Separations by Random Oracles and "Almost" Classes for Generalized Reducibilities

Wolfgang Merkle[1] and Yongge Wang[2] *

[1] Universität Heidelberg, Mathematisches Institut, Im Neuenheimer Feld 294, D–69120 Heidelberg, Germany, merkle@math.uni-heidelberg.de
[2] Certicom Research, Certicom Corp., 5520 Explorer Dr., Mississauga, ON, L4W 5L1, Canada, ywang@certicom.com

Abstract. Let $\le_r$ and $\le_s$ be two binary relations on $2^{\mathbb{N}}$ which are meant as reducibilities. Let both relations be closed under finite variation (of their set arguments) and consider the uniform distribution on $2^{\mathbb{N}}$, which is obtained by choosing elements of $2^{\mathbb{N}}$ by independent tosses of a fair coin. Then we might ask for the probability that the lower $\le_r$-cone of a randomly chosen set X, that is, the class of all sets A with $A \le_r X$, differs from the lower $\le_s$-cone of X. By closure under finite variation, the Kolmogorov 0-1 law yields immediately that this probability is either 0 or 1; in case it is 1, the relations are said to be separable by random oracles. Again by closure under finite variation, for every given set A, the probability that a randomly chosen set X is in the upper $\le_r$-cone of A is either 0 or 1; let $Almost_r$ be the class of sets for which the upper $\le_r$-cone has measure 1.

In the following, results about separations by random oracles and about Almost classes are obtained in the context of generalized reducibilities, that is, for binary relations on $2^{\mathbb{N}}$ which can be defined by a countable set of total continuous functionals on $2^{\mathbb{N}}$ in the same way as the usual resource-bounded reducibilities are defined by an enumeration of appropriate oracle Turing machines. The concept of generalized reducibility comprises all natural resource-bounded reducibilities, but is more general; in particular, it does not involve any kind of specific machine model or even effectivity. The results on generalized reducibilities yield corollaries about specific resource-bounded reducibilities, including several results which have been shown previously in the setting of time or space bounded Turing machine computations.

MSC: 03D15, 03D30, 03D75, 68Q10, 68Q15.
Key words: resource-bounded reducibilities, generalized reducibilities, separations by random oracles, almost all classes, use of a reduction.

* Both authors were partially supported by the EU network *Complexity, Logic and Recursion Theory (COLORET)*, EU Contract No. ERBCHRXCT930415. The main part of the work was done when the second author was a PhD student at the University of Heidelberg.

1 Introduction

1.1 Random Oracles and Generalized Reducibilities

Random Oracles. Recall that reducibilities between sets of natural numbers, such as polynomial time bounded Turing reducibility $\leq_{\mathrm{T}}^{\mathsf{P}}$ or (unbounded) truth-table reducibility $\leq_{\mathrm{tt}}$, are binary relations on the powerset $2^{\mathbb{N}}$ of the natural numbers. We say a set D SEPARATES two binary relations $\leq_r$ and $\leq_s$ on $2^{\mathbb{N}}$ iff the lower cones of D with respect to $\leq_r$ and $\leq_s$ are different. Observe that there is such a separating oracle D iff the two relations are different (as relations on $2^{\mathbb{N}}$). Considering the class

$$\mathcal{D} \ := \ \{D \subseteq \mathbb{N} : \leq_r(D) \neq \leq_s(D)\}$$

of all oracles which separate the two given relations, we might ask for the "size" of $\mathcal{D}$ in $2^{\mathbb{N}}$. One possibility to make this query more precise is to ask for the measure of $\mathcal{D}$ under the uniform distribution μ on $2^{\mathbb{N}}$ as introduced in Definition 1. In the sequel, we refer by the term measure always to the measure μ and we say, a property of sets holds for ALMOST ALL or for RANDOM sets iff the class of sets which satisfies the property has measure one.

Definition 1. *The measure on $2^{\mathbb{N}}$ obtained by independent tosses of a fair coin is denoted by μ (i.e., μ is the product measure derived from the uniform distribution on $\{0,1\}$).*

Definition 2. *Two binary relations $\leq_r$ and $\leq_s$ on $2^{\mathbb{N}}$ can be* SEPARATED BY RANDOM ORACLES *iff the class of separating oracles has measure one.*

Observe in connection with Definition 2 that for relations on $2^{\mathbb{N}}$ which are closed under finite variation the class of separating oracles can only have measure 0 or measure 1, as follows from the Kolmogorov 0-1 law stated in Proposition 13. By a similar argument, for a relation which is closed under finite variation, the measure of every particular upper cone can only be either 0 or 1.

