Syracuse University
SURFACE

Electrical Engineering and Computer Science Technical Reports

L.C. Smith College of Engineering and Computer Science

6-20-1990

A Simpler Proof of PH C BP[ΘP]

Kenneth W. Regan
SUNY Buffalo

James S. Royer
Syracuse University

Follow this and additional works at: http://surface.syr.edu/eecs_techreports

Part of the Computer Sciences Commons

Recommended Citation
Regan, Kenneth W. and Royer, James S., "A Simpler Proof of PH C BP[ΘP]" (1990). *Electrical Engineering and Computer Science Technical Reports.* Paper 96.
http://surface.syr.edu/eecs_techreports/96

This Report is brought to you for free and open access by the L.C. Smith College of Engineering and Computer Science at SURFACE. It has been accepted for inclusion in Electrical Engineering and Computer Science Technical Reports by an authorized administrator of SURFACE. For more information, please contact surface@syr.edu.

SU-CIS-90-17

A Simpler Proof of PH $\subseteq$ BP[$\oplus$P]

Kenneth W. Regan
SUNY/Buffalo
regan@cs.buffalo.edu

James S. Royer
Syracuse University
royer@top.cis.syr.edu

June 20, 1990

School of Computer and Information Science
Syracuse University
Suite 4-116
Center for Science and Technology
Syracuse, New York 13244-4100

A Simpler Proof of PH $\subseteq$ BP[$\oplus$P]

Kenneth W. Regan
SUNY/Buffalo
regan@cs.buffalo.edu

James S. Royer
Syracuse University
royer@top.cis.syr.edu

June 20, 1990

Abstract

We simplify the proof by S. Toda [Tod89] that the polynomial hierarchy PH is contained in BP[$\oplus$P]. Our methods bypass the technical quantifier-interchange lemmas in the original proof, and clarify the counting principles on which the result depends. We also show that relative to a random oracle R, PH^R is strictly contained in $\oplus\mathrm{P}^R$.

Keywords Computational complexity, theory of computation, polynomial-time hierarchy, randomness, oracles.

1. Overview

S. Toda [Tod89] defined general BP[$\cdot$] and $\oplus$P[$\cdot$] operators on complexity classes, and proved that PH $\subseteq$ BP[$\oplus$P] through a series of technical lemmas which interleave probability amplification and parity counting arguments. By using relativization we separate and refine these two elements of his proof. We begin by observing that Toda's lemma NP $\subseteq$ BP[$\oplus$P] relativizes to any oracle set. Then we use probability amplification to obtain the following "interchange result": for relativizable complexity classes $\mathcal{A}$ and $\mathcal{C}$ which meet some reasonable polynomial-time closure conditions,

$$\mathcal{A}^{\mathrm{BP}[\mathcal{C}]} \subseteq \mathrm{BP}[\mathcal{A}^{\mathcal{C}}]. \tag{1}$$

Next, by substituting $\oplus$P for both $\mathcal{A}$ and $\mathcal{C}$ in (1), we show that the parity counting argument in Toda's succeeding lemmas is accounted for by the theorem of Papadimitriou and Zachos [PZ83] that $\oplus\mathrm{P}^{\oplus\mathrm{P}} = \oplus\mathrm{P}$. Finally, an induction on k shows that $\Sigma_k^p \subseteq \mathrm{BP}[\oplus\mathrm{P}]$ for all k, completing our presentation of Toda's theorem in Section 3.

We interpret (1) as saying that in fairly common circumstances, explicit access to polynomially many random coin flips is as good as implicit access to exponentially many random coin flips, when the latter have been "precomputed" into an oracle set $L \in \mathrm{BP}[\mathcal{C}]$. In Section 4 we consider a third source of randomness for a computation, namely treating oracle answers themselves as though they are random coin flips. By abstracting an argument of Bennett and Gill [BG81], we show that relative to a random oracle R, $\mathrm{PH}^R \subset \oplus\mathrm{P}^R$. In conclusion we give some related results and open problems.

