# MEASURE ONE RESULTS IN COMPUTATIONAL COMPLEXITY THEORY[1]

*Heribert Vollmer and Klaus W. Wagner*

Theoretische Informatik, Universität Würzburg, Am Exerzierplatz 3,
D-97072 Würzburg, Germany

## 1 INTRODUCTION

Starting with Bennet and Gill's seminal paper [13] a whole new research line in complexity theory was opened: the examination of relativized complexity theoretic statements which hold for a measure one set of oracles in the measure defined by putting each string into the oracle with probability $\frac{1}{2}$ independent of all other strings (a formal definition is given below).

Bennet and Gill were concerned with the subtlety of the $\mathrm{P} \overset{?}{=} \mathrm{NP}$ question pointed out in a paper by Baker, Gill, and Solovay [8] where oracles $A$ and $B$ were exhibited such that $\mathrm{P}^A = \mathrm{NP}^A$ but $\mathrm{P}^B \neq \mathrm{NP}^B$. However since these two oracles are of a very "intentional nature" [59], Bennet and Gill wanted to examine the relation between P and NP relative to an oracle which is produced "at random." They showed that $\mathrm{P}^A \neq \mathrm{NP}^A$ for a measure one set of oracles $A$. In their own words: "Relative to a random oracle $A$, $\mathrm{P}^A \neq \mathrm{NP}^A \neq \mathrm{coNP}^A$ with probability 1" [13]. Since then results of this form have been called "random oracle results" in complexity theory. What we want to point out here is that this term does not refer to *algorithmically random languages* in the sense of Martin-Löf [65]. To avoid confusion, results as the one by Bennet and Gill should better be referred to as "measure one results". This however does not deny that there are certain relations among measure one oracle sets and the set of algorithmically random oracles as will be pointed out in the next section.

Though there are a lot of beautiful and compelling results along this line the status of measure one oracle sets, especially in connection with the so called *Random Oracle Hypothesis*, is still unclear. This hypothesis, as stated by Bennett and Gill, claims that every statement holding for a measure one set of oracles also holds in the unrelativized world. In the meantime however it turned out that this does not hold. What we will show is that even a much more restricted formulation of the hypothesis is false.

[1] This paper is dedicated to Ronald V. Book on the occasion of his 60th birthday.

In this survey we want to make the reader familiar with this kind of approach to relativized computation. We do not claim that this paper is a comprehensive compilation of all results relevant to the subject matter—it is just a presentation of some results which to the authors seem to be interesting and important.

## 2 MEASURE AND ALGORITHMIC RANDOMNESS

We start with the basic questions *how to define a measure on sets of oracles* and *how to define a random language.* Let $\{0,1\}^*$ denote the set of finite binary words, whereas $\{0,1\}^\omega$ denotes the set of infinite binary words. Using the lexicographic ordering of $\{0,1\}^*$, there is a natural bijection between $\{0,1\}^*$ and the set $\mathbb{N}$ of natural numbers, and in fact we identify the elements of $\{0,1\}^*$ and $\mathbb{N}$ in this way. Furthermore, we identify a language $A \subseteq \{0,1\}^* \cong \mathbb{N}$, with its characteristic sequence $A(0)A(1)A(2)A(3)\cdots \in \{0,1\}^\omega$ where $A(i) = 1$ if $i \in A$ and $A(i) = 0$ otherwise. For $w \in \{0,1\}^*$ we denote the $i$-th bit of $w$ by $w(i)$.

For a set $W \subseteq \{0,1\}^*$ and a class $X \subseteq \{0,1\}^\omega$ define $W \cdot X =_{\text{def}} \left\{ w\xi \;\middle|\; w \in W \text{ and } \xi \in X \right\}$, where $w\xi$ is the infinite sequence which is obtained by simply concatenating $w$ and $\xi$. In particular, we set $C_w =_{\text{def}} \{w\} \cdot \{0,1\}^\omega$, the *basic open set* defined by $w$, and $\mathbf{D} =_{\text{def}} \left\{ W \cdot \{0,1\}^\omega \;\middle|\; W \subseteq \{0,1\}^* \text{ is finite} \right\}$. $\mathbf{D}$ is the class of all *open* sets. A *closed* set is the complement of an open set. Observe that $\mathbf{D}$ contains $\emptyset$ and is closed under union and complement, hence forms an algebra. On $\mathbf{D}$ we define a measure as follows: Given $W \subseteq \{0,1\}^*$, define $W'$ to consist of all words $v \in W$ for which there is no proper prefix $w \sqsubset v$ in $W$. Now,

$$\mu\left[W \cdot \{0,1\}^\omega\right] = \mu\left[W' \cdot \{0,1\}^\omega\right] = \mu\left[\bigcup_{w \in W'} C_w\right] =_{\text{def}} \sum_{w \in W'} \left(\frac{1}{2}\right)^{|w|}.$$

This measure can be extended in the obvious way to the smallest $\sigma$-algebra containing $\mathbf{D}$, i.e., the closure of $\mathbf{D}$ under countable union and countable intersection.

An alternative way to get the same measure is first to start with the measure $\mu_0 \colon 2^{\{0,1\}} \to [0,1]$ which is defined by $\mu_0(\{0\}) = \mu_0(\{1\}) = \frac{1}{2}$ and then define $\mu \colon 2^{\{0,1\}^\omega} \to [0,1]$ to be the product measure based on $\mu_0$.

Let $H(A)$ be an expression in $A$. To simplify the notation, we will in the following sometimes use $\mu_A\left[H(A)\right]$ as a shorthand for $\mu\left[\left\{ A \;\middle|\; H(A) \right\}\right]$. In the case that $\mu_A\left[H(A)\right] = 1$ we will also say that $H(A)$ is true for almost all $A$.

Similar to the above, we define some $\mathcal{C} \subseteq \{0,1\}^\omega$ to be *recursively open,* if $\mathcal{C} = W \cdot \{0,1\}^\omega$ for some recursively enumerable set $W \subseteq \{0,1\}^*$. A set is *recursively closed,* if it is the complement of some recursively open set. A set $\mathcal{C}$ is *recursively* $\mathrm{G}_\delta$, if $\mathcal{C} = \bigcap_{i=1}^\infty \mathcal{C}_i$ where the $\mathcal{C}_1, \mathcal{C}_2, \ldots$ are recursively open. A set $\mathcal{C}$ is *recursively* $\mathrm{F}_\sigma$, if $\mathcal{C}$ is the complement of a set which is recursively $\mathrm{G}_\delta$.

In the following, we assume an effective enumeration of the recursively enumerable languages as $W_1, W_2, W_3, \ldots$. Now we say that a class $\mathcal{C}$ is a *constructive null set* if there is a total recursive function $g$ with the properties that for every $k$,

1. $\mathcal{C} \subseteq W_{g(k)} \cdot \{0,1\}^\omega$ and
2. $\mu\left[W_{g(k)} \cdot \{0,1\}^\omega\right] \leq 2^{-k}$.

Note that a constructive null set has measure zero in the above sense.

Let NULL be the union of all constructive null sets, and define RAND $=_{\text{def}}$ $\{0,1\}^\omega$ $-$ NULL to be the class of *algorithmically random languages*. This definition is due to Martin-Löf [65] (cf. also [62, Section 2.5]).

Since NULL is a countable union of measure 0 sets, we have $\mu\,[\text{NULL}] = 0$ and hence $\mu\,[\text{RAND}] = 1$. This simple observation can be strengthened in the following way [24, 20, 57, 26]. We say that a class $\mathcal{C}$ is closed under finite variations if whenever $A \in \mathcal{C}$ and $A$ and $B$ have a finite symmetric difference $A \bigtriangleup B$ then also $B \in \mathcal{C}$. The Kolmogorov 0-1-Law says that every measurable set that is closed under finite variations has either measure 0 or measure 1. Now we have:

**Lemma 2.1 [26].** *If $\mathcal{C}$ is in the $\sigma$-algebra (i.e., the closure under complementation and countable intersection) over the class of all recursivly $G_\delta$ sets which are closed under finite variation, then the following are equivalent:*

*(1)* $\mu\,[\mathcal{C}] > 0$.

*(2)* $\mu\,[\mathcal{C}] = 1$.

*(3)* RAND $\cap\, \mathcal{C} \neq \emptyset$.

*(4)* RAND $\subseteq \mathcal{C}$.

If will be our aim in the upcoming sections to apply Lemma 2.1 to certain sets of oracles which are attached to machines and complexity classes. We assume the reader is familiar with basic complexity theory notions, classes and reducibilities, see e.g. [10, 9, 56, 71].

Let $\{M_i\}_{i\in\mathbb{N}}$ be a recursive enumeration of all oracle Turing machines. Let $M_i^A(x)$ be the result of $M_i$'s work on input $x$ and oracle $A$ if this computation stops, and let $M_i^A(x)$ be undefined otherwise. Define $L(M_i) =_{\text{def}} \left\{ (A, x) \;\middle|\; M_i^A(x) = 1 \right\}$ and $L(M_i^A) =_{\text{def}} \left\{ x \;\middle|\; M_i^A(x) = 1 \right\}$.

A class $\mathcal{K}^{(\cdot)} \subseteq 2^{\{0,1\}^\omega \times \{0,1\}^*}$ is a *recursively presentable relativized class* or for short, *relativized class* if and only if there exists a recursive function $f$ such that

- $M_{f(j)}^A(x) \in \{0,1\}$ for every $j, x, A$.
- $\mathcal{K}^{(\cdot)} = \left\{ L(M_{f(j)}) \;\middle|\; j \in \mathbb{N} \right\}$.

Define $\mathcal{K}^A =_{\text{def}} \left\{ L(M^A_{f(j)}) \mid j \in \mathbb{N} \right\}$ and $\mathcal{K} =_{\text{def}} \mathcal{K}^{\emptyset}$. If no confusion is possible we also use $\mathcal{K}$ instead of $\mathcal{K}^{(\cdot)}$; particularly we do so if we emphasize that $\mathcal{K}$ is a relativized class. We say that a relativized class $\mathcal{K}$ is *invariant under finite variations of the oracle,* if and only if $\mathcal{K}^A = \mathcal{K}^B$ for every $A, B \in \{0,1\}^\omega$ which have a finite symmetric difference.