Definition 3. *Let $\leq_r$ be a binary relation on $2^{\mathbb{N}}$. We denote by L_r the class of least sets with respect to $\leq_r$ (i.e., the class of sets which have an upper $\leq_r$-cone equal to $2^{\mathbb{N}}$) and we let Almost_r be the class of sets which have an upper $\leq_r$-cone of measure 1.*

For a binary relation $\leq_r$ on $2^{\mathbb{N}}$, the class of least sets L_r is trivially contained in Almost_r, but in general it might be hard to tell whether this containment is proper.

Generalized Reducibilities. Basically all (uniform) time or space bounded reducibilities, such as $\leq_{\mathrm{T}}^{\mathsf{P}}$ and logarithmic space bounded many-one reducibility $\leq_{\mathrm{m}}^{\log}$, can be defined by specifying an effective listing of recursive functionals. This suggests to introduce a corresponding notion of bounded reducibility (see for example [6]) where, formally, a binary relation $\leq_r$ on $2^{\mathbb{N}}$ is a BOUNDED REDUCIBILITY iff there is a recursive set E such that, firstly, Φ_e is total for all e in E and, secondly, for all subsets A and B of $\mathbb{N}$, we have

$$A \leq_r B \text{ iff there is some } e \text{ in } E \text{ with } A = \Phi_e(B) \quad . \tag{1}$$

Here Φ_e is the partial recursive functional computed by the eth oracle Turing machine T_e and Φ_e is total iff T_e is total, that is, for all inputs x and oracles A, the Turing machine T_e eventually outputs $\Phi_e(A, x)$. A total oracle Turing machine computes its result after scanning a finite part of its oracle and consequently for a (total) recursive functional Γ the value of $\Gamma(A, x)$ is determined by a finite part of A. Definition 4 relates to the fact that a functional Γ has the latter property iff it is a continuous mapping in the usual topological sense with respect to the standard topology on $2^{\mathbb{N}}$. Recall in this connection that in general a functional Γ is a function from $2^{\mathbb{N}}$ to $2^{\mathbb{N}}$ which equivalently can be viewed as a function from $2^{\mathbb{N}} \otimes \mathbb{N}$ to the set $\{0, 1\}$ via the equation $\Gamma(A, x) := (\Gamma(A))(x)$.

Definition 4. *A functional Γ is* CONTINUOUS *iff for all sets A and all x in $\mathbb{N}$, there is some finite subset $I(A, x)$ of $\mathbb{N}$ such that for all sets B which agree with A on $I(A, x)$, the sets $\Gamma(A)$ and $\Gamma(B)$ agree at x.*

Bounded reducibilities are effective in two respects due to being defined via an effective listing of recursive functionals. With the more general concept generalized reducibility introduced next, we drop both conditions on effectivity and require just that the reducibility under consideration can be defined via a countable set of continuous, but not necessarily recursive functionals.

Definition 5. *Let $\leq_r$ be a binary relation on $2^{\mathbb{N}}$.*

- *A functional Γ is a* REDUCTION *iff it is continuous. A reduction Γ is a reduction with respect to $\leq_r$ or an $\leq_r$-*REDUCTION, *for short, iff $\Gamma(B) \leq_r B$ holds for all sets B. For sets A and B, a fact $A \leq_r B$ is witnessed by the functional Γ, $A \leq_r B$* VIA *Γ for short, iff Γ is a $\leq_r$-reduction where $A = \Gamma(B)$.*
- *A set $\mathcal{R}$ of functionals is a* REDUCTION COVER *for $\leq_r$ iff $\mathcal{R}$ is a countable set of $\leq_r$-reductions such that when $A \leq_r B$ holds for sets A and B, then this fact is witnessed by some Γ in $\mathcal{R}$.*
- *The relation $\leq_r$ is a* GENERALIZED REDUCIBILITY *iff there is some reduction cover for $\leq_r$.*

Bounded reducibilities are generalized reducibilities which have an EFFECTIVE REDUCTION COVER, that is, a reduction cover of the special form $\{\Phi_e : e \text{ in } E\}$ where E is recursive. Here the definition of reduction cover implies that Φ_e is total for all e in E. An example of a generalized reducibility which is not a bounded reducibility is given by truth-table reducibility $\leq_{\mathrm{tt}}$. By compactness of $2^{\mathbb{N}}$ (see the proof of Proposition 6), the set of all recursive functionals provides a reduction cover for $\leq_{\mathrm{tt}}$, but there is no reduction cover for $\leq_{\mathrm{tt}}$ which has the form $\{\Phi_e : e \text{ in } E\}$ where E is recursive. Otherwise, by a simple diagonalization argument, we could construct a recursive set which is not $\le_{\mathrm{tt}}$-reducible to the empty set.

