Open Problems Column
Edited by William Gasarch
This Issue's Column!

This issue's Open Problem Column is by Lance Fortnow and its titled *Worlds to Die For: Open Oracle Questions for the 21st Century.*

Request for Columns!

I invite any reader who has knowledge of some area to contact me and arrange to write a column about open problems in that area. That area can be (1) broad or narrow or anywhere in between, and (2) really important or really unimportant or anywhere in between.

Worlds to Die Harder For
Open Oracle Questions for the 21st Century

Lance Fortnow

August 18, 2021

Abstract

Most of the interesting open problems about relationships between complexity classes have either been resolved or have relativizable worlds in both directions. We discuss some remaining open questions, updating questions from a similar 1995 survey of Hemaspaandra, Ramachandran and Zimand and adding a few new problems.

1 Introduction

Most of the interesting questions in complexity have relativized worlds in both directions, like whether the polynomial-time hierarchy is infinite [Yao85, Hås89], or whether the Berman-Hartmanis isomorphism conjecture holds [FFK96, BBF98].

Some have questioned the importance of relativization after the non-relativizing techniques of interactive proof systems [FS88, LFKN92]. However these techniques have had limited use and in the thirty years hence we have not seen any significant new non-relativizing techniques and there have been no new examples of theorems that go against previously published relativization results.

For an introduction and defintions of relativization I recommend the original oracle paper by Baker, Gill and Solovay [BGS75], the author's survey on the role of relativization in complexity [For94] and

In 1995, Lane Hemaspaandra, Ajit Ramachandran and Marius Zimand wrote a survey entitled "Worlds to Die For" [HRZ95], giving a list of several open questions about the existence of oracles and random oracles that would make various complexity classes true. We review progress in these questions in Section 5. Even though 26 years have passed, only a few of the problems mentioned by Hemaspaandra et al. have been fully solved showing the vast difficulty of these problems.

2 The Complexity Zoo

The Complexity Zoo [Aar], created by Scott Aaronson, lists most, if not all, of the known complexity classes. For the many classes mentioned in this survey I recommend visiting the zoo if you are unfamiliar with them.

One can use the zoo itself for finding open questions, looking for the minimal classes $\mathcal{C}$ and $\mathcal{D}$ where it is open whether $\mathcal{C} \subseteq \mathcal{D}$ and whether there is an oracle A such that $\mathcal{C}^{\mathcal{A}} \not\subseteq \mathcal{D}^{\mathcal{A}}$.

Robert Sanders [San19] automated this process to generate open questions, such as whether **BQP** has (non-quantum) interactive proofs. Since **BQP** is in **PSPACE** [ADH97], languages in **BQP** have interactive proof systems in the "real world" making the oracle question less interesting. Automating the creation of open questions might reveal some good problems otherwise missed but one needs to carefully check that the problems would reveal new insights into complexity.

3   How to Solve Tough Oracle Questions

Underlying many oracle questions is a combinatorics one. In the most famous example, Yao's paper "Separating the polynomial-time hierarchy by oracle" [Yao85] is heralded more for showing parity doesn't have constant-depth polynomial-size circuits. Some of the oracle questions below, specifically Problems 5.5 and 6.4, are hard because the underlying combinatorial problems are difficult.

Another challenge for oracle constructions are trying to fulfill conflicting requirements. For example in Problem 5.4, we know how to collapse the Boolean hierarchy or make the polynomial-time hierarchy infinite with relativizations but doing both at the same time conflict in ways we don't know how to resolve.

One approach is to create the oracle first and then show it has the right properties. Fenner, Fortnow and Kurtz [FFK94] used this approach to give the first oracle relative to which the Berman-Hartmanis isomorphism conjecture held. The "An Oracle Builders Toolkit" [FFKL03] by Steve Fenner, Lance Fortnow, Stuart Kurtz and Lide Li, explores this approach in detail.