2. Definitions

Conventions $\mathbf{N}$ denotes the set of natural numbers. We identify each $n \in \mathbf{N}$ with the n-th string of $\{\mathbf{0},\mathbf{1}\}^*$ under lexigraphic ordering. A set A is identified with its characteristic function and predicates are identified with 0–1 valued functions (where $0 \equiv$ false and $1 \equiv$ true). Uppercase roman letters (exclusive of $\mathbf{N}$) are used as variables over subsets of $\mathbf{N}$. For each n, $\mathbf{N}_n$ denotes $\{\mathbf{0},\mathbf{1}\}^n$. $\langle\cdot,\cdot\rangle$ stands for a fixed polynomial-time pairing function, with projection functions π_1 and π_2; the pairing function from Rogers [Rog67] will do. We often write $R(x,y)$ for $R(\langle x,y\rangle)$. For each $z \in \mathbf{N}$ and each $A \subseteq \mathbf{N}$, define $\pi_z(A) := \{\, y : \langle y,z\rangle \in A \,\}$.

Our closure conditions below require a notion of "relativized class" which is finer than the familiar one of a mapping from oracle sets B to classes $\mathcal{A}^B$.

Definition 1. A *relativized set* L is a mapping from sets to sets (i.e., $L\colon 2^{\mathbf{N}} \to 2^{\mathbf{N}}$). L is a *recursive relativized set* if and only if there is an oracle Turing machine (OTM) M such that for each oracle A, $L^A = L(M^A)$ and M^A is total. An *acceptable relativized class* $\mathcal{A}$ is a collection $\{\, L_i : i \in \mathbf{N} \,\}$ of recursive relativized sets. For any oracle set B, we define $\mathcal{A}^B := \{\, L_i^B \,\}$.

We often specify acceptable relativized classes by collections of oracle Turing machines. For example, relativized P can be given by a collection $\{\, P_i \,\}$ of deter-

ministic OTM's such that each P_i is "clocked" to run in some fixed polynomial time independent of the oracle. Relativized NP is given by a similar collection $\{ N_i \}$ of clocked nondeterministic OTM's. If one then defines Q_i to be an OTM which accepts an input x if and only if N_i on input x has an odd number of accepting computations, then the collection $\{ Q_i \}$ gives the standard way of relativizing $\oplus$P.

Definition 2. Suppose $\mathcal{C}$ is a class of sets. A set A belongs to BP[$\mathcal{C}$] if and only if there is an $R \in \mathcal{C}$, a polynomial p, and an $\epsilon > 0$ such that

$$(\forall x)[\,\mathrm{Prob}[\, y \in \mathbf{N}_{p(|x|)} : A(x) = R(x,y)\,] \geq 0.5 + \epsilon\,].$$

For instance, BP[P] is just BPP, and BP[NP] equals L. Babai's class AM of languages having 2-round "Arthur-Merlin games" (cf. [NW88]). The notion of "bounded-error probabilistic parity-P" given by BP[$\oplus$P] is restricted, in that the same polynomial-length sequence of coin flips is used for each branch of a $\oplus$P computation, but this notion suffices for Toda's lemma NP $\subseteq$ BP[$\oplus$P]. Since this restriction is built into the BP[$\cdot$] operator, it seems evident that the following is the correct way to relativize BP[$\mathcal{C}$] in general:

Definition 3. Let $\mathcal{C}$ be an acceptable relativized class. Then for any oracle set X, define 'BP[$\mathcal{C}$] relative to X' to be BP[$\mathcal{C}^X$].