If was shown in [24] that if $\mathcal{K}$ is a recursively presentable relativized class which is invariant under finite variations of the oracle, then for any $i \in \mathbb{N}$ the set $\left\{ A \mid L(M^A_i) \notin \mathcal{K}^A \right\}$ is recursively $G_\delta$ and closed under finite variations. Thus we get immediately from the above lemma the following Theorem:

**Theorem 2.2 [26].** *Let $\mathcal{K}_1, \mathcal{K}_2$ be relativized classes which are closed under finite variations of the oracle. Then the following are equivalent:*

1. $\mu_A \left[\mathcal{K}^A_1 \subseteq \mathcal{K}^A_2\right] > 0$.
2. $\mu_A \left[\mathcal{K}^A_1 \subseteq \mathcal{K}^A_2\right] = 1$.
3. $\mathcal{K}^A_1 \subseteq \mathcal{K}^A_2$ *for some random oracle* $A$.
4. $\mathcal{K}^A_1 \subseteq \mathcal{K}^A_2$ *for all random oracles* $A$.

An important tool when considering measure in complexity theory is the Lebesgue Density Theorem (see e.g. [66, Lemma 5]). The following is a formulation which is useful for our purposes.

**Theorem 2.3** *Let $\mathcal{C} \subseteq \{0,1\}^\omega$ be measurable and $\mu\,[\mathcal{C}] > 0$. For every $\delta < 1$ there is an $\alpha \in \{0,1\}^*$ such that $\mu_A\,[\alpha A \in \mathcal{C}] \geq \delta$.*

The Lebesgue Density Theorem is typically applied as follows (cf. e.g. [75, Theorem 13.XIV on p. 272] or [69, Fact on p. 163]): Suppose you have a statement $\Phi(i, A)$ about the $i$-th machine of a relativized class $\mathcal{K} = \{L(M_{f(i)}) \mid i \in \mathbb{N}\}$ and the oracle $A$ such that $\mu_A\,[\Phi(i, A)] > 0$. Theorem 2.3 now yields for every $\delta < 1$ a prefix $\alpha$ such that $\mu_A\,[\Phi(i, \alpha A)] \geq \delta$. Thus, if it is possible to find a $j \in \mathbb{N}$ such that $M^A_{f(j)}(x) = M^{\alpha A}_{f(i)}(x)$ for all $x$ then $\mu_A\,[\Phi(j, A)] \geq \delta$.

## 3 MEASURE ONE SEPARATIONS

Research in computational complexity on random oracles and measure one oracle sets was started by the seminal 1981 paper by Bennet and Gill [13]. They proved that for almost all oracles $A$,

$$\mathrm{P}^A \neq \mathrm{NP}^A \neq \mathrm{coNP}^A.$$

We want to give a (very simplified) outline of their proof argument, since it suggests a somewhat general approach which has been used later quite a number of times to obtain similar random oracle separations. So suppose we consider two relativized classes $\mathcal{K}_1$ and $\mathcal{K}_2$ and we want to show that $\mathcal{K}^A_2 \not\subseteq \mathcal{K}^A_1$ for almost all oracles $A$.

*Step 1:* Choose a test language $L^A$ depending on the oracle $A$ such that $L^A \in \mathcal{K}_2^A$ for all oracles $A$.

It will be our aim to prove $L^A \notin \mathcal{K}_1^A$ for almost all oracles $A$. For this, we use the following observation which though it looks like a minor technical point is essential for the argumentation in [13] and a lot of the subsequent papers. If $L^A$ and a chosen recursive presentation $M_{f(0)}, M_{f(1)}, M_{f(2)}, \ldots$ of $\mathcal{K}_1$ fulfill some minor requirements (conditions 1–4 in [13]), then the following holds:

**Lemma 3.1 (Bennet and Gill's Lemma 1).** *If there exists a constant* $\epsilon > 0$ *such that* $\mu_A \left[L^A \neq L(M^A_{f(i)})\right] > \epsilon$ *for every* $i \in \mathbb{N}$, *then* $\mu_A \left[L^A \notin \mathcal{K}_1^A\right] = 1$.

Observe that the lemma actually states that a certain form of quantifier swapping is possible: From

$$(\exists \epsilon)(\forall i)\mu_A \left[L^A \neq L(M^A_{f(i)})\right] > \epsilon$$

one can conclude

$$(\exists \epsilon)\mu_A \left[(\forall i)(L^A \neq L(M^A_{f(i)}))\right] > \epsilon$$

(and thus by the Kolmogorov 0-1-Law this latter probability is actually 1); thus in a sense the quantifiers $\forall$ and $\mu$ swap.

Now we go on as follows:

*Step 2:* Show that $\mu_A \left[M^A_{f(i)} \text{ makes a mistake deciding the test language } L^A\right] > \epsilon$ for all $i \in \mathbb{N}$ and a universal $\epsilon > 0$.

This second step is of course the main combinatorial difficulty in the overall argument, and this is where the proofs of different separations have to diverge and make use of particular properties of the considered classes.

In some cases, Step 2 is reduced to a related result about boolean circuits making use of a connection between Turing machines and circuits first established by Furst, Saxe, and Sipser [44] (see also [93] and the comprehensive presentation in [48, Chapter 7]).

Let us now mention some specific results:

**Theorem 3.2 [13].** $\mu_A \left[\mathrm{P}^A \neq \mathrm{NP}^A \neq \mathrm{coNP}^A\right] = 1$.

*Proof outline.* Define

$$\mathrm{RANGE}^A =_{\mathrm{def}} \left\{ x \;\middle|\; \text{there is a } y \text{ s.t. } A(y1)A(y10)A(y100)\cdots A(y10^{|y|-1}) = x \right\}.$$

Clearly, $\mathrm{RANGE}^A \in \mathrm{NP}^A$, thus the complement $\mathrm{CORANGE}^A$ is always in $\mathrm{coNP}^A$. Appealing to their Lemma 1, Bennet and Gill then show that every NP machine has an input on which it errs for an oracle set with measure at least one third. ❑

Using notions from resource bounded measure (see e.g. [64]), this result has been improved in [58].

Now we relate time and space complexity classes. Note that throughout this paper relativized space complexity classes are defined by oracle machines where the space bound also applies to the oracle tape (the so called *bounded query model* [31]).

**Theorem 3.3 [13].** *1.* $\mu_A\left[\text{LOGSPACE}^A \subset \text{P}^A\right] = 1.$

*2.* $\mu_A\left[\text{PSPACE}^A \subset \text{EXPTIME}^A\right] = 1.$

Considering alternating Turing machines the just given theorem was improved by Orponen in [70] as follows: It is well known from [37] that alternating logspace ALOGSPACE equals P, alternating polynomial time AP equals PSPACE, alternating polynomial space APSPACE equals EXPTIME, etc. Under the bounded query model the equality of AP and PSPACE is relativizable (trivially, it does not hold in the unrestricted model where longer queries are allowed for PSPACE), while the other two equalities are not [31]. The following can even be shown:

**Theorem 3.4 [70].** *1.* $\mu_A\left[\text{ALOGSPACE}^A \subset \text{P}^A\right] = 1.$

*2.* $\mu_A\left[\text{APSPACE}^A \subset \text{EXPTIME}^A\right] = 1.$

Let PH be the class of all sets in the polynomial time hierarchy [67, 92, 56]. Cai proved in [33] that PH is properly included in PSPACE for almost all oracles, but in fact he proved the stronger result which appears as the following theorem. Let #P be the class of all counting functions, i.e the class of all functions $f$ such that there exists a nondeterministic polynomially time bounded machine $M$ such that $f(x)$ is the number of accepting paths of $M$ on input $x$ [86]. Let further $\oplus$P be the class of those sets $L$ for which there exists some $f \in \#\text{P}$ such that $x \in L \Leftrightarrow f(x) \equiv 1 \pmod 2$ [72].

**Theorem 3.5 [33].** $\mu_A\left[\oplus \text{P}^A \not\subseteq \text{PH}^A\right] = 1.$

*Proof outline.* The test language is

$$\text{Parity}^A =_{\text{def}} \left\{ 1^n \;\middle|\; \text{there is an odd number of strings of length } n \text{ in } A \right\},$$

which is certainly in $\oplus \text{P}^A$. For step 2, Cai proved that all constant depth circuit families of unbounded fan-in AND and OR gates err on approximately half of their inputs when computing the parity function. His proof relies on a very sophisticated extension of Furst, Saxe and Sipser's random restriction technique. ❑

A generalization is the following:

**Theorem 3.6** *For all* $k \geq 2$, $\mu_A\left[\text{Mod}_k\,\text{P} \not\subseteq \text{PH}^A\right] = 1.$

*Proof outline.* The generalization from $\oplus$P to for $\text{Mod}_k\,\text{P}$, $k \geq 3$ is more or less immediate from [33, Corollary 4.3]. ❑

Since $\oplus \text{P}^A \subseteq \text{PSPACE}^A$ for all oracles $A$ we obtain:

**Corollary 3.7 [33].** $\mu_A\left[\text{PH}^A \subset \text{PSPACE}^A\right] = 1.$

Corollary 3.7 was later proved in a somewhat more direct way in [6]. This corollary can even be strengthened. Let QBF denote the satisfiability problem for quantified boolean formulae, and let $A \oplus B$ be the marked union of the sets $A$ and $B$. Relativized classes of the form $\mathrm{P}^{(\cdot)\oplus\mathrm{QBF}}$, $\mathrm{NP}^{(\cdot)\oplus\mathrm{QBF}}$, and $\mathrm{PH}^{(\cdot)\oplus\mathrm{QBF}}$ were studied in [15, 28]. The corresponding machines are called *bounded query machines*, since they can be thought of as PSPACE machines with restricted oracle access. The following consequence of Cai's proof was noted by Book (a weaker statement was proved earlier by Kurtz in [59]):

**Theorem 3.8 [18].** $\mu_A \left[\mathrm{PH}^{A\oplus\mathrm{QBF}} \subset \mathrm{PSPACE}^{A}\right] = 1.$

Let $\mathrm{NP}(k)$ be the $k$-th class of the Boolean hierarchy (take as one of the many possible definitions $\mathrm{NP}(1) =_{\mathrm{def}} \mathrm{NP}$ and $\mathrm{NP}(k+1) =_{\mathrm{def}} \left\{ A \triangle B \;\middle|\; A \in \mathrm{NP}(k) \text{ and } B \in \mathrm{NP} \right\}$), and let BH be the union of all classes of the Boolean hierarchy (see e.g. [34]).

**Theorem 3.9 [32].** $\mu_A \left[\mathrm{NP}(1)^A \subset \mathrm{NP}(2)^A \subset \mathrm{NP}(3)^A \subset \cdots\right] = 1.$

The proof of Theorem 3.9 combines a technique from [35] used to construct *some* oracle relative to which the boolean hierarchy does not collapse together with the result of Bennet and Gill (Theorem 3.2) for the base case.