In the following we will show results about "Almost" classes and separations by random oracles for generalized reducibilities, thus generalizing on previous results for bounded reducibilities. From this extension of results to generalized reducibilities it will become clear that several previous results on bounded reducibilities essentially do not depend on the effectivity of the reducibilities involved, but rely on basically combinatorial properties, which can be formulated in terms of the concept *generalized use* as introduced in Definition 7 below.

1.2 Related Work

Bennett and Gill [4] showed, among other results, that the relations $\le_{\mathrm{T}}^{\mathsf{P}}$ and $\le_{\mathrm{T}}^{\log}$, as well as the relations $\le_{T}^{\mathsf{E}}$ and $\le_{T}^{\mathsf{PSPACE}}$ can be separated by random oracles. Here the subscript T stands for a reducibility of Turing type and the superscripts E and PSPACE indicate time bounds of the form $2^{c|x|+c}$ and polynomial space bounds, respectively. For the reducibilities $\le_{k-\mathrm{tt}}^{\mathsf{P}}$ with $k \ge 0$, i.e., polynomial time bounded reducibilities which are restricted to a constant number k of non-adaptive queries to their oracle, it is shown in [7] that for all $k \ge 0$, $\le_{(k+1)-\mathrm{tt}}^{\mathsf{P}}$ and $\le_{k-\mathrm{tt}}^{\mathsf{P}}$ can be separated by random oracles. It was shown implicitly in [5] that the latter result remains valid with $\le_{k-\mathrm{tt}}^{\mathsf{P}}$ replaced by the reducibility $\le_{k-\mathrm{tt}}$, i.e., the result remains valid if the reducibility restricted to fewer queries is allowed to run in arbitrary instead of polynomial time.

All results mentioned in the preceding paragraph can be derived as corollaries to the results on generalized reducibilities shown below. These results on generalized reducibilities imply, furthermore, that for most of the generalized reducibilities which can be found in the literature, reducibilities of k-tt-type can be separated by random oracles from any reducibility of btt-type which is *not* of k-tt-type itself. Moreover, we show that for a wide class of reducibilities random separations are possible for reducibilities of btt-type vs reducibilities of truth-table or Turing type, and the same holds for truth-table vs Turing type. Note that the latter result cannot hold for all pairs of resource-bounded reducibilities of truth-table and Turing type because for example in the case of reductions restricted to elementary time, the corresponding reducibility notions are the same.

It is known that $\mathsf{Almost}_{\mathrm{btt}}^{\mathsf{P}}$ coincides with P, see [1, 2, 7]. We extend this result by showing that for all generalized reducibilities of btt-type which are upwards closed under finite variation, the corresponding "Almost" class is just the class of least sets. We introduce an oracle-based bounded-error probability operator BP_{o} which, if applied to a generalized reducibility $\le_r$, yields a class of sets $\mathsf{BP}_{\mathrm{o}}(\le_r)$. Assuming that $\le_r$ is upwards closed under finite variation, we show that Almost_r is always contained in $\mathsf{BP}_{\mathrm{o}}(\le_r)$ and that in fact for a wide class of generalized reducibilities both classes coincide. The latter result then yields that $\mathsf{Almost}_{\mathrm{tt}}^{\mathsf{P}}$ coincides with BPP, as has been shown previously by Bennett and Gill [4]. Indeed they showed that not only $\mathsf{Almost}_{\mathrm{tt}}^{\mathsf{P}}$ but also $\mathsf{Almost}_{\mathrm{T}}^{\mathsf{P}}$ coincides with BPP and similarly it is shown in [7] that not only $\mathsf{Almost}_{\mathrm{btt}}^{\mathsf{P}}$ but also $\mathsf{Almost}^{\mathsf{P}}_{\log n-\mathrm{T}}$ coincides with P. While these two latter results are beyond the scope of this article it is shown in [12] that both results rely on a basically combinatorial principle which applies to time bounded (and in fact also to space bounded) deterministic reducibilities but apparently not to relativized classes defined in terms of randomized or nondeterministic computations. Thus in particular results such as $\mathsf{Almost}^{\mathsf{NP}} = \mathsf{BP} \cdot \mathsf{NP}$ and $\mathsf{Almost}^{\mathsf{PH}} = \mathsf{PH}$ due to Nisan and Wigderson [14] seem to be outside the range of this approach. For further work in the direction of showing results on random oracles for comprising classes of bounded reducibilities which satisfy certain conditions see [6, 8, 9], as well as the related article [17].