The questions in this survey have stymied the various attempts to settle them and likely some clever new techniques will be needed.

4   The Extremes

These are oracles which push the limits of what we don't know how to prove and of which many other oracle results follow. Pushing these limits further are good open problems.

4.1   P = PSPACE

Discovered by Baker, Gill and Solovay in the original oracle paper [BGS75].

Collapses everything between **P** and **PSPACE**.

$$\mathbf{P} = \mathbf{NP} = \mathbf{coNP} = \mathbf{PH} = \oplus\mathbf{P} = \mathbf{PP} = \mathbf{BQP} = \mathbf{P}^{\#\mathbf{P}} = \mathbf{PSPACE} = \mathbf{NPSPACE}$$

4.2 Generic Oracles

First applied to computational complexity by Blum and Impagliazzo [BI87].

These oracles separate as much as possible. $\mathbf{P} \neq \mathbf{NP}$, the polynomial-time hierarchy is infinite, $\mathbf{PP}$ is not in $\mathbf{P^{NP}}$, $\mathbf{NP}$ is not in $\oplus\mathbf{P}$ and much more. Oddly enough they diagonalize against machines that need to fulfill a promise condition and so with the appropriate construction one also gets $\mathbf{P} = \mathbf{NP} \cap \mathbf{coNP} = \mathbf{UP} = \mathbf{BPP} = \mathbf{BQP}$.

4.3 $\mathbf{P} = \oplus\mathbf{P}$ and $\mathbf{NP} = \mathbf{EXP}$

First proved by Beigel, Buhrman and Fortnow [BBF98].

Relative to this oracle $\mathbf{ZPP} = \oplus\mathbf{EXP}$ and the Berman-Harmanis isomorphism conjecture [BH77] holds (all $\mathbf{NP}$-complete problems are reducible to each other via invertible bijections).

4.4 $\mathbf{P} = \mathbf{NP}$ and $\oplus\mathbf{P} = \mathbf{EXP}$

Discovered by Beigel and Maciel [BM99].

The polynomial-time hierarchy collapses to $\mathbf{P}$ and yet the exponential hierarchy sits inside $\oplus\mathbf{P}$.

4.5 $\mathbf{P} = \oplus\mathbf{P}$ and $\mathbf{BPP} = \mathbf{EXP^{NP}}$

Discovered by Buhrman and Torenvliet [BT00, Corollary 4.8].

No even very weak derandomization for $\mathbf{BPP}$. Valiant-Vazirani puts $\mathbf{NP}$ in $\mathbf{RP^{\oplus P}}$ but in this oracle $\mathbf{NP}$ is not even in $\mathbf{coNP^{\oplus P}}$.

4.6 $\mathbf{P^{RP}} = \mathbf{NEXP}$

Discovered by Buhrman, Fenner, Fortnow and Torenvliet [BFFT01].

No even very weak derandomization for $\mathbf{RP}$. Implies $\mathbf{P^{NP}} = \mathbf{P^{NEXP}}$ (also implied by the next oracle).

4.7 $\mathbf{P^{NP}} = \oplus\mathbf{P} = \mathbf{PEXP}$

A strong version of Beigel's oracle where $\mathbf{P^{NP}}$ is not in $\mathbf{PP}$ [Bei91] (though the entire polynomial-time is in $P^{\mathbf{PP}}$ relative to any oracle [Tod91]) and $\mathbf{PP}$ is not closed under Turing-reductions.

You can replace $\oplus\mathbf{P}$ with $\mathbf{Mod}_k\mathbf{P}$ for any prime k in any of the above. We don't believe any of the statements to be true in the unrelativized world but all of them remain open and would require nonrelativizing techniques to disprove.

5 Updates to Die For

A brief update on the problems asked by Hemaspaandra et al. [HRZ95]. We refer you back to that paper for details on the problems.