It is known that (relative to all oracles) both a collapse of the boolean hierarchy or a collapse of PSPACE to PH implies that there are only a finite number of different levels in the polynomial time hierarchy. The converse is not known. Thus Corollary 3.7 and Theorem 3.9 leave open the possibility that for almost all oracles the polynomial time hierarchy is finite. This question is unresolved so far. (However, see Corollary 8.5 below.)

The following corollaries are consequences of Theorem 3.9.

**Corollary 3.10 [32].** $\mu_A \left[\mathrm{BH}^A \textit{ has no } \leq_m^p \textit{-complete language}\right] = 1.$

For $k \geq 2$ let $\Theta_k^p = \mathrm{LOGSPACE}^{\Sigma_{k-1}^p}$ [91].

**Corollary 3.11 [32].** $\mu_A \left[\mathrm{BH}^A \subset \Theta_2^{p,A}\right] = 1.$

Now we turn to measure one relations between different counting classes. Let FP denote the class of all (deterministically) polynomial time computable functions. Let PP denote the class of those sets $A$ for which there exist functions $f \in \#\mathrm{P}$ and $g \in \mathrm{FP}$ such that $x \in A \iff f(x) \geq g(x)$ [45, 79, 90].

**Theorem 3.12 [4].** $\mu_A \left[\oplus \mathrm{P}^A \not\subseteq \mathrm{PP}^A\right] = 1.$

*Proof outline.* Again, the test language $\mathrm{Parity}^A$ is used. Voting polynomials (introduced in [4] as a new lower bound technique) are used to establish that any probabilistic polynomial-time machine will fail for a non measure zero oracle set on a typical input $x$ when deciding $x \in \mathrm{Parity}^A$. ❑

Since $\oplus\mathrm{P}^A \subseteq \mathrm{P}^{\mathrm{PP}^A}$ for all oracles $A$ we obtain:

**Corollary 3.13** $\mu_A\left[\mathrm{PP}^A \subset \mathrm{P}^{\mathrm{PP}^A}\right] = 1.$

Let $\mathrm{C}_=\mathrm{P}$ denote the exact counting class [79, 90]; i.e. $\mathrm{C}_=\mathrm{P}$ consists of those sets $A$ for which there exist functions $f \in \#\mathrm{P}$ and $g \in \mathrm{FP}$ such that $x \in A \iff f(x) = g(x)$.

**Corollary 3.14** $\mu_A\left[\mathrm{C}_=\mathrm{P}^A \neq \mathrm{coC}_=\mathrm{P}^A\right] = 1$

*Proof.* Relative to any oracle $A$, $\mathrm{C}_=\mathrm{P}^A \subseteq \mathrm{PP}^A$ [12], and $\mathrm{C}_=\mathrm{P}^A = \mathrm{coC}_=\mathrm{P}^A$ implies $\mathrm{C}_=\mathrm{P}^A = \mathrm{P}^{\mathrm{PP}^A}$ [46]. Thus the statement follows from Corollary 3.13. ❑

Since $\mathrm{PH}^A$ and $\mathrm{PP}^A$ are closed under complement we conclude from the preceding corollary:

**Corollary 3.15** $\mu_A\left[\mathrm{PH}^A \neq \mathrm{C}_=\mathrm{P}^A\right] = 1.$

**Corollary 3.16** $\mu_A\left[\mathrm{C}_=\mathrm{P}^A \subset \mathrm{PP}^A\right] = 1.$

Finally we mention a few examples involving interactive protocols. We do not present the definitions here; the reader who is unfamiliar with the relevant notions might want to consult a textbook (for instance [73] or Chapters 13 and 19 in [71]).

Arora et al. [3] (see also [81]) gave a characterization of NP in terms of so called *probabilistically checkable proof systems*. As claimed in [47] this does not hold with random oracles. (In a relativized PCP, the verifier has access to the oracle.)

**Theorem 3.17 [47].** $\mu_A\left[\mathrm{PCP}^A(\log n, 1) \subset \mathrm{NP}^A\right] = 1.$

The power of *interactive proofs* as a game theoretical model for computation was not clear for a long time. The basic class in this context, IP, was known to be a subclass of PSPACE (relativizably), but oracles were known relative to which even coNP is not included in IP [43]. Using the test language $\mathrm{Parity}^A$ Chang et al. in [38] separated IP from PSPACE for almost all oracles. In fact, they were even able to improve this by showing that the non-containment of coNP in IP holds for almost all oracles. On the other hand, Shamir obtained the surprising result that IP $=$ PSPACE [78]. This was the first non-relativizable result in complexity theory that attained considerable attention.

**Theorem 3.18 [38].** $\mu_A\left[\mathrm{coNP}^A \not\subseteq \mathrm{IP}^A\right] = 1$, *thus* $\mu_A\left[\mathrm{IP}^A \subset \mathrm{PSPACE}^A\right] = 1.$

As a side remark, when we consider the class IPP of *unbounded* interactive proofs, which is defined like IP but the verifier is a PP machine rather than a BPP machine, then we have that IPP $=$ PSPACE for all oracles [38]. This is also true if the verifier is a coNP machine [7].

**Separability and Immunity.** Bennet and Gill also showed in their 1981 paper that $\mathrm{NP}^A$ contains a $\mathrm{P}^A$-immune set (i.e. an infinite set which has no infinite subset in $\mathrm{P}^A$) for almost all oracles $A$. This was later extended by Vereshchagin [88], who showed that NP$^A$ contains a coNP$^A$-immune set (i.e. an infinite set which has no infinite subset in coNP$^A$) for almost all oracles $A$. Moreover, Vereshchagin proved that there are two disjoint NP$^A$ sets which are not separable by a P$^A$ set for almost all oracles $A$. Other structural properties of NP which hold for almost all oracles are investigated in [27].

**Separating Reducibilities.** The above given results on separating complexity classes can of course always be interpreted as results on showing that certain reducibilities differ on almost all sets. For a reducibility $\leq_y^x$ and a set $A$, let $\mathcal{R}_y^x(A)$ be the class of all sets reducible to $A$ via $\leq_y^x$. Then we have as consequences of Theorem 3.3:

**Corollary 3.19 [13].** *1.* $\mu_A\left[\mathcal{R}_T^{log}(A) \subset \mathcal{R}_T^p(A)\right] = 1.$

*2.* $\mu_A\,[\mathcal{R}_T^{pspace}(A) \subset \mathcal{R}_T^{exp}(A)] = 1.$

Some more results along these lines, requiring new proofs with sometimes combinatorially involved arguments, are the following. Let $\leq_{tt}^p$ denote the polynomial time truth table reducibility. For a function $r\colon \mathbb{N} \longrightarrow \mathbb{N}$, let $\leq_{r\text{-tt}}^p$ ($\leq_{r\text{-T}}^p$, resp.) denote that restriction of $\leq_{tt}^p$ ($\leq_T^p$), where the number of queries is bounded by $r(|x|)$ for input $x$. In particular, the function $r$ can be a constant. Finally, let the bounded truth table reducibility $\leq_{btt}^p$ be the union of all $\leq_{k\text{-}tt}^p$ for constants $k \geq 1$.

**Theorem 3.20** *1.* $\mu_A\left[\mathcal{R}_{k\text{-}tt}^p(A) \subset \mathcal{R}_{(k+1)\text{-}tt}^p(A)\right] = 1$ *for every* $k \geq 1$ [82, 22].

*2.* $\mu_A\left[\mathcal{R}_{btt}^p(A) \subset \mathcal{R}_{\log\text{-T}}^p(A)\right] = 1$ [66].

*3.* $\mu_A\,[\mathcal{R}_{tt}^p(A) \subset \mathcal{R}_T^p(A)] = 1$ [66].

**The Isomorphism Conjecture.** Berman and Hartmanis in 1977 were lead to the conjecture that any two sets complete for NP under polynomial time many-one reductions are actually isomorphic in a strong sense (i.e. under a polynomial time computable and polynomial time invertible isomorphism). In [60] it was shown that this conjecture is false for almost all oracles.

## 4 RELATIVIZABLE INCLUSIONS

If an inclusion $\mathcal{K}_1 \subseteq \mathcal{K}_2$ between relativizable complexity classes holds *relativizably*, i.e. for all oracles, then trivially it holds for almost all oracles. Interestingly, there is an often very simple to use criterion to establish such relativizable relations, if the relevant classes are definable in a certain way.

In the leaf language approach to the characterization of complexity classes, the acceptance of a word input to a nondeterministic machine depends only on the values printed at the leaves of the computation tree. To be more precise, let $M$ be a nondeterministic Turing machine, halting on every path, with some order on the nondeterministic choices. Then, leafstring$^M(x)$ is the concatenation of the symbols printed at the leaves of the computation tree of $M$ on input $x$. Call a computation tree of a machine $M$ *balanced*, if all of its computation paths have the same length, and moreover, if we identify every path with the string over $\{0, 1\}$ describing the sequence of nondeterministic choices on this path, then there is some string $z$ such that all paths $y$ with $|y| = |z|$ and $y \leq z$ (in lexicographic ordering) exist, but no such path with $y > z$ exists. Now given a language $B$ (a so called *leaf language*), this language defines the class $\text{Leaf}^{\text{P}}(B)$ of all languages $L$ for which there exists a nondeterministic polynomial time machine $M$ whose computation tree is always balanced, such that $x \in L \iff \text{leafstring}^{M}(x) \in B$. (In the literature the above classes are often denoted by $\text{BalancedLeaf}^{\text{P}}(B)$. However since we will only be talking about the balanced case we chose to keep the notation as simple as possible.) Since the definition of the class $\text{Leaf}^{\text{P}}(B)$ is based on nondeterministic polynomial time machines its relativization $\text{Leaf}^{\text{P}}(B)^{A}$ to an oracle $A$ can be defined in an obvious mannner.

This computation model was introduced by Bovet, Crescenzi, and Silvestri [29, 30] and Vereshchagin [89], and it was later examined among others by Hertrampf, Lautemann, Schwentick, Vollmer, and Wagner [50], and Jenner, McKenzie, and Thérien [55].

The following basic technical result in connection with leaf language definability was proved by Bovet, Crescenzi, and Silvestri [30] and independently by Vereshchagin [89]: Let $B_1$ and $B_2$ be two leaf languages. Say that $B_1$ is polylogarithmically bit-reducible to $B_2$ (in symbols: $B_1 \leq_m^{plt} B_2$) via the reduction function $f$ iff every bit of $f(x)$ can be computed in a time polylogarithmically in $|x|$ by a deterministic machine (with random access input tape). For an exact definition, see [30, 50].