1.3 Notation

For notation not explained here or below in the text, see the textbooks by Balcázar, Díaz, and Gabarró [3] and by Odifreddi [15]. The set $\mathbb{N} = \{0, 1, \dots\}$ of natural numbers will be identified with the set $\{0,1\}^* = \{\lambda, 0, 1, 00, \dots\}$ of finite binary strings via the uniquely determined order isomorphism which takes the standard ordering $\leq$ on $\mathbb{N}$ to the length-lexicographical ordering on $\{0,1\}^*$. Subsets of $\mathbb{N}$ are identified with their characteristic functions and $2^{\mathbb{N}}$ denotes the powerset of $\mathbb{N}$. The set of all functions from $\mathbb{N}$ to $\mathbb{N}$ is denoted by $\mathbb{N}^{\mathbb{N}}$. Note that unless explicitly attributed as being partial, all functions and functionals are meant to be total.

If not explicitly stated otherwise, upper case Latin letters always denote subsets of $\mathbb{N}$ and for example we will use "for all sets A and B" instead of the more clumsy expression "for all subsets A and B of $\mathbb{N}$" and similarly $\{A \subseteq \mathbb{N} : \dots\}$ is shortened to $\{A : \dots\}$. Upper-case greek letters $\Gamma, \Delta, \dots$ denote functionals, that is functions from $2^{\mathbb{N}}$ to $2^{\mathbb{N}}$.

Lower-case Greek letters $\alpha, \beta, \gamma, \dots$ denote partial characteristic functions, that is (total) functions from some subset I of $\mathbb{N}$ to $\{0,1\}$. The domain of a partial characteristic function α is denoted by $\mathrm{dom}(\alpha)$. A partial characteristic function is finite iff its domain is finite. The symbol $\sqsubseteq$ denotes the partial ordering on partial characteristic functions where $\alpha \sqsubseteq \beta$ iff $\mathrm{dom}(\alpha)$ is a subset of $\mathrm{dom}(\beta)$ and α agrees with β on all arguments in $\mathrm{dom}(\alpha)$. Equivalently, $\alpha \sqsubseteq \beta$ iff the graph of α is a subset of the graph of β. For sets A and I, the term $A|I$ denotes the uniquely determined partial characteristic function $\alpha \sqsubseteq A$ with domain I.

A set A is a finite variation of a set B, written $A =^* B$, iff A and B differ at most at finitely many places. An n-ary relation $\mathcal{P}$ on $2^{\mathbb{N}}$ is closed under finite variation iff for all sets $A_1, A_1', \dots A_n, A_n'$ with $A_i =^* A_i'$ for $i = 1, \dots, n$, we have $\mathcal{P}(A_1, \dots, A_n)$ iff $\mathcal{P}(A_1', \dots, A_n')$. A binary relation $\leq_r$ on $2^{\mathbb{N}}$ is upwards closed under finite variation iff for all sets A, B_0, and B_1 with $B_0 =^* B_1$, we have $A \leq_r B_0$ iff $A \leq_r B_1$. Observe that a reflexive and transitive relation $\leq_r$ is closed under finite variation iff it is upwards closed under finite variation.

Recall from the introduction that μ refers to the measure on $2^{\mathbb{N}}$ obtained by independent tosses of a fair coin. We write conditional measures as $\mu[\ .\ |\ .\ ]$. In case the abbreviation is not ambiguous, usually we shorten expressions such as $\mu[\ \{A \subseteq \mathbb{N} : \mathcal{P}(A)\}\ ]$ to $\mu[\ \mathcal{P}(A)\ ]$, and similarly for conditional measures. The lower cone $\leq_r (A)$ of a set A with respect to a binary relation $\leq_r$ on $2^{\mathbb{N}}$ is the class $\{X : X \leq_r A\}$, and similarly, the upper cone of A is the class $\{X : A \leq_r X\}$.

Effective reducibilities will be denoted by the relation symbol $\leq$ with appropriate sub- and superscripts which indicate the type of oracle access allowed and the corresponding resource bounds, respectively. We distinguish reducibilities of Turing type (T), where the oracle can be asked adaptively (i.e., a query might depend on the answers to previous queries asked on the same input) and reducibilities of truth-table type (tt), where the oracle has to be asked non-adaptively (i.e., for every input the queries have to be computed in advance without accessing the oracle). Special cases of the latter are reducibilities of btt-type (btt), where for each reduction there is a constant which bounds the number of oracle queries asked on a single input, and reducibilities of k-truth-table type (k-tt), where for all reductions the numbers of queries is bounded by the single constant k. Finally, a reducibility of many-one type is a reducibility of 1-tt type where the evaluation of the oracle query is always positive, i.e., if on input x the oracle is queried at place z while reducing set A to oracle B, then x is in A iff z is in B.

For resource-bounded reducibilities such as $\leq_{\mathrm{T}}^{\mathsf{P}}$, the class of resource bounds is indicated by the superscript, while for example $\leq_{\mathrm{T}}$ denotes an effective reducibility of Turing type which might run in arbitrary time and space. We consider polynomial (P) and exponential (E) time bounds, which are given by functions of the form $|x|^c + c$ and $2^{c|x|+c}$, as well as logarithmic (log) and polynomial (PSPACE) space bounds, which are given by functions of the forms $c \log |x| + c$ and $|x|^c + c$; here c always stands for a constant.