5.1 Show that with probability one, the polynomial time hierarchy is proper

Resolved by Håstad, Rossman, Servedio and Tan [HRST17] who showed that a random oracle will, with probability one, separate all the levels of the polynomial-time hierarchy.

5.2 Construct an oracle relative to which $\mathbf{BPTIME}[n] = \mathbf{BPTIME}[n^2]$.

Still open in its full generalization. Rettinger and Verbeek [RV01] show there exists an oracle A such that $\mathbf{BPP}_{tt}^A = \mathbf{BPTIME}_{tt}^A(n)$, equality if the machines only have truth-table (non-adaptive) access to the oracle.

You can get a separation (for all oracles) if you allow the machine a single bit of advice, i.e.,
$\mathbf{BPTIME}(n^2)/1 \neq \mathbf{BPTIME}(n)/1$ (see [FS06]).

5.3 Show that relative to a random oracle there are secure pseudorandom generators

Settled in the affirmative by Marius Zimand [Zim98].

5.4 Build an oracle such that the Boolean Hierarchy collapses yet differs from the polynomial hierarchy

Remains open. We can show that if $\mathbf{P^{NP[1]}} = \mathbf{P^{NP[2]}}$ then $\mathbf{P} = \mathbf{P^{NP}}$ [BF99] and $\mathbf{PH} = \mathbf{S}_2^p \subseteq \mathbf{ZPP^{NP}}$ [FPS08] and these proofs relativize.

Nevertheless there still may be relativized world where $\mathbf{P^{NP[1]}} = \mathbf{P^{NP[2]}}$ and $\mathbf{P^{NP}} \neq \mathbf{ZPP^{NP}}$. To settle 5.4 in the negative, one would need relativizable proofs of the following.

1. Prove the same consequence for any collapse of the Boolean hierarchy, i.e., $\mathbf{P^{NP[k]}} = \mathbf{P^{NP[k+1]}}$ for some k implies $\mathbf{P} = \mathbf{P^{NP}}$ and $\mathbf{PH} = \mathbf{S}_2^p \subseteq \mathbf{ZPP^{NP}}$. I suspect this would follow with a careful analysis of the earlier proofs.

2. Get the final collapse of $\mathbf{ZPP^{NP}}$ to $\mathbf{P^{NP}}$. This would seem to require a new technique.

5.5 Build an oracle relative to which $\mathbf{PP^{\oplus P}} \subsetneq \mathbf{PSPACE}$.

Still open. This question is roughly equivalent to showing that any poly-logarithmic degree polynomial over GF[2] has exponentially-small correlation with Mod_3, or some other problem in $\mathbf{NC}^1$. Jean Bourgain [Bou05] shows exponentially-small correlation for degree slightly less than log. Bhowmick and Lovett [BL15] proposed a potential barrier that could explain the difficulty.

5.6 Build a tally oracle T such that $\mathbf{P}^T \neq \mathbf{NP}^T$.

This one was a bit of a joke in the Hemaspaandra et al. survey as it is equivalent to $\mathbf{P} \neq \mathbf{NP}$ unrelativized. Still open.

5.7 Build an oracle A relative to which SPP has no complete sets.

Resolved in the affirmative. Vereschagin [Ver93] showed that, modulo some technical restrictions, that if there was an oracle making a class $\mathcal{C}$ different than $\mathbf{P}$ and generic oracles collapse $\mathcal{C}$ and $\mathbf{P}$ then there is an oracle where $\mathcal{C}$ does not have complete sets. Fenner, Fortnow, Kurtz and Li [FFKL03] showed these conditions held for $\mathbf{SPP}$.

6 A Few of My Favorite Open Oracle Questions

I've banged my head against the wall on all of these problems. Please help out.