The intuitive point is that so long as a polynomial limit is placed on the number of coin flips allotted, there is no loss of generality in making all the coin flips at the outset. We leave the interested reader to check that for all X, BPP^X (which is usually defined in terms of polynomial-time NOTMs) equals BP[P^X], and AM^X equals BP[NP^X]. In addition, we note (but do not need) that Definition 3 also makes BP[$\mathcal{C}$] an acceptable relativized class—on the condition that for every oracle set X, $\mathcal{C}^X$ contains all finite sets.

Proposition 4. *For any oracle set X,* NP$^X \subseteq$ BP[$\oplus$P^X].

Proof Sketch. Toda's proof of NP $\subseteq$ BP[$\oplus$P] in [Tod89] relies on a general counting argument of L. Valiant and V. Vazirani [VV86], and on the fact that a product of integers is odd iff each factor is odd. It uses no details of specific NP or $\oplus$P

languages. This suffices for an inspection that Toda's proof relativizes to give the stated result. $\square$

The next condition, used by Schöning [Sch87] and Toda, allows one to amplify probabilities to a great extent.

Definition 5. Given sets $A, B \subseteq \mathbf{N}$, we say that A *polynomial-time majority truth-table reduces to* B (written: $A \leq^{\mathrm{p}}_{\mathrm{mtt}} B$) if and only if there is a deterministic polynomial-time precedure which, for each x, constructs a set $S(x)$ of an odd number of strings such that

$$x \in A \iff \text{at least half the strings in } S(x) \text{ are in } B.$$

Proposition 6 ([Sch87]). *Suppose $\mathcal{C}$ is a class of sets which is closed downward under $\leq^{\mathrm{p}}_{\mathrm{mtt}}$. Then, for each $A \in \mathrm{BP}[\mathcal{C}]$ and for each polynomial q there is a set $R \in \mathcal{C}$ and a polynomial p such that*

$$(\forall n)[\,\mathrm{Prob}[\,y \in \mathbf{N}_{p(n)} : (\forall x : |x| \leq n)[\,A(x) = R(x,y)]\,] \geq 1 - 2^{-q(n)}\,].$$

Corollary 7. *If $\mathcal{C}$ is closed downward under $\leq^{\mathrm{p}}_{\mathrm{mtt}}$, then* $\mathrm{BP}[\mathrm{BP}[\mathcal{C}]] = \mathrm{BP}[\mathcal{C}]$.

Definition 8. Let L be a relativized set, and let p be a polynomial. We say that p *bounds the height of L's oracle use* if and only if, for all x and all distinct $A, B \subseteq \mathbf{N}$,

$$|\min(A \triangle B)| > p(|x|) \Longrightarrow L^A(x) = L^B(x).$$

A class $\mathcal{A}$ of relativized sets has *polynomially bounded oracle use* if and only if, for each $L \in \mathcal{A}$, there is a polynomial p that bounds the height of L's oracle use.

Definition 9. Suppose $\mathcal{A}$ is a class of relativized sets. We say that $\mathcal{A}$ is *closed under oracle projections* if and only if, for all $X \subseteq \mathbf{N}$ and each $A \in \mathcal{A}$, there is an $\widehat{A} \in \mathcal{A}$ such that, for all $x, z \in \mathbf{N}$,

$$\widehat{A}^X(x,z) = A^{\pi_z(X)}(x).$$

Furthermore, $\mathcal{A}$ is closed under *uniform* oracle projections if $\widehat{A}$ can be the same for all oracle sets X.

To see what is happening in this last definition, think of A and $\widehat{A}$ as being computed by OTMs M and $\widehat{M}$, respectively. Then $\widehat{M}^X$ on input $\langle x, z\rangle$ simulates M^X on input x, *except* that whenever M would make an oracle query y, $\widehat{M}$ makes the query $\langle y, z\rangle$ instead. For well-behaved relativized classes $\mathcal{A}$ such as P and $\oplus$P, this simulation (which resembles the *S-m-n property*; cf. [Rog67]) doesn't depend on X itself. However, we only know how to make relativized BPP closed under (nonuniform) oracle projections, owing to the apparent lack of well-behaved oracle BPP-machines. In point of fact we do not need such uniformity for the proofs in this paper.