**Theorem 4.1 [30, 89].** *For all languages* $B_1$ *and* $B_2$,

$$B_1 \leq_m^{plt} B_2 \iff \text{Leaf}^{\text{P}}(B_1)^{A} \subseteq \text{Leaf}^{\text{P}}(B_2)^{A} \textit{ for all oracles } A$$

To show that there is an oracle separating $\text{Leaf}^{\text{P}}(B_1)$ and $\text{Leaf}^{\text{P}}(B_2)$ we thus have to show that $B_1$ is not reducible to $B_2$ in the above sense. Thus Theorem 4.1 turns out to be a criterion which reduces the construction of oracles with certain properties to purely combinatorial arguments, avoiding the stage construction diagonalization which often underlies oracle separations.

Building on this criterion a lot of remarkable results have been obtained; e.g. several interesting characterizations of classes as PSPACE [50, 55] and PP [52], an algorithm to detect whether two so called bounded counting classes are separable by an oracle [49, 39], the identification of all relativizable functional closure properties of $\#\text{P}$ [51], and even (unconditional) separations of circuit classes [36].

Certainly it would be very nice to have a criterion similar to Theorem 4.1 for measure one inclusions, and in fact this wish inspired some of the research reported in the next section and eventually led to Corollary 5.4 below, which allows one to conclude from a certain relativizable inclusion that a related measure one inclusion holds.

## 5 MEASURE ONE COLLAPSES

Bennett and Gill not only separated complexity classes relative to almost all oracles (see Theorems 3.2 and 3.3), but they also showed that relative to almost all oracles some unexpected inclusions hold. For example, they proved that for almost all oracles deterministic polynomial time is as powerful as bounded error probabilistic polynomial time.

**Theorem 5.1 [13].** $\mu_A\left[\mathrm{P}^A = \mathrm{BPP}^A\right] = 1$

Let us generalize this result. For a class $\mathcal{K}$ of languages and a function $h\colon \{0,1\}^* \to \mathbb{N}$ define $\mathrm{BP}_h \cdot \mathcal{K}$ as the class of all languages $L$ for which there exists an $L' \in \mathcal{K}$ such that $\#\left\{ z \;\middle|\; |z| = h(|x|) \wedge (x \in L \leftrightarrow (x,z) \in L') \right\} \geq \frac{2}{3} \cdot 2^{h(|x|)}$. Define $\mathrm{BP}^{\mathrm{p}} \cdot \mathcal{K}$ ($\mathrm{BP}^{\mathrm{exp}} \cdot \mathcal{K}$, resp.) as the class of languages $L$ for which there exists a polynomial $p$ such that $L \in \mathrm{BP}_p \cdot \mathcal{K}$ ($L \in \mathrm{BP}_{2^p} \cdot \mathcal{K}$, resp.). Say that $\mathcal{K}$ has the *polynomial amplification property*, iff $L \in \mathrm{BP}^{\mathrm{p}} \cdot \mathcal{K}$ iff for every polynomial $q$ there exist a polynomial $p$ and some $L' \in \mathcal{K}$ such that $\#\left\{ z \;\middle|\; |z| = p(|x|) \wedge (x \in L \leftrightarrow (x,z) \in L') \right\} \geq (1 - 2^{-q(|x|)}) \cdot 2^{p(|x|)}$. It is known that $\mathcal{K}$ has the polynomial amplification property if it is closed under majority reductions which is a special case of positive reductions (see [76]). Analogously we say that $\mathcal{K}$ has the *exponential amplification property*, iff $\mathrm{BP}^{\mathrm{exp}} \cdot \mathcal{K}$ is the class of all sets $L$ such that for every polynomial $q$ there exist a polynomial $p$ and some $L' \in \mathcal{K}$ such that $\#\left\{ z \;\middle|\; |z| = 2^{p(|x|)} \wedge (x \in L \leftrightarrow (x,z) \in L') \right\} \geq (1 - 2^{-q(|x|)}) \cdot 2^{2^{p(|x|)}}$. Since most of the time it is clear from the context what we are talking about we will omit the prefix *polynomial* and *exponential*.

Because of $\mathrm{BPP}^A = \mathrm{BP}^{\mathrm{p}} \cdot \mathrm{P}^A$ for every oracle $A$, Theorem 5.1 says that the class $\mathrm{P}^A$ is a fixpoint of the operator $\mathrm{BP}^{\mathrm{p}}$ for almost all oracles $A$. The question is whether this is true for a greater variety of complexity classes. The answer is affirmative, even if the operator $\mathrm{BP}^{\mathrm{exp}}$ is considered rather than $\mathrm{BP}^{\mathrm{p}}$.

**Theorem 5.2 [26].** *For every relativized class $\mathcal{K}$ such that $\mathcal{K} = \mathrm{Leaf}^{\mathrm{P}}(B)$ for some recursive language $B$ and $\mathcal{K}$ has the amplification property,*

$$\mu_A\left[\mathcal{K}^A = \mathrm{BP}^{\mathrm{exp}} \cdot \mathcal{K}^A\right] = 1.$$

**Corollary 5.3 [26].** *For all relativized classes $\mathcal{K}_1$ and $\mathcal{K}_2$ such that $\mathcal{K}_2 = \mathrm{Leaf}^{\mathrm{P}}(B)$ for some recursive language $B$ and $\mathcal{K}_2$ has the amplification property,*

$$\mu_A\left[\mathcal{K}_1^A \subseteq \mathcal{K}_2^A\right] = \mu_A\left[\mathcal{K}_1^A \subseteq \mathrm{BP}^{\mathrm{exp}} \cdot \mathcal{K}_2^A\right].$$

*In particular,*

$$\mu_A\left[\mathcal{K}_1^A \subseteq \mathcal{K}_2^A\right] = 1 \Leftrightarrow \mu_A\left[\mathcal{K}_1^A \subseteq \mathrm{BP}^{\mathrm{exp}} \cdot \mathcal{K}_2^A\right] = 1$$

*and*

$$\mu_A\left[\mathcal{K}_1^A \not\subseteq \mathcal{K}_2^A\right] = 1 \Leftrightarrow \mu_A\left[\mathcal{K}_1^A \not\subseteq \mathrm{BP}^{\mathrm{exp}} \cdot \mathcal{K}_2^A\right] = 1.$$

**Corollary 5.4** *Let $\mathcal{K}_1$ and $\mathcal{K}_2$ be relativized classes such that $\mathcal{K}_2 = \mathrm{Leaf}^{\mathrm{P}}(\mathrm{B})$ for some recursive language* B *and $\mathcal{K}_2$ has the amplification property. If $\mathcal{K}_1^A \subseteq \mathrm{BP}^p \cdot \mathcal{K}_2^A$ for all oracles* A *then $\mu_A\left[\mathcal{K}_1^A \subseteq \mathcal{K}_2^A\right] = 1$.*

The latter corollary allows a number of applications. For $k \geq 2$, let $\mathrm{Mod}_k\,\mathrm{P}$ be the class of those sets $A$ for which there exists some $f \in \#\mathrm{P}$ such that $x \in A \iff f(x) \not\equiv 0 \pmod{k}$ [11]. Note that $\mathrm{Mod}_2\,\mathrm{P} = \oplus\,\mathrm{P}$.

**Theorem 5.5** *1.* $\mu_A\left[\mathrm{PH}^A \subset \oplus\,\mathrm{P}^A\right] = 1$ [74].

*2.* $\mu_A\left[\mathrm{PH}^A \subset \mathrm{Mod}_p\,\mathrm{P}^A\right] = 1$ *for every prime* $p \geq 3$.

*3.* $\mu_A\left[\mathrm{PH}^A \subset \mathrm{C_{=}P}^A \subset \mathrm{PP}^A\right] = 1$.

*Proof.* The inclusions follow from Corollary 5.4 and the relativizable results $\mathrm{PH} \subseteq \mathrm{BP}^p \cdot \oplus\,\mathrm{P}$ [84], $\mathrm{PH} \subseteq \mathrm{BP}^p \cdot \mathrm{Mod}_k\,\mathrm{P}$ for $k \geq 3$ [85], and $\mathrm{PH} \subseteq \mathrm{BP}^p \cdot \mathrm{C_{=}P}$ [85]. Note that for $\mathrm{Mod}_k\,\mathrm{P}$ the amplification property is known to hold only if $k$ is prime. The properness of the inclusions follows from Theorem 3.6, Corollary 3.15, and Corollary 3.16. ❑

Observe that the proper inclusion $\mu_A\left[\mathrm{PH}^A \subset \mathrm{PP}^A\right] = 1$ yields as a corollary Cai's measure one separation of PH and PSPACE (Corollary 3.7).

The preceding theorem can be generalized as follows: Let GapP be the class of all functions which can be written as the difference of two $\#\mathrm{P}$ functions, i.e. GapP $=$ #P $-$ #P [41]. Let $\mathrm{GapP}^A = \#\mathrm{P}^A - \#\mathrm{P}^A$. Let B be any subset of $\mathbb{Z}$. Then $\mathcal{R}_m^{\mathrm{GapP}}(B)$ is the GapP many-one reducibility closure of B, i.e. $L \in \mathcal{R}_m^{\mathrm{GapP}}(B)$ if and only if there exists some $f \in$ GapP such that $x \in L \iff f(x) \in B$ for all $x$. For an oracle $A$, we write $\mathcal{R}_m^{\mathrm{GapP}^A}(B)$ for the $\mathrm{GapP}^A$ many-one reducibility closure of B.

**Theorem 5.6** *Let $\emptyset \subset B \subset \mathbb{Z}$ be such that $\mathcal{R}_m^{\mathrm{GapP}}(B)$ has the amplification property. Then*

$$\mu_A\left[\mathrm{PH}^A \subseteq \mathcal{R}_m^{\mathrm{GapP}^A}(B)\right] = 1.$$

*Proof.* This follows from the inclusion $\mathcal{R}_m^{\mathrm{GapP}^{\mathrm{PH}}}(B) \subseteq \mathrm{BP}^p \cdot \mathcal{R}_m^{\mathrm{GapP}}(B)$ given in [85], which turns out to be relativizable. ❑

Finally, we give two more applications of Corollary 5.4. Let AM be Babai's *Arthur-Merlin class* [5].

**Theorem 5.7** $\mu_A\left[\mathrm{NP}^A = \mathrm{AM}^A\right] = 1$

*Proof.* This follows from the representation $\mathrm{AM} = \mathrm{BP}^p \cdot \mathrm{NP}$, see e.g. [76]. ❑

Let US be class of those sets $A$ for which there exists some $f \in \#\mathrm{P}$ such that $x \in A \iff f(x) = 1$ [14]. Let $\mathcal{R}_{dtt}^p$ denote polynomial time disjunctive truth table reducibility.