6.1 Build an oracle where UP = NP and the polynomial-time hierarchy is infinite

Suppose for every $\mathbf{NP}$ machine M there is another $\mathbf{NP}$ machine N such that for all x if $M(x)$ has an accepting path then

1. $N(x)$ has a unique accepting path

2. The accepting path of $N(x)$ encodes a single accepting path of $M(x)$.

Hemaspaandra, Naik, Ogihara and Selman [HNOS96] show that under this condition the polynomial-time hierarchy collapses to the second level.

$\mathbf{NP} = \mathbf{UP}$ is similar but doesn't require condition (2), the $\mathbf{UP}$ machine's accepting path may be unrelated to any accepting path of the $\mathbf{NP}$ machine. We don't know if $\mathbf{NP} = \mathbf{UP}$ implies the polynomial-time hierarchy collapses, or a relativized counterexample.

6.2 Build an oracle that separates $\mathbf{S}_2^p$ from $\mathbf{ZPP^{NP}}$

Jin-Yi Cai [Cai07] has a clever proof that $\mathbf{S}_2^p \subseteq \mathbf{ZPP^{NP}}$ and the original $\mathbf{S}_2^p$ paper [RS98] shows $\mathbf{P^{NP}} \subseteq \mathbf{S}_2^p$. Russell and Sundaram [RS98] also give a relativizable proof that $\mathbf{BPP} \subseteq \mathbf{S}_2^p$ which implies an oracle separating $\mathbf{P^{NP}}$ from $\mathbf{S}_2^p$ (follows from 4.5). Whether there is a relativizing proof showing that $\mathbf{ZPP^{NP}} \subseteq \mathbf{S}_2^p$ remains an interesting open problem.

6.3 Build an oracle where the polynomial-time hierarchy looks like the arithmetic hierarchy

We know the structure of the arithmetic hierarchy in computability theory: for all k, $\Sigma_k \neq \Sigma_{k+1}$ and $\Sigma_{k+1} \cap \Pi_{k+1}$ are exactly the languages computable by a Turing machine with an oracle for Σ_k.

Can we create an oracle relative to which the polynomial-time hierarchy has the same structure, i.e., the hierarchy is infinite and $\Sigma_{k+1}^p \cap \Pi_{k+1}^p = \mathbf{P}^{\Sigma_k^p}$ for all $k \geq 0$?

Relative to a generic oracle, the polynomial-time hiearchy is infinite and $\mathbf{P} = \mathbf{NP} \cap \mathbf{coNP}$ [BI87] which suggested that generic oracles could give the oracle for Problem 6.3. Fortnow and Yamakami [FY96] show this isn't true, $\Sigma_{k+1}^p \cap \Pi_{k+1}^p \neq \mathbf{P}^{\Sigma_k^p}$ for $k \geq 1$.

One can generalize this question in uncountably many ways. Let $\alpha = \alpha_0 \alpha_1 \ldots$ be an infinite binary string. Build an oracle relative to which

1. The polynomial-time hierarchy is infinite.

2. For all k,

    (a) If $\alpha_k = 0$ then $\Sigma_{k+1}^p \cap \Pi_{k+1}^p = \mathbf{P}^{\Sigma_k^p}$.

    (b) If $\alpha_k = 1$ then $\Sigma_{k+1}^p \cap \Pi_{k+1}^p \neq \mathbf{P}^{\Sigma_k^p}$.

Problem 6.3 asks to build an oracle for $\alpha = 0000\ldots$. The only solved cases are for generic oracles that satisfy the above for $\alpha = 0111\ldots$ and by straightforward diagonalization for $\alpha = 1111\ldots$ There is no α for which we know no such oracle exists.

On the other hand we can't even rule out a relativizable proof that $\Sigma_2^p \cap \Pi_2^p = \mathbf{P^{NP}}$ implies $\Sigma_2^p = \Pi_2^p$.

6.4 Is P $\neq$ BQP relative to a random oracle?

This is widely believed to be true. If $\mathbf{P} = \mathbf{BQP}$ relative to a random oracle than $\mathbf{BQP} = \mathbf{BPP}$ [FR99], and thus the factoring problem has an efficient probabilistic algorithm.

