a, b)_p$-verbose sets [BKS], and Membership comparable sets [Ogi95].

Because of the structural relation between **P**-selective sets and sparse sets, one might not be too surprised that hardness of **P**-selective sets for **NP** is as unlikely as hardness for **NP** of sparse sets. It is quite easy to see that **SAT** itself cannot be **P**-selective unless **P** = **NP**. Buhrman and Torenvliet [BT96b] showed that **SAT** cannot be 1-tt reducible to a **P**-selective set.

Toda [Tod91a], building upon insights provided by Ko [Ko83], proved that in the special case of the existence of only one satisfying assignment, reduction to a **P**-selective set would imply polynomial time decidability. In fact Toda's results hold for the more general k-approximable sets. In this section we cite all results for k-approximable sets. Since **P**-selective sets are k-approximable sets with $k = 2$, all these results also hold for **P**-selective sets. Similar ideas were obtained independently by Beigel [Bei88].

Theorem 4.1 (Beigel-Toda)

1. **P** = **UP** *if and only if* **UP** $\leq^p_{tt}$ **bAPP**.
2. *Unique*-**SAT** $\in$ **P** *if and only if Unique*-**SAT**$_Q$ $\leq^p_{tt}$ **bAPP** *for some Q*.
3. **P** = **NP** *if and only iff* $\Delta^p_2 \leq^p_{tt}$ **bAPP**
4. **P** = **PSPACE** *if and only* **PSPACE** $\leq^p_{tt}$ **bAPP**.
5. **EXP** $\not\leq^p_{tt}$ **bAPP**

The Turing reduction of **bAPP** sets to sparse sets (Theorem 2.3) allows us to apply the famous Karp-Lipton theorem [KL80] showing a collapse of the polynomial-hierarchy if **SAT** is Turing-reducible to a sparse sets.

Theorem 4.2 (Karp-Lipton) *If* **SAT** $\leq^p_T$ **bAPP** *then* **PH** $= \Sigma^p_2$

or in its currently sharpest form proved in [BCG+96, KW95].

Theorem 4.3 (BCGKTKW) *If* **SAT** $\leq^p_T$ **bAPP** *then* **PH** = **ZPP**$^{\mathbf{NP}}$

Both directions of strengthening the consequence of **SAT** $\leq^p_T$ **bAPP** and weakening the reduction type r in **SAT** $\leq^p_r$ **bAPP** $\Rightarrow$ **P** = **NP** are currently the subject of active research. Of course in the present context the latter type is the more interesting. In 1994 a major breakthrough was achieved by three independent sets of authors: Beigel, Kummer and Stephan[BKS95], Agrawal and Arvind[AA96] and Ogihara[Ogi95].

Theorem 4.4 (AABKOS) *If* **SAT** $\leq^p_{btt}$ **bAPP** *then* **P** = **NP**

Or in its currently strongest form

Theorem 4.5 (AABKOS) *If* **SAT** $\leq^p_{n^\alpha-tt}$ *to some k-approximable set for some* $\alpha < \frac{1}{k-1}$ *then* **P** = **NP**.

For **P**-selective sets $k = 2$ and hence $\alpha < 1$ follows.

To understand this result we first show a relationship between reducing to **bAPP** and $r \log n$-approximability.

Theorem 4.6 *If* **SAT** $\leq^p_{n^\alpha-tt}$ *to some k-approximable set for some* $\alpha < \frac{1}{k-1}$ *then* **SAT** *is* $r \log n$ *approximable for some* $r < 1$.

Proof: Note that in Lemma 3.4 the number of vectors is actually bounded by $k \times n^{k-1}$. Hence if we have $r \log n$ formulae $\phi_1, \ldots, \phi_{r \log n}$ we can reduce these to a k-approximable set A via a reduction that produces n^α queries for a total of $(r \log n)n^\alpha < r \times n^\beta$ where $\beta < \frac{1}{k-1}$. Applying Lemma 3.4 gives $(r \times n^\beta)^{k-1}$ vectors including the characteristic vector of these formulae. Hence if $1 > r > \frac{\beta}{k-1}$ we can exclude at least one possibility, which means that **SAT** is $r \log n$-approximable. □

We can then apply the following result from [AA96, BKS95, Ogi95].