Lemma 10. *Relativized* P *and* $\oplus$P *are closed under uniform oracle projections and have polynomially bounded oracle use. For any oracle set* X, P^X *and* $\oplus\mathrm{P}^X$ *are closed downward under* $\leq^{\mathrm{p}}_{\mathrm{mtt}}$, *and in fact under* $\leq^{\mathrm{p}}_{\mathrm{T}}$.

Proof Sketch. The first two statements follow from properties of the OTMs $\{ P_i \}$ for P and $\{ Q_i \}$ for $\oplus$P given above. The last statement for $\oplus$P follows on observing that the proof given by Papadimitriou and Zachos [PZ83] relativizes to yield: for all oracle sets X, $\oplus\mathrm{P}^{\oplus\mathrm{P}^X} = \oplus\mathrm{P}^X$. $\square$

3. Main Result

We may now state and prove our key counting argument.

Proposition 11. *Suppose* $\mathcal{A}$ *is a class of relativized sets which is closed under oracle projections and which has polynomially bounded oracle use.*

Suppose $\mathcal{C}$ *is a class of sets closed downward under* $\leq^{\mathrm{p}}_{\mathrm{mtt}}$*-reductions.*

Then, $\mathcal{A}^{\mathrm{BP}[\mathcal{C}]} \subseteq \mathrm{BP}[\mathcal{A}^{\mathcal{C}}]$.

Proof. Suppose that A is in $\mathcal{A}$ and that B is in $\mathrm{BP}[\mathcal{C}]$. We show that A^B is in $\mathrm{BP}[\mathcal{A}^{\mathcal{C}}]$.

Suppose p is a polynomial that bounds A's oracle use. Since $\mathcal{C}$ satisfies the hypotheses of Proposition 6, it follows that there is a $C \in \mathcal{C}$ and a polynomial q such that, for all n,

$$\mathrm{Prob}[\, z \in \mathbf{N}_{q(n)} : (\forall y : |y| \leq n)[B(y) = C(y, z)]\,] \geq 3/4. \tag{2}$$

For each n, define

$$Z_n := \{\, z \in \mathbf{N}_{q(p(n))} : (\forall y : |y| \leq p(n))[B(y) = C(y,z)] \,\}. \tag{3}$$

By (2) we have that, for all n,

$$\frac{\|Z_n\|}{\|\mathbf{N}_{q(p(n))}\|} \geq 3/4. \tag{4}$$

Since p bounds A's oracle use, it follows from (3) that, for all x,

$$(\forall z \in Z_{|x|})[\, A^B(x) = A^{\pi_z(C)}(x) \,].$$

Hence, by (4), for all x,

$$\mathrm{Prob}[\, z \in \mathbf{N}_{q(p(|x|))} : A^B(x) = A^{\pi_z(C)}(x) \,] \geq 3/4. \tag{5}$$

Now since $\mathcal{A}$ is closed under oracle projections, there is an $\widehat{A} \in \mathcal{A}$ such that for all $x, y \in \mathbf{N}$, $\widehat{A}^C(x,z) = A^{\pi_z(C)}(x)$. So, we can restate (5) as

$$\mathrm{Prob}[\, z \in \mathbf{N}_{q(p(|x|))} : A^B(x) = \widehat{A}^C(x,z) \,] \geq 3/4. \tag{6}$$

Since $\widehat{A} \in \mathcal{A}$ and $C \in \mathcal{C}$, we have that A^B is in $\mathrm{BP}[\mathcal{A}^{\mathcal{C}}]$. □

An immediate corollary is the known result that $\mathrm{BPP}^{\mathrm{BPP}} = \mathrm{BPP}$. Our proof of Toda's theorem now goes through quickly.