2 Separating Generalized Reducibilities

Generalized Use. For bounded reducibilities, diagonalization results are often shown by considering the use of the oracle Turing machines which are involved in the definition of the bounded reducibilities under consideration. For generalized reducibilities, instead we will consider the generalized use of continuous functionals as introduced in Definition 7.

Proposition 6. *Let Γ be a continuous functional and let x be in $\mathbb{N}$. Then among all subsets I of $\mathbb{N}$ which satisfy*

$$A|I \ = \ B|I \ \textit{implies} \ \Gamma(A,x) = \Gamma(B,x) \quad \textit{for all sets } A, B \ . \tag{2}$$

there is a least one (with respect to set theoretical inclusion) which is actually finite.

Definition 7. *In the situation of Proposition 6, we write $u(\Gamma, x)$ for the least set which satisfies (2) and we call this set the* GENERALIZED USE *of Γ at place x.*

Proof (of Proposition 6). Let Γ be a continuous functional and let x be in $\mathbb{N}$. First note that the existence of a finite set I that satisfies (2) amounts to the fact that $\Gamma(A, x)$ can be characterized by some truth table condition on A; that this is the case follows due to compactness of $2^{\mathbb{N}}$ by the same argument as in the effective case of a recursive functional Γ (see for example [15], p.269).

Thus in order to prove Proposition 6 it is sufficient to show that the sets I which satisfy (2) are closed under intersection. So let I_0 and I_1 be two such sets and let the sets A and B agree on $I_0 \cap I_1$. Fix a set C which agrees with A on I_0 and agrees with B on I_1. Now, $\Gamma(., x)$ is defined for the arguments A, B, and C and $\Gamma(C, x)$ is equal to $\Gamma(A, x)$, by assumption on I_0, and is equal to $\Gamma(B, x)$, by assumption on I_1, that is, $\Gamma(A, x)$ is equal to $\Gamma(B, x)$. □

Remark 8. *Consider the following equivalent characterization of the concept of generalized use. A number z is in the generalized use $u(\Gamma, x)$ of a reduction Γ at x iff there is a set X such that the values of $\Gamma(X \cup \{z\}, x)$ and $\Gamma(X \setminus z, x)$ differ. First, if z is not in $u(\Gamma, x)$, then for all sets X, both values agree by definition of generalized use. Conversely, assuming that for all sets X both values are the same, we infer that z cannot be in $u(\Gamma, x)$ because otherwise also $I = u(\Gamma, x) \setminus z$ would satisfy (2), thus contradicting the minimality of $u(\Gamma, x)$.*

Given a reduction Γ and an argument x, from Remark 8 it should be clear, for example, that $u(\Gamma, x)$ is equal to I in the special case where for all sets A the value of $\Gamma(A, x)$ is just the conjunction of $A|I$ and that the assertion remains valid with conjunction replaced by disjunction or parity.

We will show in subsequent sections that many of the standard diagonalization arguments employed in order to separate reducibilities ultimately rely on the fact that the reducibilities to be separated work with a generalized use of different cardinality. Beyond these applications, we consider the concept of generalized use as a complexity theoretic tool of independent interest. For example it is shown in [12] that in terms of generalized use we can characterize bounded reducibilities which induce distributive degree structures.

Honest Reductions. In the proof of Proposition 11 we will give a first example how the concept generalized use can be applied in diagonalization argument. Before, we have to introduce some further notation.

Definition 9. *Let Γ be a reduction and let I be some set.*

- *The reduction Γ is* HONEST ON *I iff there is some function f from $\mathbb{N}$ to $\mathbb{N}$ such that for all x in I, if y is in $u(\Gamma, x)$ then x is less than or equal to $f(y)$. The reduction Γ is* HONEST *iff Γ is honest on $\mathbb{N}$.*
- *The reduction Γ has* DISJOINT USE ON *I iff for every pair x and y of distinct elements of I, the sets $u(\Gamma, x)$ and $u(\Gamma, y)$ are disjoint. The reduction Γ has* DISJOINT USE *iff it has disjoint use on $\mathbb{N}$.*

Remark 10. *The concepts of honesty and disjoint use are closely related. In fact it is not so hard to see that if a reduction is honest on some infinite set I then it has disjoint use on an infinite subset of I, and conversely, if a reduction has disjoint use on some infinite set J then it is honest on an infinite subset of J. Thus a reduction is honest on an infinite set iff it has disjoint use on an infinite set.*

Observe that an honest reduction Γ respects finite variation in the sense that $A =^* B$ implies $\Gamma(A) =^* \Gamma(B)$ for all sets A and B. The concept of an honest reduction has been used by Bennett and Gill, see their Condition 4 [4, p.98] and further references given there. The honest reductions as defined in Definition 9 might more precisely be called $\mathbb{N}^\mathbb{N}$-honest, in accordance with standard terminology according to which a reduction is $\mathcal{F}$-honest for some subclass $\mathcal{F}$ of $\mathbb{N}^\mathbb{N}$ iff there is some f in $\mathcal{F}$ such that on input x the reduction does only depend on places y of the oracle with $x \leq f(y)$. Finally note that there is a dated use of the term *honest* according to which *honesty* refers to a concept which now is usually called time-constructibility.