Consider a variation: If $\mathbf{P} = \mathbf{PSPACE}$ (unrelativized) then $\mathbf{P} = \mathbf{BQP}$ relative to a random oracle. This statement follows from Conjecture 6.1 below about decision tree complexity.

Conjecture 6.1 *For all $p(x_1, \ldots, x_n)$, polynomials of degree d over the reals such that*

1. *For all $(x_1, \ldots, x_n) \in \{0,1\}^n$, $p(x_1, \ldots, x_n) \in [0,1]$.*

2. *For 0.99 fraction of the $(x_1, \ldots, x_n) \in \{0,1\}^n$, $|p(x_1, \ldots, x_n) - 1/2| \geq 1/6$.*

There is a function $f : \{0,1\}^n \to \{0,1\}$ of decision tree complexity polynomial in d and $\log n$ such that for 0.51 fraction of the $(x_1, \ldots, x_n) \in \{0,1\}^n$, $|p(x_1, \ldots, x_n) - f(x_1, \ldots, x_n)| \leq 1/3$.

Aaronson and Ambainis [AA14] give some evidence that Conjecture 6.1 might be false.

6.5 Build an oracle where for all $f \in \#\mathbf{P}$, $\mathbf{P}^f \neq \mathbf{P}^{\mathbf{NP}}$

A language L is checkable if given a program P as an oracle there is a polynomial-time probabilistic algorithm A such that for all x,

1. If $P(x) \neq L(x)$ then $A^P(x)$ outputs "P is wrong on some input".

2. If for all y, $L(y) = P(y)$ then $A^P(x)$ outputs "P is correct on input x."

Blum and Kannan [BK89] show that a language L is checkable if and only if both L and $\overline{L}$ have multi-prover interactive proof systems where the provers are computable in probabilistic polynomial-time with oracle access to L. Early results on interactive proofs imply $\#\mathbf{P}$-complete, $\mathbf{PSPACE}$-complete, $\mathbf{EXP}$-complete and Graph Isomorphism are all checkable among others. Whether $\mathbf{NP}$-complete problems are checkable is still a major open question and boils down to Conjecture 6.2.

Conjecture 6.2 *There is a multi-prover interactive proof system for $\overline{\mathbf{SAT}}$ where the provers are probabilistic polynomial-time with oracle access to $\mathbf{SAT}$.*

We already know Conjecture 6.2 fails relative to an oracle because Fortnow, Rompel and Sipser [FRS94] give an oracle relative to which $\mathbf{coNP}$ has no multi-prover interactive proof no matter how powerful the prover. But this doesn't give much evidence against Conjecture 6.2 since Lund, Fortnow, Karloff and Nisan [LFKN92] show that $\mathbf{coNP}$ does have an interactive proof system.

There is a related complexity conjecture that may, or may not, shed light on the checkability question.

Conjecture 6.3 *Is there a function $f \in \#\mathbf{P}$ such that $\mathbf{P}^f = \mathbf{P}^{\mathbf{NP}}$?*

Even an f such that $\mathbf{NP} \subseteq \mathbf{P}^f \subseteq \mathbf{PH}$ remains open.

One would hope that if such an f existed one could use it as a basis of an interactive proof for $\overline{SAT}$. Unfortunately it's difficult to find an f in $\#\mathbf{P}$ that captures $\mathbf{NP}$ without counting solutions. Trying to find a relativized counterexample seems equally difficult.

Acknowledgments

Thanks to Bill Gasarch who suggested this column, to Lane Hemaspaandra and Marius Zimand for discussions of problems old (Section 5) and new, and to Fred Green for updates on the polynomial questions in Section 5.5. Most of Section 4 first appeared in the author's blog [For05].

References

[AA14]   Scott Aaronson and Andris Ambainis. The need for structure in quantum speedups. *Theory of Computing*, 10(6):133–166, 2014.