**Theorem 5.8 [26].** $\mu_A \left[ {\Theta_2^p}^A = \mathcal{R}_{dtt}^p(\mathrm{US})^A \right] = 1$

*Proof.* In [87] it is shown that every NP set (and hence every $\mathrm{NP}(2)$ set) can be randomly reduced to a US set. Unfortunately, US is not known to have the amplification property. However, it is easy to see that $\mathcal{R}_{dtt}^p(\mathrm{US})$ has this property. Hence, $\mathrm{NP}(2) \subseteq \mathrm{BP}^p \cdot \mathcal{R}_{dtt}^p(\mathrm{US})$ and, consequently, $\Theta_2^p = \mathcal{R}_{dtt}^p(\mathrm{NP}(2)) \subseteq \mathcal{R}_{dtt}^p(\mathrm{US})$. ❑

Some of the inclusions and separations between complexity classes holding for a measure one set of oracles given in the preceding sections are subsumed in Figure 1.

## 6 ALMOST-Classes

ALMOST-classes are classes which are just defined by a measure-one condition.

**Definition 6.1** Let $\mathcal{K}$ be a recursively presentable relativized class. Then we say that a language $L$ belongs to ALMOST-$\mathcal{K}$ if and only if $\mu_A \left[ L \in \mathcal{K}^A \right] = 1$.

There are very different characterizations of the ALMOST-operator and ALMOST-classes. We start with a characterization using random languages in the sense of Martin-Löf. Let REC denote the class of all recursive sets.

**Theorem 6.2 [24].** *If $\mathcal{K}$ is a relativized class which is closed under finite variations of the oracle, then*

$$\text{ALMOST-}\mathcal{K} = \mathcal{K}^{\mathrm{RAND}} \cap \mathrm{REC},$$

*i.e.* ALMOST-$\mathcal{K}$ *coincides with the class of recursive sets that are in $\mathcal{K}^A$ for some random language $A$.*

An extension of this result is given by Book as follows:

**Theorem 6.3 [20].** *Let $\mathcal{K}$ be a relativized class which is closed under finite variations of the oracle.*

1. *For every* $B \in \mathrm{RAND}$, ALMOST-$\mathcal{K} = \mathcal{K}^B \cap \mathrm{REC}$.
2. *For every pair of languages* $A, B$ *such that* $A \oplus B \in \mathrm{RAND}$,

$$\text{ALMOST-}\mathcal{K} = \mathcal{K}^A \cap \mathcal{K}^B.$$

Statement 2 is a generalization of a result by Lutz [63] where the special case $\mathcal{K} = \mathrm{P}$ was proved.

An intuitive account of these results is the following: If we have a set $B \in \mathrm{RAND}$, there is so much irregularity (non-recursiveness) in $B$ that a $\mathcal{K}$ machine (when forced to operate recursive in its overall behaviour) cannot retrieve much sensible information from B—all we get is ALMOST-$\mathcal{K}$ which is presumably very close to $\mathcal{K}$.

More results along these lines can be found in [17, 23, 25, 40].

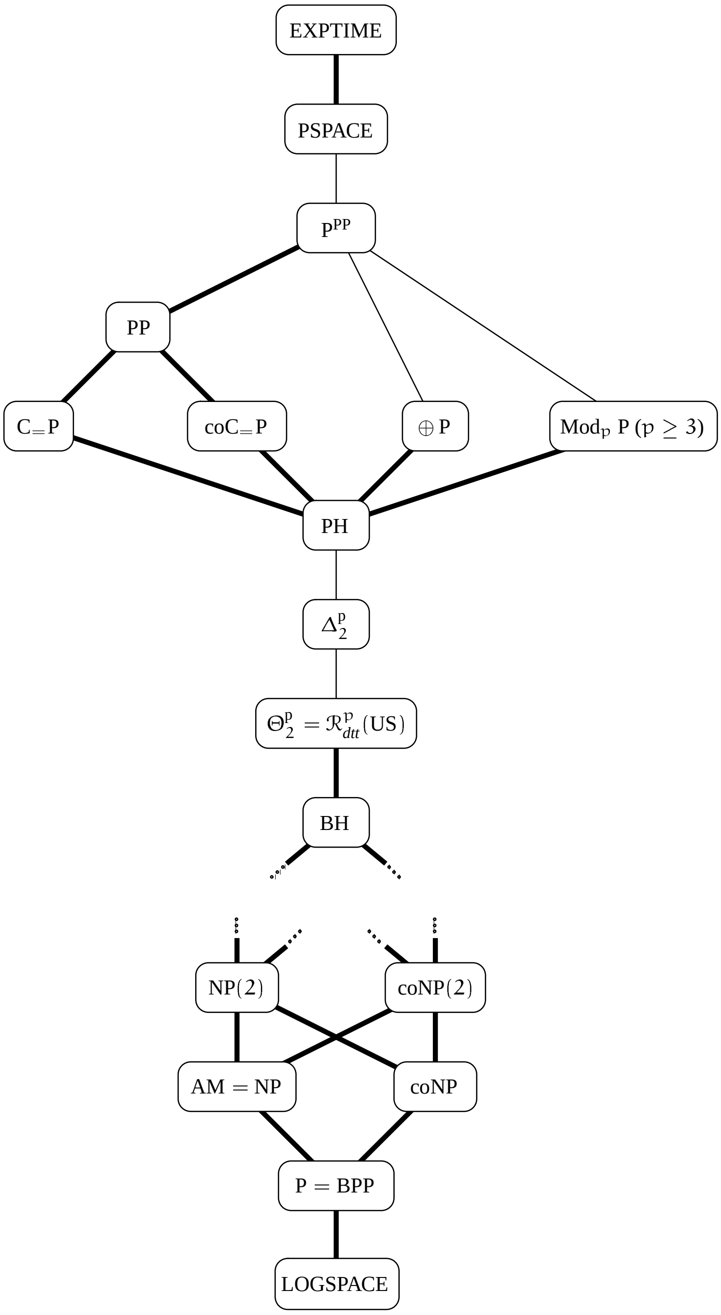
EXPTIME
PSPACE
$\mathrm{P}^{\mathrm{PP}}$
PP
$\mathrm{C}_{=}\mathrm{P}$
$\mathrm{coC}_{=}\mathrm{P}$
$\oplus\mathrm{P}$
$\mathrm{Mod}_p\,\mathrm{P}\ (p \geq 3)$
PH
$\Delta_2^p$
$\Theta_2^p = \mathcal{R}_{dtt}^p(\mathrm{US})$
BH
NP(2)
coNP(2)
AM = NP
coNP
P = BPP
LOGSPACE

Figure 1: Inclusion between important complexity classes which hold for a measure one set of oracles. Boldface lines mean strict inclusion whereas thin lines do not exclude equality.

If we take a close look at the ALMOST-operator, then we see that it is some form of probabilistic type 2 operator, i.e. an operator quantifying over infinite objects (oracles) instead of (finite) words. Building on this it was proved that the ALMOST-operator actually coincides with a type 2 analogue of the well-known $\mathrm{BP}^{\mathrm{p}}$ operator.

**Definition 6.4** Let $\mathcal{K}$ be a recursively presentable relativized class. Then $L \in \mathrm{BP}^2 \cdot \mathcal{K}$ iff there exists an $L' \in \mathcal{K}$ such that for all $x$,

$$\mu_A\,[x \in L \leftrightarrow (A, x) \in L'] \geq \frac{2}{3}.$$

As it turns out we will also have to consider some form of probability amplification in the context of relativized classes and the $\mathrm{BP}^2$ operator. We say that a relativizable class $\mathcal{K}^{(\cdot)}$ has the *type 2 amplification property,* if $L \in \mathrm{BP}^2\mathcal{K}$ iff for every polynomial $p$ there exists an $L' \in \mathcal{K}$ such that for all $x$, $\mu_A\,[x \in L \leftrightarrow (A, x) \in L'] \geq 1 - 2^{-p(|x|)}$. Again, we will omit the prefix *type 2,* if no confusion can arise.

Now it was shown:

**Theorem 6.5 [66, 26].** *If $\mathcal{K}$ is a relativized class which has the type 2 amplification property and which is closed under finite variations of the oracle, then*

$$\text{ALMOST-}\mathcal{K} = \mathrm{BP}^2 \cdot \mathcal{K}.$$

The proof of this result follows essentially from the Lebesgue Density Theorem plus a recursion theoretic argument by Sacks [75, page 272].

It is now not too hard to see that if we apply the $\mathrm{BP}^2$ operator to complexity classes defined by nondeterministic polynomial time Turing machines, then it coincides with the BP type operator quantifying over exponentially long strings.

**Corollary 6.6** *For every class $\mathcal{K}$ such that $\mathcal{K} = \mathrm{Leaf}^{\mathrm{P}}(B)$ for some recursive language $B$ and $\mathcal{K}$ has the amplification property,*

$$\text{ALMOST-}\mathcal{K} = \mathrm{BP}^{\exp} \cdot \mathcal{K}.$$

This applies to a wide variety of complexity classes $\mathcal{K}$, e.g. P, NP, $\Sigma_k^p$, $\Pi_k^p$, $\Delta_k^p$, $\Theta_k^p$, $\mathrm{NP}(k)$, UP, $\oplus$ P, $\mathrm{Mod}_p$ P ($p$ prime), PP, $\mathrm{C_{=}P}$, and PSPACE. For some classes $\mathcal{K}$ we even have $\mathrm{BP}^{\exp} \cdot \mathcal{K} = \mathrm{BP}^{\mathrm{p}} \cdot \mathcal{K}$. This yields some of the results of the following theorem.

**Theorem 6.7**

1. ALMOST-L $= \mathrm{BP}^{\mathrm{p}} \cdot \mathrm{L}$ [68].
2. ALMOST-P $=$ BPP [13, 2].
3. ALMOST-$\mathrm{NP_B}$ $=$ ALMOST-NP $= \mathrm{BP}^{\mathrm{p}} \cdot \mathrm{NP} =$ AM [18, 69].
   *($\mathrm{NP_B}$ is a certain restricted relativization of* NP *introduced in* [21]*.)*
4. ALMOST-$\Sigma_k^p = \mathrm{BP}^{\mathrm{p}} \cdot \Sigma_k^p \subseteq \Pi_{k+1}^p$ *for* $k \geq 2$ [69, 76].
5. ALMOST-$\Pi_k^p = \mathrm{BP}^{\mathrm{p}} \cdot \Pi_k^p \subseteq \Sigma_{k+1}^p$ *for* $k \geq 2$ [69, 76].