Diagonalization. Proposition 11 gives some indication how honest reductions might be applied in diagonalization arguments. In the proof of Proposition 11 we use an abstract version of techniques employed by Ladner, Lynch and Selman [10] for separating several variants of polynomial time bounded reducibilities. In fact we obtain many of their separation results as immediate corollaries to Proposition 11. Here, however, we obtain separating sets which are recursive, while Ladner et al. showed that there are separating sets which can be computed in deterministic time $2^{|x|}$.

Proposition 11. *Let $\mathcal{R}$ be a reduction cover for a generalized reducibility $\leq_r$. Let Γ be an honest reduction such that for every reduction Δ in $\mathcal{R}$ there are infinitely many x where $u(\Gamma, x)$ is not contained in $u(\Delta, x)$.*

Then Γ is not an $\leq_r$-reduction, that is, there is some set B where $\Gamma(B)$ is not $\leq_r$-reducible to B. In case in addition the reduction cover $\mathcal{R}$ is effective and the reduction Γ is recursive, we can choose the separating set B to be recursive.

Proof. We construct the set B by a finite extension construction, where we assume that at the beginning of stage s of the construction the already specified part of B is given by a finite partial characteristic function τ_s. At stage s we let Δ be the sth reduction in $\mathcal{R}$ and we pick some x such that the set $u(\Gamma, x)$ neither intersects the domain of τ_s nor is contained in $u(\Delta, x)$. We choose an element z of $u(\Gamma, x)$ which is not in $u(\Delta, x)$. For the remainder of this proof, for every set X, we refer by X_0 to the set $X \setminus z$, and by X_1 to the set $X \cup \{z\}$. By Remark 8, we choose a set X where $\Gamma(., x)$ differs on X_0 and X_1, and we let Y be equal to $\langle X, \tau_s \rangle$ according to Definition 15, i.e., Y agrees with X except on the domain of τ_s where Y agrees with τ_s.

Then by choice of x and Y, the function $\Gamma(., x)$ differs on Y_0 and Y_1, while $\Delta(Y_0, x)$ and $\Delta(Y_1, x)$ are both the same. So we simply choose i such that $\Gamma(Y_i, x)$ differs from $\Delta(Y_i, x)$ and we let τ_{s+1} be equal to $Y_i|I$ where I is a finite initial segment of the natural numbers which properly extends the domain of τ_s and contains $u(\Gamma, x)$ and $u(\Delta, x)$. The second assertion in Proposition 11 then follows because under the additional assumptions given the construction of the set B can be made effective. □

Remark 12. *For further use, observe that Proposition 11 remains valid (and can be shown by essentially the same proof) if we drop the the assumption that*

Γ is honest and require instead that for every reduction Δ in $\mathcal{R}$ there is an infinite set J such that Γ is honest on J and for all x in J, the set $u(\Gamma, x)$ is not contained in $u(\Delta, x)$.

3 Separating Generalized Reducibilities by Random Oracles

Kolmogorov 0-1 law and Lebesgue density theorem. For reductions Γ and Δ, classes such as

$$\{A : \Gamma(A, x) \neq \Delta(A, x)\} \quad \text{and} \quad \{A : \Gamma(A, x) = B\}$$

are always measurable because they are elements of the σ-algebra generated by the measurable sets of the form $\{X : \alpha \sqsubseteq X\}$ where α is a finite partial characteristic function. Likewise, for a generalized reducibility upper and lower cones are always measurable and the same holds for the class of oracles which separates two generalized reducibilities. For generalized reducibilities which are closed under finite variation, all such classes are closed under finite variation themselves and thus in fact have either measure 0 or measure 1 due to the Kolmogorov 0-1 law.

Theorem 13 (Kolmogorov 0-1 law). *Every measurable subclass of $2^{\mathbb{N}}$ which is closed under finite variation has either measure zero or measure one.*

The Kolmogorov 0-1 law follows from the Lebesgue density theorem stated as Theorem 14 because given a class which is closed under finite variation then, intuitively speaking, if for some α, we can amplify the conditional probability of the class relative to $\{X : \alpha \sqsubseteq X\}$, then we can in fact amplify the probability of the class itself. We omit the proofs of Theorems 13 and 14 and refer the reader to Oxtoby [16] for a more comprehensive account of the Lebesgue density theorem.