Theorem 4.7 (AABKOS) *If* **SAT** *is* $r \log n$*-approximable for some* $r < 1$ *then* **P** = **NP**.

To give a flavor of the proof we prove the following weaker result.

Theorem 4.8 *If* **SAT** *is 2-approximable, then* **P** = **NP**.

Proof: Given a formula ϕ, apply the standard self-reduction to produce four formulae ϕ_1, ϕ_2, ϕ_3, ϕ_4 with the property that ϕ is satisfiable iff at least one of these formulae is satisfiable. Now let f be a 2-approximator and let $f(\phi_1 \vee \phi_2, \phi_1 \vee \phi_3) = (b_1, b_2)$. If $b_1 = b_2 = 0$ then ϕ is satisfiable and we're done. If (b_1, b_2) is $(1, 0)$ then ϕ_2 can not be the only satisfiable formula. If $(b_1, b_2) = (0, 1)$ then ϕ_3 can not be the only satisfiable formula. Finally, if $(b_1, b_2) = (1, 1)$ then ϕ_1 is not satisfiable.

In all cases one formula in the self-reduction can be discarded and the corresponding branch in the self-reduction tree ends. Hence the self-reduction can be expanded always keeping only four formulae in the game. When all remaining self-reduction branches are extended to their full length, satisfiability of ϕ can be decided trivially. □

A polynomial (even fixed) number of queries in Theorem 4.5 is not yet in sight, nor does the proof technique seem to be extendible to obtain such a result. On the other hand there is no known oracle where $\mathbf{P} \neq \mathbf{NP}$ and $\mathbf{SAT} \leq_{tt}^{p}$ **Psel**.

The notion of **P**-selectivity has been extended to other types of selector functions ([HHN+95]) for these (mostly nondeterministic) selector types similar results are known. These are however outside the scope of this paper.

The value $r < 1$ seems to be a real bottleneck of the technique (see [Ogi95] for a discussion) used for the proof, but on the other hand no oracle is known where $\mathbf{P} \neq \mathbf{NP}$ and **SAT** is $O(\log n)$-approximable.

5 $\mathbf{FP}_{||}^{\mathbf{NP}} = \mathbf{FP}^{\mathbf{NP}[\log]}$

At first glance one might think that $\mathbf{FP}_{||}^{\mathbf{NP}} = \mathbf{FP}^{\mathbf{NP}[\log]}$ since this is true for the language classes: $\mathbf{P}_{||}^{\mathbf{NP}} = \mathbf{P}^{\mathbf{NP}[\log]}$ [BH91, Wag90]. Indeed this result yields that $\mathbf{FP}_{||}^{\mathbf{NP}} = \mathbf{FP}^{\mathbf{NP}[\log]}$ when only functions are considered that compute $\log(n)$ output bits (i.e. functions from $\{0,1\}^n$ to $\{0,1\}^{O(\log(n))}$). However $\mathbf{FP}_{||}^{\mathbf{NP}} = \mathbf{FP}^{\mathbf{NP}[\log]}$ implies Unique-**SAT** in **P** and this implies that the polynomial hierarchy collapses (see Section 6). For overview papers on functions classes and related problems see [JT95, JT97, Sel96].

In Lemma 2.9 we saw that $\mathbf{FP}_{||}^{\mathbf{NP}} = \mathbf{FP}^{\mathbf{NP}[\log]}$ is equivalent to $\mathbf{F}_{\mathbf{SAT}}$ being polynomial enumerable. We can use these ideas to get equivalences of $\mathbf{FP}_{||}^{\mathbf{NP}} = \mathbf{FP}^{\mathbf{NP}[\log]}$ to many other hypotheses.