*6.* ALMOST-PH $=$ PH [69].

*7.* ALMOST-$\mathrm{P}^{\mathrm{QBF}}$ $=$ ALMOST-$\mathrm{NP}^{\mathrm{QBF}}$ $=$ ALMOST-$\mathrm{PH}^{\mathrm{QBF}}$ $=$ PSPACE [40].

The proofs of Statements 3–6 rely on Nisan and Wigderson's results $\mathrm{BP}^{\exp} \cdot \Sigma_k^p = \mathrm{BP}^p \cdot \Sigma_k^p$ and $\mathrm{BP}^{\exp} \cdot \Pi_k^p = \mathrm{BP}^p \cdot \Pi_k^p$ for $k \geq 0$ [69] as well as Schöning's results $\mathrm{BP}^p \cdot \Sigma_k^p \subseteq \Pi_{k+1}^p$ and $\mathrm{BP}^p \cdot \Pi_k^p \subseteq \Sigma_{k+1}^p$, which are generalizations of Lautemann [61] and Sipser's [80] inclusion BPP $\subseteq \Sigma_2^p \cap \Pi_2^p$ [76].

In a number of prominent classes, no characterization is known; it is e.g. an open question whether ALMOST-PP or ALMOST-PSPACE coincide with one of the classical complexity classes. For ALMOST-PSPACE it is known that it is included in the second level of the exponential time hierarchy [26]. Furthermore, ALMOST-PSPACE can be characterized in terms of checking stack automata (introduced in [54])—it corresponds to polynomial space on probabilistic two-sided bounded error checking stack automata [26].

A relativized class is of course nothing else than a reducibility notion (all the examples mentioned so far directly correspond to certain Turing reductions). But also more sensible reducibility notions are expressible in this way, e.g. $\mathcal{R}_m^p(A) = \mathcal{K}_1^A$, $\mathcal{R}_{btt}^p(A) = \mathcal{K}_2^A$, and $\mathcal{R}_{tt}^p(A) = \mathcal{K}_3^A$ for suitable relativized classes $\mathcal{K}_1$, $\mathcal{K}_2$, and $\mathcal{K}_3$, resp. Instead of ALMOST-$\mathcal{K}_1$ we also use ALMOST-$\mathcal{R}_m^p$ etc.

**Theorem 6.8** *1.* ALMOST-$\mathcal{R}_m^p$ $=$ ALMOST-$\mathcal{R}_{\text{log-T}}^p$ $=$ P [2, 82].

*2.* ALMOST-$\mathcal{R}_{tt}^p$ $=$ ALMOST-P $=$ BPP [13, 82].

We have seen in Theorem 6.5 that the $\mathrm{BP}^2$ operator corresponds to the ALMOST-operator. It should be remarked that the usual $\mathrm{BP}^p$ operator also has a correspondence in terms of ALMOST-classes. Tang and Watanabe studied already in 1989 statements holding for "almost every tally set" [83]. To define this notion, they first established a one-one correspondence between tally sets and $\omega$-words by identifying a tally set $T \subseteq \{0\}^*$ with the infinite sequence $\tau_T =_{\text{def}} T(\epsilon)T(0)T(00)T(000)\cdots \in \{0,1\}^\omega$. Then they used the measure $\mu$ on $\{0,1\}^\omega$ to measure classes of tally sets. A statement $H(T)$ in $T$ is said to hold for almost all tally sets, iff $\mu\left[\left\{\, \tau_T \;\middle|\; H(T)\,\right\}\right] = 1$. They proved the following:

**Theorem 6.9 [83].** *Let* $\mathcal{K} = \mathrm{Leaf}^{\mathrm{P}}(B)$ *for a recursive* $B$ *have the amplification property. Then*

$$A \in \mathrm{BP}^p \cdot \mathcal{K} \Leftrightarrow A \in \mathcal{K}^T \textit{ for almost all tally sets } T.$$

## 7 THE RANDOM ORACLE HYPOTHESIS

The role of relativization in complexity theory has been a source for constant debate (see e.g. [1, 42]). For a long time contradicting relativizations of a statement about complexity classes were taken as evidence that a proof or disproof of the statement will be hard to obtain [53]. However it seems this has changed since the development of non-relativizing proof techniques (e.g. [78, 3]).

The construction of oracles to force a certain statement to be true often failed to have a real impact on the non-relativized world. This is since the oracles were constructed with the sole purpose to make that particular statement true. Thus they have a very “intentional nature” [59]. However, random oracles are certainly not of this kind but structureless by nature. Thus one can hope that they do not distort the relations among complexity classes holding in the absolute sense. Therefore Bennet and Gill were led to the conjecture that every statement holding relative to almost all oracles is also true in the unrelativized case.

Certainly one has to be careful to exclude certain trivial counterexamples. Without going into the technical details (for that, consult [13] or [59]) we just want to remark that to exclude pathological examples as “$\mathrm{P} = \mathrm{P}^A$”, Bennet and Gill introduced what they called *acceptable relativized statements.* Let us just remark that all the examples we discuss below are acceptable in this sense.

The formal statement of the Random Oracle Hypothesis is now as follows: Let $\Phi^{(\cdot)}$ be an acceptable relativized statement. Then *the corresponding unrelativized statement, i.e.* $\Phi^{\emptyset}$*, holds if and only if* $\mu_A\left[\Phi^A\right] = 1$.

Unfortunately the hypothesis as just stated is false. Let us mention the best-known counterexamples. All of them are measure 1 separations where in the unrelativized world we have equality.

1. Since QBF is PSPACE-complete, certainly $\mathrm{PH}^{\mathrm{QBF}} = \mathrm{PSPACE}$, but this does not hold relative to a measure 1 set of oracles (see Theorem 3.8).

2. Polynomial space on alternating machines is of the same power as deterministic exponential time [37], but this does not hold relative to a measure 1 set of oracles (see Theorem 3.4).

3. NP is the class of languages accepted by probabilistically checkable proof systems with logarithmically many random bits and a constant number of bits in the proof to be looked at [3, 81], but this does not hold relative to a measure 1 set of oracles (see Theorem 3.17).

4. PSPACE is the class of languages acceptable by polynomial time interative proof systems [78], but this does not hold relative to a measure 1 set of oracles (see Theorem 3.18).

What should we conclude from all this? The meaning of random oracle results is unclarified and remains an interesting open problem. For some researchers the existence of a random oracle making statement $\Phi$ true is nothing more than the existence of *some* oracle with this property [42]. The only advantage of random oracles seen is that all statements holding under some random oracle hold simultaneously under all random oracles. But it is argued that a more powerful tool for such purposes is the use of generic oracles that also allow to combine different oracle requirements. For generic oracles it is e.g. known that they make the isomorphism conjecture true in contrast to random oracles (see Section 3). But do we really believe in the unrelativized isomorphism conjecture?

For a number of other researchers it is considered to be a challenge to find a more sensible formulation of the random oracle hypothesis [32, 38]. It is clear that in Examples 2 and 3 above different computation models with different abilities to access their oracles are compared. Thus it is of no surprise that separating oracles exist, and to show that the separation even holds for a measure one set of oracles requires often only some more technical work. Here "oracles do not relativize complexity classes, they only relativize machines" [47], in particular they relativize their different ways to access the oracle.

To formulate a more sensible random oracle hypothesis one should therefore restrict onself to comparison of classes with equal oracle access mechnism. This is for example given when all classes involved are leaf language definable in the sense of Section 4. Every leaf language definable class is based on nondeterministic polynomial time oracle machines. Only the external evaluation modes of the computation trees differ between different leaf language definable classes. Thus one might hope that the following is true: *If* $\Phi^{(\cdot)}$ *is an acceptable relativized statement involving only leaf language defined classes, then* $\Phi^{\emptyset}$ *iff* $\mu_A\left[\Phi^A\right]=1$.

What we want to point out, however, is that again there are counterexamples to this hypothesis. Consider Example 4 above. The class PSPACE corresponds relativizably to alternating polynomial time, which immediately leads to a leaf language characterization of PSPACE (relativizably; recall that we use the bounded query model). On the other hand, Vereshchagin in [89] gave a leaf language characterization of IP. Also, the class $\mathrm{PH}^{\mathrm{QBF}\oplus(\cdot)}$ is easily leaf language characterizable. Thus we see that Examples 1 and 4 are again counterexamples to the above hypothesis.

The random oracle hypothesis, even in the very restricted form where all classes are uniformly definable and the oracle access mechanism in all involved classes is equal, does not hold.

## 8 POSITIVE RELATIVIZATIONS

Though as we have seen the Random Oracle Hypothesis even in a restricted formulation fails in the general case, it is interesting to identify special cases where the hypothesis holds, i.e. where for relativizable classes $\mathcal{K}_1$ and $\mathcal{K}_2$ one can prove $\mathcal{K}_1 \subseteq \mathcal{K}_2 \iff \mu_A\left[\mathcal{K}_1^A \subseteq \mathcal{K}_2^A\right]=1$. For the purpose of the present paper, we call such an equivalence a *positive relativization*. (Originally, the term positive relativization was coined considering equivalences $\mathcal{K}_1 \subseteq \mathcal{K}_2 \iff (\forall A)\left[\mathcal{K}_1^A \subseteq \mathcal{K}_2^A\right]$, cf. [15, 28, 77, 16].)

There are a few such results which are basically of the form

$$\begin{aligned} \mathrm{BP}^{\mathrm{p}} \cdot \mathcal{K}^{B} \subseteq \mathrm{BP}^{\mathrm{p}} \cdot \mathcal{K} \quad &\iff \quad \mu_A\left[\mathrm{BP}^{\mathrm{p}} \cdot \mathcal{K}^{A\oplus B} \subseteq \mathrm{BP}^{\mathrm{p}} \cdot \mathcal{K}^{A}\right]=1 \\ &\iff \quad \mu_A\left[\mathcal{K}^{A\oplus B} \subseteq \mathcal{K}^{A}\right]=1 \end{aligned}$$

for fixed set $B$, i.e. they concern the question whether a fixed oracle can enlarge a given complexity class of the form $\mathrm{BP}^{\mathrm{p}} \cdot \mathcal{K}$. Though one could state a more general theorem of this kind, we restrict ourselves to two interesting examples.