[Aar]   S. Aaronson. Complexity Zoo. http://complexityzoo.net.

[ADH97]   L. Adleman, J. DeMarrais, and M. Huang. Quantum computability. *SIAM Journal on Computing*, 26(5):1524–1540, 1997.

[BBF98]   R. Beigel, H. Buhrman, and L. Fortnow. NP might not be as easy as detecting unique solutions. In *Proceedings of the 30th ACM Symposium on the Theory of Computing*, pages 203–208. ACM, New York, 1998.

[Bei91]   R. Beigel. Relativized counting classes: relations among thresholds, parity and mods. *Journal of Computer and System Sciences*, 42(1):76–96, 1991.

[BF99]   H. Buhrman and L. Fortnow. Two queries. *Journal of Computer and System Sciences*, 59(2):182–194, 1999. Special issue for selected papers from the 13th IEEE Conference on Computational Complexity.

[BFFT01] H. Buhrman, S. Fenner, L. Fortnow, and L. Torenvliet. Two oracles that force a big crunch. *Computational Complexity*, 10(2):93–116, 2001.

[BGS75]   T. Baker, J. Gill, and R. Solovay. Relativizations of the P = NP question. *SIAM Journal on Computing*, 4(4):431–442, 1975.

[BH77]   L. Berman and J. Hartmanis. On isomorphism and density of NP and other complete sets. *SIAM Journal on Computing*, 1:305–322, 1977.

[BI87]   M. Blum and R. Impagliazzo. Generic oracles and oracle classes. In *Proceedings of the 28th IEEE Symposium on Foundations of Computer Science*, pages 118–126. IEEE, New York, 1987.

[BK89]   M. Blum and S. Kannan. Designing programs that check their work. In *Proceedings of the 21st ACM Symposium on the Theory of Computing*, pages 86–97. ACM, New York, 1989.

[BL15]   Abhishek Bhowmick and Shachar Lovett. Nonclassical Polynomials as a Barrier to Polynomial Lower Bounds. In David Zuckerman, editor, *30th Conference on Computational Complexity (CCC 2015)*, volume 33 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 72–87, Dagstuhl, Germany, 2015. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik.

[BM99]   R. Beigel and A. Maciel. Circuit lower bounds collapse relativized complexity classes. In *Proceedings. Fourteenth Annual IEEE Conference on Computational Complexity (Formerly: Structure in Complexity Theory Conference) (Cat.No.99CB36317)*, pages 222–226, 1999.

[Bou05]   Jean Bourgain. Estimation of certain exponential sums arising in complexity theory. *Comptes Rendus Mathematique*, 340(9):627–631, 2005.

[BT00]   Harry Buhrman and Leen Torenvliet. Randomness is hard. *SIAM Journal on Computing*, 30(5):1485–1501, 2000.

[Cai07]   J. Cai. $S_2^p \subseteq ZPP^{NP}$. *Journal of Computer and System Sciences*, 73(1):25 − 35, 2007.

[FFK94]   S. Fenner, L. Fortnow, and S. Kurtz. Gap-definable counting classes. *Journal of Computer and System Sciences*, 48(1):116–148, 1994. Special issue for selected papers from the 6th IEEE Structure in Complexity Theory Conference.

[FFK96]   S. Fenner, L. Fortnow, and S. Kurtz. The isomorphism conjecture holds relative to an oracle. *SIAM Journal on Computing*, 25(1):193–206, 1996.

[FFKL03]   S. Fenner, L. Fortnow, S. Kurtz, and L. Li. An oracle builder's toolkit. *Information and Computation*, 182(2):95–136, 2003.

[For94]   L. Fortnow. The role of relativization in complexity theory. *Bulletin of the European Association for Theoretical Computer Science*, 52:229–244, February 1994. Computational Complexity Column.