Theorem 12 ([Tod89]). $\mathrm{PH} \subseteq \mathrm{BP}[\oplus\mathrm{P}]$.

Proof. By Proposition 4, we have that for all oracle sets X, $\mathrm{NP}^X \subseteq \mathrm{BP}[\oplus\mathrm{P}^X]$. Hence

$$\begin{aligned}
\mathrm{NP}^{\mathrm{NP}} &\subseteq \mathrm{BP}[\oplus\mathrm{P}^{\mathrm{NP}}] \\
&\subseteq \mathrm{BP}[\oplus\mathrm{P}^{\mathrm{BP}[\oplus\mathrm{P}]}] && \text{(since } \mathrm{NP} \subseteq \mathrm{BP}[\oplus\mathrm{P}]) \\
&\subseteq \mathrm{BP}[\mathrm{BP}[\oplus\mathrm{P}^{\oplus\mathrm{P}}]] && \text{(by Proposition 11)} \\
&\subseteq \mathrm{BP}[\mathrm{BP}[\oplus\mathrm{P}]] && \text{(by [PZ83])} \\
&\subseteq \mathrm{BP}[\oplus\mathrm{P}] && \text{(by Corollary 7).}
\end{aligned}$$

By iterating this argument, the theorem follows. □

We remark that this proof establishes that $\mathrm{BP}[\oplus\mathrm{P}^{\mathrm{BP}[\oplus\mathrm{P}]}] = \mathrm{BP}[\oplus\mathrm{P}]$, which is somewhat stronger than the lemma $\mathrm{BP}[\oplus\mathrm{P}[\mathrm{BP}[\oplus\mathrm{P}]]] = \mathrm{BP}[\oplus\mathrm{P}]$ in Toda's paper. If $\mathcal{D}$ is a relativized class which "incorporates $\leq_{\mathrm{T}}^{\mathrm{P}}$ reductions" in the sense that $\mathcal{D}^{\mathrm{P}^X} = \mathcal{D}^X$ for all X, then we have

$$\mathcal{D}^{\mathrm{BPP}^{\mathcal{C}}} = \mathcal{D}^{\mathrm{BP}[\mathrm{P}^{\mathcal{C}}]} \subseteq \mathrm{BP}[\mathcal{D}^{\mathrm{P}^{\mathcal{C}}}] = \mathrm{BP}[\mathcal{D}^{\mathcal{C}}]. \tag{7}$$

Hence $\oplus\mathrm{P}^{\mathrm{BPP}^{\oplus\mathrm{P}}} = \mathrm{BP}[\oplus\mathrm{P}]$, and also $\mathrm{BPP}^{\oplus\mathrm{P}} = \mathrm{BP}[\oplus\mathrm{P}]$. This gives us equality in Proposition 11 in the case $\mathcal{A} = \mathcal{C} = \oplus\mathrm{P}$. We do not have good general conditions under which equality holds.

Last, we observe that the proof of Theorem 12 relativizes in a straightforward manner to give:

Corollary 13. *For any oracle set X, $\mathrm{PH}^X \subseteq \mathrm{BP}[\oplus\mathrm{P}^X]$.* □

4. Random Oracles

The following is essentially an abstraction of the proof of Theorem 5 in [BG81]. Let μ be the standard Lebesgue measure on $2^{\mathbf{N}}$ (see [Rog67]); this is analogous to, but not the same as, the standard measure on the real interval $[0,1]$. All the oracle properties we consider are first-order definable, so that the subsets of $2^{\mathbf{N}}$ they define are Borel, and hence measurable. Say a property $\Psi(\cdot)$ *holds relative to a random oracle R* if and only if $\mu(\{\, R \subseteq \mathbf{N} : \Psi(R) \,\}) = 1$.

For short in the proof, we say that a TM M "has the strong-BP property for an input x and polynomials p, q" if $\mathrm{Prob}[\, y \in \mathbf{N}_{p(|x|)} : M(x,y) \,]$ is either less than $2^{-q(|x|)}$ or greater than $1 - 2^{-q(|x|)}$.