**Theorem 8.1** *For every set* $B$,

1. $B \in \mathrm{BPP} \iff \mathrm{BPP}^B = \mathrm{BPP} \iff \mu_A\left[\mathrm{BPP}^{A\oplus B} = \mathrm{BPP}^A\right] = 1$
$\iff \mu_A\left[\mathrm{P}^{A\oplus B} = \mathrm{P}^A\right] = 1.$

2. $B \in \mathrm{PH} \iff \mathrm{PH}^B = \mathrm{PH} \iff \mu_A\left[\mathrm{PH}^{A\oplus B} = \mathrm{PH}^A\right] = 1.$

*Proof.* We prove Statement 1, the other statement can be proved similarly.

The first equivalence is obvious. From $B \in \mathrm{BPP}$ we conclude $\mathrm{BPP}^{A\oplus B} \subseteq \mathrm{BPP}^A$ for every $A$. From $\mu_A\left[\mathrm{BPP}^{A\oplus B} = \mathrm{BPP}^A\right] = 1$ we conclude $\mu_A\left[\mathrm{P}^{A\oplus B} = \mathrm{P}^A\right] \geq \mu_A\left[\mathrm{BPP}^{A\oplus B} = \mathrm{P}^A\right] = \mu_A\left[\mathrm{BPP}^{A\oplus B} = \mathrm{BPP}^A\right] = 1$, because of Bennett and Gill's result $\mu_A\left[\mathrm{P}^A = \mathrm{BPP}^A\right] = 1$ (see Theorem 5.1). From $\mu_A\left[\mathrm{P}^{A\oplus B} = \mathrm{P}^A\right] = 1$ we conclude $\mu_A\left[B \in \mathrm{P}^A\right] = 1$ and hence $B \in$ ALMOST-P $=$ BPP (see Theorem 6.7.2). ❑

Let SAT be the satisfiability problem for boolean formulae. The following corollary of the preceding theorem was shown by Book [18] (the first statement appears there in a slightly different formulation).

**Corollary 8.2**

1. $\mathrm{SAT} \in \mathrm{BPP} \iff \mathrm{AM} = \mathrm{BPP} \iff \mu_A\left[\mathrm{P}^{A\oplus\mathrm{SAT}} = \mathrm{P}^A\right] = 1.$

2. $\mathrm{QBF} \in \mathrm{PH} \iff \mathrm{PSPACE} = \mathrm{PH} \iff \mu_A\left[\mathrm{PH}^{A\oplus\mathrm{QBF}} = \mathrm{PH}^A\right] = 1.$

It might be interesting to note that from Corollary 6.6 one can conclude the following "partial" positive relativization:

**Theorem 8.3 [26].** *For all relativized classes* $\mathcal{K}_1$ *and* $\mathcal{K}_2$ *such that* $\mathcal{K}_2 = \mathrm{Leaf}^{\mathrm{P}}(B)$ *for some recursive language* $B$ *and* $\mathcal{K}_2$ *has the amplification property,*

$$\mathcal{K}_1 \subseteq \mathrm{BP}^{\mathrm{exp}}\mathcal{K}_2 \iff \mu_A\left[\mathcal{K}_1 \subseteq \mathrm{BP}^{\mathrm{exp}}\mathcal{K}_2^A\right] = 1 \iff \mu_A\left[\mathcal{K}_1 \subseteq \mathcal{K}_2^A\right] = 1.$$

**Corollary 8.4** 1. $\mathrm{AM} = \mathrm{BPP} \iff \mu_A\left[\mathrm{NP} \subseteq \mathrm{AM}^A\right] = 1.$

2. $\mathrm{PSPACE} = \mathrm{PH} \iff \mu_A\left[\mathrm{PSPACE} \subseteq \mathrm{PH}^A\right] = 1.$

3. $\mathrm{PH} = \mathrm{BP}^{\mathrm{p}} \cdot \Sigma_k^{\mathrm{p}} \iff \mu_A\left[\mathrm{PH} \subseteq \Sigma_k^{\mathrm{p},A}\right] = 1.$

From the latter statement, one can immediately conclude the following result by Book:

**Corollary 8.5 [19].** *If the polynomial hierarchy collapses for almost all oracles, then the unrelativized polynomial hierarchy collapses.*

**Acknowledgement.** Thanks for helpful hints are due to Jin-Yi Cai, Buffalo, and Fred Green, Worcester.

## References

[1] E. ALLENDER, *Oracles versus proof techniques that do not relativize*, in Proceedings 1st International Symposium on Algorithms, vol. 450 of Lecture Notes in Computer Science, Springer-Verlag, 1990, pp. 39–52.

[2] K. AMBOS-SPIES, *Randomness, relativizations, and polynomial reducibilities*, in Proceedings 1st Structure in Complexity Theory, vol. 223 of Lecture Notes in Computer Science, Springer-Verlag, 1986, pp. 200–207.

[3] S. ARORA, C. LUND, R. MOTWANI, M. SUDAN, AND M. SZEGEDY, *Proof verification and the intractability of approximation problems*, in Proceedings 33rd Symposium on the Foundations of Computer Science, IEEE Computer Society Press, 1992, pp. 14–23.

[4] J. ASPNES, R. BEIGEL, M. FURST, AND S. RUDICH, *The expressive power of voting polynomials*, in Proceedings 23rd Symposium on Theory of Computing, ACM Press, 1991, pp. 402–409.

[5] L. BABAI, *Trading group theory for randomness*, in Proceedings 17th Symposium on Theory of Computing, ACM Press, 1985, pp. 421–429.

[6] ——, *Random oracles separate PSPACE from the polynomial-time hierarchy*, Information Processing Letters, 26 (1987), pp. 51–53.

[7] H. BAIER AND K. W. WAGNER, *The analytic polynomial-time hierarchy*, Tech. Rep. 148, Institut für Informatik, Universität Würzburg, 1996.

[8] T. BAKER, J. GILL, AND R. SOLOVAY, *Relativizations of the P=NP problem*, SIAM Journal on Computing, 4 (1975), pp. 431–442.

[9] J. L. BALCÁZAR, J. DÍAZ, AND J. GABARRÓ, *Structural Complexity II*, Springer-Verlag, 1990.

[10] ——, *Structural Complexity I*, Springer-Verlag, 2nd ed., 1995.

[11] R. BEIGEL, J. GILL, AND U. HERTRAMPF, *Counting classes: thresholds, parity, mods, and fewness*, in Proceedings 7th Symposium on Theoretical Aspects of Computer Science, vol. 415 of Lecture Notes in Computer Science, Springer-Verlag, 1990, pp. 49–57.

[12] R. BEIGEL, N. REINGOLD, AND D. SPIELMAN, *PP is closed under intersection*, in Proceedings 23rd Symposium on Theory of Computing, ACM Press, 1991, pp. 1–9.

[13] C. BENNETT AND J. GILL, *Relative to a random oracle $P^A \neq NP^A \neq coNP^A$ with probability 1*, SIAM Journal on Computing, 10 (1981), pp. 96–113.

[14] A. BLASS AND Y. GUREVICH, *On the unique satisfiability problem*, Information and Control, (1982), pp. 80–88.

[15] R. V. BOOK, *Bounded query machines: On NP and PSPACE*, Theoretical Computer Science, 15 (1981), pp. 27–39.

[16] ———, *Restricted relativizations of complexity classes*, in Computational Complexity Theory, J. Hartmanis, ed., vol. 38 of Proceedings Symposia in Applied Mathematics, American Mathematical Society, 1989, pp. 47–74.

[17] ———, *On random oracle separations*, Information Processing Letters, 39 (1991), pp. 7–10.

[18] ———, *Some observations on separating complexity classes*, SIAM Journal on Computing, 20 (1991), pp. 246–258.

[19] ———, *On collapsing the polynomial-time hierarchy*, Information Processing Letters, 52 (1994), pp. 235–237.

[20] ———, *On languages reducible to algorithmically random languages*, SIAM Journal on Computing, 23 (1994), pp. 1275–1282.

[21] R. V. BOOK, T. LONG, AND A. SELMAN, *Quantitative relativizations of complexity classes*, SIAM Journal on Computing, 13 (1984), pp. 461–487.

[22] R. V. BOOK, J. LUTZ, AND D. MARTIN, *The global power of additional queries to random oracles*, Information and Computation, 120 (1995), pp. 49–54.

[23] R. V. BOOK, J. LUTZ, AND S. TANG, *Additional queries to random and pseudorandom oracles*, in Proceedings 17th International Colloquium on Automata, Languages and Programming, vol. 443 of Lecture Notes in Computer Science, Springer-Verlag, 1991, pp. 283–293.

[24] R. V. BOOK, J. LUTZ, AND K. W. WAGNER, *An observation on probability versus randomness with applications to complexity classes*, Mathematical Systems, 27 (1994), pp. 201–209.

[25] R. V. BOOK AND E. MAYORDOMO, *On the robustness of Almost-R*, R.A.I.R.O. Informatique Théoretique et Applications, (1996). To appear.

[26] R. V. BOOK, H. VOLLMER, AND K. W. WAGNER, *On type-2 probabilistic quantifiers*, in Proceedings 23rd International Colloquium on Automata, Languages and Programming, vol. 1099 of Lecture Notes in Computer Science, Springer-Verlag, 1996, pp. 369–380.

[27] R. V. BOOK AND O. WATANABE, *On random hard sets for NP*, Information and Computation, 125 (1996), pp. 70–76.

[28] R. V. BOOK AND C. WRATHALL, *Bounded query machines: On NP() and NPQUERY()*, Theoretical Computer Science, 15 (1981), pp. 41–50.

[29] D. P. BOVET, P. CRESCENZI, AND R. SILVESTRI, *Complexity classes and sparse oracles*, in Proceedings 6th Structure in Complexity Theory, IEEE Computer Society Press, 1991, pp. 102–108.

[30] ——, *A uniform approach to define complexity classes*, Theoretical Computer Science, 104 (1992), pp. 263–283.

[31] J. F. BUSS, *Relativized alternation and space-bounded computation*, Journal of Computer and System Sciences, 36 (1988), pp. 351–278.

[32] J. Y. CAI, *Probability one separation of the boolean hierarchy*, in Proceedings 4th Symposium on Theoretical Aspects of Computer Science, vol. 38 of Lecture Notes in Computer Science, Springer-Verlag, 1987, pp. 148–158.

[33] ——, *With probability one, a random oracle separates PSPACE from the polynomial-time hierarchy*, Journal of Computer and System Sciences, 38 (1989), pp. 68–85.

[34] J.-Y. CAI, T. GUNDERMANN, J. HARTMANIS, L. A. HEMACHANDRA, V. SEWELSON, K. W. WAGNER, AND G. WECHSUNG, *The boolean hierarchy I: Structural properties*, SIAM Journal on Computing, 17 (1988), pp. 1232–1252.