[For05]   L. Fortnow. Extreme oracles. *Computational Complexity Weblog*, August 2005.

[FPS08]   L. Fortnow, A. Pavan, and S. Sengupta. Proving SAT does not have small circuits with an application to the two queries problem. *Journal of Computer and System Sciences*, 74(3):358–363, May 2008. Special issue for selected papers from the 18th IEEE Conference on Computational Complexity.

[FR99]   L. Fortnow and J. Rogers. Complexity limitations on quantum computation. *Journal of Computer and System Sciences*, 59(2):240–252, 1999.

[FRS94]   L. Fortnow, J. Rompel, and M. Sipser. On the power of multi-prover interactive protocols. *Theoretical Computer Science A*, 134:545–557, 1994.

[FS88]   L. Fortnow and M. Sipser. Are there interactive protocols for co-NP languages? *Information Processing Letters*, 28:249–251, 1988.

[FS06]   L. Fortnow and R. Santhanam. Recent work on hierarchies for semantic classes. *SIGACT News*, 37(3):36–54, September 2006.

[FY96]   L. Fortnow and T. Yamakami. Generic separations. *Journal of Computer and System Sciences*, 52(1):191–197, 1996.

[Hås89]   J. Håstad. Almost optimal lower bounds for small depth circuits. In S. Micali, editor, *Randomness and Computation*, volume 5 of *Advances in Computing Research*, pages 143–170. JAI Press, Greenwich, 1989.

[HNOS96] Lane A. Hemaspaandra, Ashish V. Naik, Mitsunori Ogihara, and Alan L. Selman. Computing solutions uniquely collapses the polynomial hierarchy. *SIAM Journal on Computing*, 25(4):697–708, 1996.

[HRST17] Johan Håstad, Benjamin Rossman, Rocco A. Servedio, and Li-Yang Tan. An average-case depth hierarchy theorem for boolean circuits. *J. ACM*, 64(5), August 2017.

[HRZ95]   Lane A. Hemaspaandra, Ajit Ramachandran, and Marius Zimand. Worlds to die for. *SIGACT News*, 26(4):5–15, December 1995.

[LFKN92] C. Lund, L. Fortnow, H. Karloff, and N. Nisan. Algebraic methods for interactive proof systems. *Journal of the ACM*, 39(4):859–868, 1992.

[RS98]   A. Russell and R. Sundaram. Symmetric alternation captures BPP. *Computational Complexity*, 7(2):152–162, 1998.

[RV01]   Robert Rettinger and Rutger Verbeek. Monte-carlo polynomial versus linear time - the truth-table case. In Rūsiņš Freivalds, editor, *Fundamentals of Computation Theory*, pages 311–322, Berlin, Heidelberg, 2001. Springer Berlin Heidelberg.

[San19]   Jr. Sanders, Robert J. *Complexity Zoology*. PhD thesis, University of California at Davis, 2019. Code and output for expert system at https://rjsworks.wordpress.com/complexity-zoology/. Copyright - Database copyright ProQuest LLC; ProQuest does not claim copyright in the individual underlying works; Last updated - 2020-11-03.

[Tod91] S. Toda. PP is as hard as the polynomial-time hierarchy. *SIAM Journal on Computing*, 20(5):865–877, 1991.

[Ver93] N. Vereshchagin. Relativizable and nonrelativizable theorems in the polynomial theory of algorithms. *Izv. RAN. Ser. Mat.*, 57(2):51–90, 1993.

[Yao85] A. Yao. Separating the polynomial-time hierarchy by oracles. In *Proceedings of the 26th IEEE Symposium on Foundations of Computer Science*, pages 1–10. IEEE, New York, 1985.

[Zim98] Marius Zimand. Efficient privatization of random bits. In Rusins Freivalds, editor, *Randomized Algorithms: Proceedings of International Workshop Brno, Czech Republik, August 27-28*. Electronic Colloquium on Computational Complexity, 1998.