Theorem 5.1 *The following are equivalent:*

- $\mathbf{FP}_{||}^{\mathbf{NP}} = \mathbf{FP}^{\mathbf{NP}[\log]}$
- $\mathbf{FP}_{||}^{\mathbf{NP}} \subseteq \mathbf{FP}^{X[\log]}$ *for some oracle X. [Bei88]*
- $\mathbf{F}_{\mathbf{SAT}}$ *is polynomial enumerable.*
- *Every* **NPSV** *function is polynomial enumerable.*

where **NPSV** is the class of single-valued nondeterministic functions (see [Sel96]).

Some progress has been made on showing the equivalence with $\mathbf{P} = \mathbf{NP}$. Jenner and Toran [JT95] showed that $\mathbf{FP}_{||}^{\mathbf{NP}} = \mathbf{FP}^{\mathbf{NP}[\log]}$ implies that SAT can be computed in less than 2^n time. They also showed that languages recognized by nondeterministic polynomial time machines that make $\log^k(n)$ nondeterministic moves are in **P**.

Theorem 5.2 (Jenner-Toran) *If* $\mathbf{FP}_{||}^{\mathbf{NP}} = \mathbf{FP}^{\mathbf{NP}[\log]}$ *then*

1. $\mathbf{NP} \subseteq \mathbf{DTIME}(2^{n^{O(1/\log\log(n))}})$.
2. $\mathbf{NP}(\log^k(n)) \subseteq \mathbf{P}$.

Buhrman and Fortnow showed that the $\mathbf{FP}_{||}^{\mathbf{NP}} = \mathbf{FP}^{\mathbf{NP}[\log]}$ question can be phrased as a question on resource bounded Kolmogorov complexity [BF97].

Theorem 5.3 (Buhrman-Fortnow) *The following are equivalent:*

1. $\mathbf{CND}^{poly}(x \mid y) \leq \mathbf{C}^{poly}(x \mid y) + O(\log(|x|))$.
2. $\mathbf{CND}^{poly}(x \mid y) \leq \mathbf{CD}^{poly}(x \mid y) + O(\log(|x|))$.
3. $\mathbf{FP}_{||}^{\mathbf{NP}} = \mathbf{FP}^{\mathbf{NP}[\log]}$.

The connection with Kolmogorov complexity enables one to use Theorem 5.2 to prove:

Theorem 5.4 (Buhrman-Fortnow) *If* $\mathbf{FP}_{||}^{\mathbf{NP}} = \mathbf{FP}^{\mathbf{NP}[\log]}$ *then the class of languages accepted by nondeterministic polynomial time machines that have at most $2^{\log^k(n)}$ accepting paths on inputs of length n is included in* **P**.

On the other hand it follows from [Ogi95] that

Theorem 5.5 *If* $\mathbf{FP}_{\beta\log n}^{\mathbf{NP}} \subseteq \mathbf{FP}^{\mathbf{NP}[\alpha\log n]}$ *for some* $1 > \beta > \alpha$ *then* $\mathbf{P} = \mathbf{NP}$.

All the above results have not established the equivalence with $\mathbf{P} = \mathbf{NP}$. We note here that in order to obtain an equivalence it is sufficient to prove that $\mathbf{FP}_{||}^{\mathbf{NP}} = \mathbf{FP}^{\mathbf{NP}[\log]} \Rightarrow \mathbf{P}^{\mathbf{NP}} = \mathbf{P}_{||}^{\mathbf{NP}}$ by the following theorem.

Theorem 5.6

$$\mathbf{P}^{\mathbf{NP}} = \mathbf{P}_{||}^{\mathbf{NP}} \text{ and } \mathbf{FP}_{||}^{\mathbf{NP}} = \mathbf{FP}^{\mathbf{NP}[\log]} \implies \mathbf{P} = \mathbf{NP}$$