[35] J. Y. CAI AND L. HEMACHANDRA, *The Boolean hierarchy: hardware over NP*, in Proceedings 1st Structure in Complexity Theory, vol. 223 of Lecture Notes in Computer Science, Springer-Verlag, 1986, pp. 105–124.

[36] H. CAUSSINUS, P. MCKENZIE, D. THÉRIEN, AND H. VOLLMER, *Nondeterministic NC*$^1$ *computation*, in Proceedings 11th Computational Complexity, IEEE Computer Society Press, 1996, pp. 12–21.

[37] A. K. CHANDRA, D. KOZEN, AND L. J. STOCKMEYER, *Alternation*, Journal of the ACM, 28 (1981), pp. 114–133.

[38] R. CHANG, B. CHOR, O. GOLDREICH, J. HARTMANIS, J. HASTAD, D. RANJAN, AND P. ROHATGI, *The random oracle hypothesis is false*, Journal of Computer and System Sciences, 49 (1994), pp. 24–39.

[39] K. CRONAUER, U. HERTRAMPF, H. VOLLMER, AND K. W. WAGNER, *The chain method to separate counting classes*, Tech. Rep. A-95-20, Department of Computer Science, University Lübeck, 1995.

[40] Z. DANG AND R. V. BOOK, *On characterizations of Almost-*$\mathrm{R}_{\mathrm{A}}$. Manuscript, 1996.

[41] S. FENNER, L. FORTNOW, AND S. KURTZ, *Gap-definable counting classes*, Journal of Computer and System Sciences, 48 (1994), pp. 116–148.

[42] L. FORTNOW, *The role of relativization in complexity theory*, Bulletin of the EATCS, 52 (1994), pp. 229–244.

[43] L. Fortnow and M. Sipser, *Are there interactive protocols for coNP languages?*, Information Processing Letters, 28 (1988), pp. 249–251.

[44] M. Furst, J. B. Saxe, and M. Sipser, *Parity, circuits, and the polynomial-time hierarchy*, Mathematical Systems Theory, 17 (1984), pp. 13–27.

[45] J. Gill, *Computational complexity of probabilistic complexity classes*, SIAM Journal on Computing, 6 (1977), pp. 675–695.

[46] F. Green, *On the power of deterministic reductions to $C_{=}P$*, Mathematical Systems Theory, 26 (1993), pp. 215–234.

[47] J. Hartmanis, R. Chang, S. Chari, D. Ranjan, and P. Rohatgi, *Relativization: a revisionistic retrospective*, in Current Trends in Theoretical Computer Science, G. Rozenberg and A. Salomaa, eds., World Scientific, 1993, pp. 537–547.

[48] J. Håstad, *Computational Limitations of Small Depth Circuits*, MIT Press, Cambridge, 1988.

[49] U. Hertrampf, *Classes of bounded counting type and their inclusion relations*, in Proceedings 12th Symposium on Theoretical Aspects of Computer Science, vol. 900 of Lecture Notes in Computer Science, Springer-Verlag, 1995, pp. 60–70.

[50] U. Hertrampf, C. Lautemann, T. Schwentick, H. Vollmer, and K. W. Wagner, *On the power of polynomial time bit-reductions*, in Proceedings 8th Structure in Complexity Theory, 1993, pp. 200–207.

[51] U. Hertrampf, H. Vollmer, and K. W. Wagner, *On the power of number-theoretic operations with respect to counting*, in Proceedings 10th Structure in Complexity Theory, 1995, pp. 299–314.

[52] ——, *On balanced vs. unbalanced computation trees*, Mathematical Systems Theory, 29 (1996), pp. 411–421.

[53] J. E. Hopcroft, *Turing machines*, Scientific American, 5 (1984), pp. 86–98.

[54] O. H. Ibarra, *Characterizations of some tape and time classes of turing machines in terms of multihead and auxiliary stack automata*, Journal of Computer and System Sciences, 5 (1971), pp. 88–117.

[55] B. Jenner, P. McKenzie, and D. Thérien, *Logspace and logtime leaf languages*, in 9th Annual Conference Structure in Complexity Theory, 1994, pp. 242–254.

[56] D. S. Johnson, *A catalog of complexity classes*, in Handbook of Theoretical Computer Science, J. van Leeuwen, ed., vol. A, Elsevier, 1990, pp. 67–161.

[57] S. Kautz, *Degrees of random sets*, PhD thesis, Cornell University, 1991.

[58] S. M. KAUTZ AND P. B. MILTERSEN, *Relative to a random oracle, NP is not small*, in Proceedings 9th Structure in Complexity Theory, IEEE Computer Society Press, 1994, pp. 162–174.

[59] S. KURTZ, *On the random oracle hypothesis*, Information and Control, 57 (1983), pp. 40–47.

[60] S. A. KURTZ, S. R. MAHANEY, AND J. S. ROYER, *The isomorphism conjecture fails relative to a random oracle*, Journal of the ACM, 42 (1995), pp. 401–420.

[61] C. LAUTEMANN, *BPP and the polynomial hierarchy*, Information Processing Letters, 117 (1983), pp. 215–217.

[62] M. LI AND P. VITÁNYI, *An Introduction to Kolmogorov Complexity and its Applications*, Texts and Monographs in Computer Science, Springer-Verlag, New York, 1993.

[63] J. LUTZ, *On independent random oracles*, Theoretical Computer Science, 92 (1992), pp. 301–307.

[64] ———, *The quantitative structure of exponential time*, in Proceedings 8th Structure in Complexity Theory, IEEE Computer Society Press, 1993, pp. 158–175.

[65] P. MARTIN-LÖF, *The definition of random sequences*, Information and Control, 9 (1966), pp. 602–619.

[66] W. MERKLE AND Y. WANG, *Separations by random oracles and "Almost" classes for generalized reducibilities*, in Proceedings 20th Symposium on Mathematical Foundations of Computer Science, vol. 969 of Lecture Notes in Computer Science, Springer-Verlag, 1995, pp. 179–190.

[67] A. R. MEYER AND L. J. STOCKMEYER, *The equivalence problem for regular expressions with squaring requires exponential time*, in Proceedings 13th Symposium on Switching and Automata Theory, IEEE Computer Society Press, 1972, pp. 125–129.

[68] N. NISAN, *On read-once vs. multiple access to randomness in logspace*, Theoretical Computer Science, 107 (1993), pp. 135–144.

[69] N. NISAN AND A. WIGDERSON, *Hardness vs. randomness*, Journal of Computer and System Sciences, 49 (1994), pp. 149–167.

[70] P. ORPONEN, *Complexity classes of alternating machines with oracles*, in Proceedings 10th International Colloquium on Automata, Languages and Programming, vol. 154 of Lecture Notes in Computer Science, Springer-Verlag, 1983, pp. 573–584.

[71] C. H. PAPADIMITRIOU, *Computational Complexity*, Addison-Wesley, 1994.

[72] C. H. PAPADIMITRIOU AND S. ZACHOS, *Two remarks on the power of counting*, in Proceedings 6th GI Conference on Theoretical Computer Science, vol. 145 of Lecture Notes in Computer Science, Springer-Verlag, 1983, pp. 269–275.

[73] J. RADHAKRISHNAN AND S. SALUJA, *Interactive proof systems*, Tech. Rep. TCS-95/4, Tata Institute of Fundamental Research, Bombay, 1995. Lecture Notes.

[74] K. W. REGAN AND J. S. ROYER, *On closure properties of bounded two-sided error complexity classes*, Mathematical Systems Theory, 28 (1995), pp. 229–243.

[75] H. ROGERS JR., *Theory of Recursive Functions and Effective Computability*, McGraw-Hill, New York, 1967.

[76] U. SCHÖNING, *Probabilistic complexity classes and lowness*, Journal of Computer and System Sciences, 39 (1989), pp. 84–100.

[77] A. L. SELMAN, M.-R. XU, AND R. V. BOOK, *Positive relativizations of complexity classes*, SIAM Journal on Computing, 12 (1983), pp. 565–579.

[78] A. SHAMIR, *IP = PSPACE*, Journal of the ACM, 39 (1992), pp. 869–877.

[79] J. SIMON, *On Some Central Problems in Computational Complexity*, PhD thesis, Cornell University, 1975.

[80] M. SIPSER, *A complexity theoretic approach to randomness*, in Proceedings of the 15th Symposium on Theory of Computing, 1983, pp. 330–335.

[81] M. SUDAN, *Efficient Checking of Polynomials and Proofs and the Hardness of Approximation Problems*, vol. 1001 of Lecture Notes in Computer Science, Springer-Verlag, 1995.

[82] S. TANG AND R. V. BOOK, *Polynomial-time reducibilities and almost all oracle sets*, Theoretical Computer Science, 81 (1991), pp. 201–209.

[83] S. TANG AND O. WATANABE, *On tally relativizations of BP-complexity classes*, SIAM Journal on Computing, 18 (1989), pp. 449–462.

[84] S. TODA, *PP is as hard as the polynomial time hierarchy*, SIAM Journal on Computing, 20 (1991), pp. 865–877.

[85] S. TODA AND M. OGIWARA, *Counting classes are at least as hard as the polynomial time hierarchy*, SIAM Journal on Computing, 21 (1992), pp. 315–328.

[86] L. G. VALIANT, *The complexity of enumeration and reliabilty problems*, SIAM Journal of Computing, 8 (1979), pp. 411–421.

[87] L. G. VALIANT AND V. V. VAZIRANI, *NP is as easy as dedecting unique solutions*, Theoretical Computer Science, (1986), pp. 85–93.

[88] N. K. VERESHCHAGIN, *Relationships between NP-sets, Co-NP-sets, and P-sets relative to random oracles*, in Proceedings 8th Structure in Complexity Theory, IEEE Computer Society Press, 1993, pp. 132–138.

[89] ———, *Relativizable and non-relativizable theorems in the polynomial theory of algorithms*, Izvestija Rossijskoj Akademii Nauk, 57 (1993), pp. 51–90. In Russian.

[90] K. W. WAGNER, *Some observations on the connection between counting and recursion*, Theoretical Computer Science, 47 (1986), pp. 131–147.

[91] ———, *Bounded query classes*, SIAM Journal on Computing, 19 (1990), pp. 833–846.

[92] C. WRATHALL, *Complete sets and the polynomial-time hierarchy*, Theoretical Computer Science, 3 (1977), pp. 23–33.

[93] A. C. C. YAO, *Separating the polynomial-time hierarchy by oracles*, in Proceedings 26th Foundations of Computer Science, IEEE Computer Society Press, 1985, pp. 1–10.