Theorem 14. *Let $\mathcal{C}$ be an acceptable relativized class which has polynomial bounded oracle use, such that for all X, $\mathcal{C}^X$ is closed downward under $\leq_{\mathrm{T}}^{\mathrm{P}}$ reductions and has X itself as a member. Then for a random oracle set R, $\mathrm{BP}[\mathcal{C}^R] \subseteq \mathcal{C}^R$.*

Proof. Let $\{\, Q_i \,\}$ be a representation of $\mathcal{C}$ by OTMs with corresponding polynomial bounds $\{\, r_i \,\}$ on their oracle use. For every i and polynomial p_j, let M_{ij} be an OTM which behaves as follows, for any input x and oracle X:

Make queries to the first $p_j(|x|)$ strings of length $r_i(|x| + p_j(|x|)) + 1$ and call the 0–1 string of results y.

Simulate Q_i^X on input $\langle x, y\rangle$.

Although the relativized language accepted by M_{ij} need not belong to relativized $\mathcal{C}$, it is true that for all oracle sets A, $L(M_{ij}^A) \in \mathcal{C}^A$, because $L(M_{ij}^A)$ $\leq_{\mathrm{T}}^{\mathrm{p}}$-reduces to the disjoint union of A and $L(Q_i)^A$. (Remark: It does not seem possible to obtain a $\leq_{\mathrm{tt}}^{\mathrm{p}}$-reduction here.)

Now let $k > 0$. For all i, j, and x define E_{ijx} to be the set of oracles A such that Q_i^A enjoys the strong-BP property for x and the polynomials p_j and $q(|x|) := 2|x| + i + j - k$, *but* M_{ij}^A on input x disagrees with the answer of the overwhelming majority for $Q_i^A(x, y)$. Because Q_i never queries those strings which are used by M_{ij} to obtain the bits for y, $\mu(E_{ijx}) \leq 2^{-q(|x|)}$. Hence we have

$$\mu(\cup_{ijx} E_{ijx}) \leq \sum_{ijx} \mu(E_{ijx}) \leq \sum_{ijx} 2^{-k} \cdot 2^{-i-j-2|x|} = \sum_{ijn} 2^{-k} \cdot 2^{-i-j-n} < 2^{-k}.$$

Now let $A \notin \cup_{ijx} E_{ijx}$. We claim that $\mathrm{BP}[\mathcal{C}^A] = \mathcal{C}^A$. Let $L \in \mathrm{BP}[\mathcal{C}^A]$. Since $\mathcal{C}^A$ is closed downwards under $\leq_{\mathrm{mtt}}^{\mathrm{p}}$ reductions, there is a polynomial p_j and a machine Q_i such that $\mathrm{Prob}[\, y \in \mathbf{N}_{p_j(|x|)} : L(x) = Q_i^A(x, y)\,] \geq 1 - 2^{-3|x|}$. Hence for all x such that $|x| \geq i + j - k$, Q_i^A enjoys the strong-BP property for x, p_j, and $i + j - k + 2|x|$, and so by choice of A, $M_{ij}^A(x) = L(x)$. Hence, L differs at most finitely from the language $L(M_{ij}^A)$, and so $L \in \mathcal{C}^A$. This proves the claim.

Since 2^{-k} can be made arbitrarily small, we conclude that the collection of oracle sets A such that $\mathrm{BP}[\mathcal{C}^A] = \mathcal{C}^A$ has measure 1. □

Corollary 15. *Relative to a random oracle R, PH^R is strictly contained in $\oplus\mathrm{P}^R$.*

Proof. From Theorem 14, we have that $\mathrm{PH}^R \subseteq \oplus\mathrm{P}^R$ for a random oracle set R. J. Cai's proof in [Cai86] establishes that for a random oracle set R, $\oplus\mathrm{P}^R$ is not contained in PH^R. □

Definition 16 ([NW88]). For any relativized class $\mathcal{C}$, *Almost*$[\mathcal{C}]$ denotes the class of languages L such that $\mu(\{\, A \subseteq \mathbf{N} : L \in \mathcal{C}^A \,\}) = 1$.