Theorem 14 (Lebesgue density theorem). *Let $\mathcal{S}$ be some measurable subclass of $2^{\mathbb{N}}$ where $\mu[\ \mathcal{S}\ ]$ differs from 0. Then for every rational $\delta < 1$, there is some partial characteristic function α with finite domain such that we have*

$$\mu[\ A \textit{ in } \mathcal{S} \mid \alpha \sqsubseteq A\ ] \ \geq \ \delta\ .$$

Occasionally, we will refer to applications of Theorem 14 by the expression PROBABILITY AMPLIFICATION according to the Lebesgue density theorem. In Definition 44 we will consider another standard technique for probability amplification where the error of a randomized computation is diminished by first iterating the computation and then taking a majority vote.

Finite Patching and Probability Amplification. In the sequel, we will frequently use the following transformation on functionals: given a functional Γ, obtain a new functional by applying Γ not to its actual set argument, but to a set which has been overwritten at finitely many places.

Definition 15. *Let α be a finite partial characteristic function.*

- *The* α-PATCH $\langle A, \alpha\rangle$ *of a set A is the unique subset of* $\mathbb{N}$ *which agrees with the partial characteristic function α on arguments in* $\mathrm{dom}(\alpha)$ *and agrees with A, otherwise.*
- *The* α-PATCH *of a functional Γ, denoted by Γ_α, is defined by*

$$\Gamma_\alpha(A) \ := \ \Gamma(\langle A, \alpha\rangle) \ .$$

We denote the transition from a functional to its α-patch as FINITE PATCHING.

Remark 16. *From a measure-theoretic point of view, finite patching corresponds to the transition to the conditional measure. For example for all functionals Γ and Δ and for all sets C, we have*

$$\mu[\ \Gamma_\alpha(A) = \Delta_\alpha(A)\ ] \ = \ \mu[\ \Gamma(A) = \Delta(A) \mid \alpha \sqsubseteq A\ ] \tag{3}$$

and

$$\mu[\ \Gamma_\alpha(A) = C\ ] \ = \ \mu[\ \Gamma(A) = C \mid \alpha \sqsubseteq A\ ] \ . \tag{4}$$

Consequently, in case $\mu[\ \Gamma(A) = C\ ]$ differs from 0, then by probability amplification according to the Lebesgue density theorem, for every $\delta < 1$ we can choose some finite partial characteristic function α where $\mu[\ \Gamma_\alpha(A) = C\ ]$ is at least δ.

Separations by Random Oracles. In case we want to proof that two generalized reducibilities $\leq_r$ and $\leq_s$ can be separated by random oracles, it suffices to show that there exist an $\leq_s$-reduction Γ and a reduction cover $\mathcal{R}$ for $\leq_r$ such that every reduction in $\mathcal{R}$ differs from Γ for almost all oracles. In fact, for such Γ and $\mathcal{R}$ we find that the class

$$\{A : \Gamma(A) \not\leq_r A\} \ = \ \bigcap_{\Delta \in \mathcal{R}} \{A : \Gamma(A) \neq \Delta(A)\}$$

is contained in a countable intersection of classes of measure 1, and hence has measure 1 by σ-additivity of μ. As a consequence, for almost all sets A, the lower $\leq_s$-cone of A is not contained in its lower $\leq_r$-cone. Informally, we call such a functional Γ a DIAGONALIZING REDUCTION. By the preceding discussion, in order to show that two generalized reducibilities can be separated by random oracles it is sufficient to show that there is a diagonalizing reduction. Diagonalizing reductions correspond to the "test languages" used by Bennett and Gill [4].

Lemma 17 states a handy sufficient criterion for a reduction to be diagonalizing. The content and the intended applications of Lemma 17 are basically the same as of Lemma 1 in [4]; however, by applying Theorem 14, the formulation of the assumptions and the proof become considerably simpler.

Lemma 17. *Two reductions Γ and Δ differ on almost all sets iff there is some rational $\varepsilon > 0$ where for all finite partial characteristic functions α, we have*

$$\mu[\, \Delta_\alpha(A) \neq \Gamma_\alpha(A)\,] \;\geq\; \varepsilon \; . \tag{5}$$

Proof. First, assume that Γ and Δ differ on almost all sets. Then, in particular, they differ on almost all sets which extend a given partial characteristic function α and thus (5) is true with ε equal to 1.