Corollary 17. $\mathrm{BP}[\oplus\mathrm{P}] \subseteq \mathit{Almost}[\oplus\mathrm{P}]$.

Whether equality holds here runs into the problem that a single relativized $\oplus$P computation may access exponentially many bits of the oracle, whereas the BP[$\oplus$P] computations have only polynomially many coin flips. The relativized $\oplus$P computations can be modeled by depth-2 circuits whose bottom level is a single parity gate. It is interesting to ask whether these can be "fooled" by strong pseudorandom generators which generate exponentially many bits from a polynomial-length random seed, along the lines of [NW88] for relativized PH computations.

Open Problem. *Does* $\mathrm{BP}[\oplus\mathrm{P}] = \mathit{Almost}[\oplus\mathrm{P}]$*?*

A positive answer would yield yet another proof of $\mathrm{PH} \subseteq \mathrm{BP}[\oplus\mathrm{P}]$ using random oracle sets R, via $\mathrm{NP}^{\mathrm{NP}} \subseteq \mathrm{BP}[\oplus\mathrm{P}^{\mathrm{BP}[\oplus\mathrm{P}]}] = \mathrm{BP}[\oplus\mathrm{P}^{\oplus\mathrm{P}^R}] = \mathrm{BP}[\oplus\mathrm{P}^R] = \oplus\mathrm{P}^R = \mathrm{BP}[\oplus\mathrm{P}]$.

Last, we remark that under the "Random Oracle Hypothesis" of [BG81], PH would be (strictly) contained in $\oplus$P. Our initial reaction is to disbelieve this even somewhat more than the hypothesis BPP = P. It is interesting to ask how these two assertions are related. In conclusion, we hope that our results add understanding to the effect of sources of randomness in polynomial-time computations.

Acknowledgments. We would like to thank Richard Beigel, Ronald Book, and Seinosuke Toda for helpful comments and suggestions on this work.

References

[BG81] C. Bennett and J. Gill. Relative to a random oracle A, $\mathrm{P}^A \neq \mathrm{NP}^A \neq \mathrm{coNP}^A$ with probability 1. *SIAM Journal on Computing*, 10:96–113, 1981.

[Cai86] J. Cai. With probability one, a random oracle separates pspace from the polynomial-time hierarchy. In *The Proceedings of the 18th Annual ACM Symposium on the Theory of Computing*, pages 21–29, 1986.

[NW88] N. Nisan and A. Wigderson. Hardness vs. randomness. In *The Proceedings of the 29th Annual IEEE Symposium on Foundations of Computer Science*, pages 2–11, 1988.

[PZ83] C. H. Papadimitriou and S. Zachos. Two remarks on the power of counting. In *The 6th GI Conference on Theoretical Computer Science*, Lecture Notes in Computer Science No. 145, pages 269–276. Springer-Verlag, 1983.

[Rog67] H. Rogers. *Theory of Recursive Functions and Effective Computability.* McGraw-Hill, 1967. Reprinted. MIT Press. 1987.

[Sch87] U. Schöning. Probabilistic complexity classes and lowness. In *The Proceedings of the 2nd Annual IEEE Structure in Complexity Theory Conference*, pages 2–8, 1987.

[Tod89] S. Toda. On the computational power of PP and $\oplus$P. In *The Proceedings of the 30th Annual IEEE Symposium on Foundations of Computer Science*, pages 514–519, 1989.

[VV86] L. Valiant and V. Vazirani. NP is as easy as detecting unique solutions. *Theoretical Computer Science*, 47:85–93, 1986.