Conversely, let Γ and Δ agree on a class of non-zero measure. Then by probability amplification according to the Lebesgue density theorem, for every given $\varepsilon > 0$ there is some finite partial characteristic function α such that Γ_α and Δ_α agree on a class of measure at least $1-\varepsilon$, i.e., for all $\varepsilon > 0$ there is some α such that equation (5) is false. □

In connection with Proposition 18, note that the parity of a finite partial characteristic function α is 0 if α attains the value 1 on an even number of elements in its domain and, otherwise, the parity of α is 1.

Proposition 18. *Let Γ be an honest reduction where for all B and x, the value of $\Gamma(B,x)$ is just the parity of $B|u(\Gamma,x)$. Further let $\mathcal{R}$ be a reduction cover for a generalized reducibility $\leq_r$ such that for every reduction Δ in $\mathcal{R}$ there are infinitely many x where $u(\Gamma,x)$ is not contained in $u(\Delta,x)$. Then for almost all oracles B, the set $\Gamma(B)$ is not $\leq_r$-reducible to B.*

Proof. We show that Γ is a diagonalizing reduction, that is, for every Δ in $\mathcal{R}$, the reductions Δ and Γ differ for almost all oracles. Here, according to Lemma 17, it suffices to show that for every Δ in $\mathcal{R}$ and for every finite partial characteristic function α, the reductions Δ_α and Γ_α differ with probability at least 1/2. Given such Δ and α, by assumption on Γ we can choose x such that the set $u(\Gamma,x)$ neither intersects the domain of α nor is contained in $u(\Delta,x)$. We choose an element z of $u(\Gamma,x)$ which is not in $u(\Delta,x)$ and for every given set X we let $X_0 = X \setminus \{z\}$ and $X_1 = X \cup \{z\}$. As a consequence, we find that for every set X, firstly, $\Delta_\alpha(X_0)$ and $\Delta_\alpha(X_1)$ agree at x whereas, secondly, $\Gamma_\alpha(X_0)$ and $\Gamma_\alpha(X_1)$ differ at x. Here the latter assertion follows because Γ, and hence by choice of x also Γ_α, computes the parity of $X_i|u(\Gamma,x)$, i=1,2. Thus for exactly one of the sets X_0 and X_1 the reductions Δ_α and Γ_α differ at x. Now X has been chosen arbitrarily and consequently Δ_α and Γ_α differ at x for exactly half of the possible assignments to the union of $u(\Delta_\alpha,x)$ and $u(\Gamma_\alpha,x)$, that is, the two reductions differ at x with probability 1/2. □

In Corollary 19, we write $\leq^{\mathsf{P}}_{f(x)-\mathrm{tt}}$ for the restriction of polynomial time bounded truth-table reducibility where at each place x at most $f(x)$ places of the oracle might be queried.

Corollary 19. *Let f and g be in $\mathbb{N}^{\mathbb{N}}$ such that $f(x) > g(x)$ holds for infinitely many x and the function $x \mapsto 1^{f(x)}$ can be computed in polynomial time. Then the relations $\leq^{\mathsf{P}}_{f(x)-\mathrm{tt}}$ and $\leq^{\mathsf{P}}_{g(x)-\mathrm{tt}}$ can be separated by random oracles. More precisely, for almost all oracles A the lower cone $\leq^{\mathsf{P}}_{f(x)-\mathrm{tt}}(A)$ is not contained in $\leq^{\mathsf{P}}_{g(x)-\mathrm{tt}}(A)$.*

Corollary 20 has been independently obtained by Lutz and Mayordomo: the corollary is implicit in Lemma 5.6 of the journal version of [11].

Corollary 20. *The relations* $\leq_{\mathrm{tt}}^{\mathsf{P}}$ *and* $\leq_{\mathrm{btt}}^{\mathsf{P}}$ *can be separated by random oracles.*

Proof. Both corollaries follow easily from Proposition 18. In the case of Corollary 19 it is sufficient to observe that there is a $\leq_{\mathrm{tt}}^{\mathsf{P}}$-reduction Γ as required in the proposition, say, the reduction which on input x returns the parity of the restriction of its oracle to the set $\{x1, \ldots, x1^{f(|x|)}\}$. Corollary 20 can be shown in the same manner or can even be derived as a special case of Corollary 19 by observing that for all sets A, the lower $\leq_{|x|-\mathrm{tt}}^{\mathsf{P}}$-cone of A is contained in its lower $\leq_{\mathrm{tt}}^{\mathsf{P}}$-cone and the lower $\leq_{\mathrm{btt}}^{\mathsf{P}}$-cone of A is contained in its lower $\leq_{\log|x|-\mathrm{tt}}^{\mathsf{P}}$-cone. □

Remark 21. *Corollary 20 can be shown for other generalized reducibilities by virtually the same proof. Trivially, the corollary remains valid in case we replace the relation* $\leq_{\mathrm{tt}}^{\mathsf{P}}$ *by a weaker reducibility such as* $\leq_{\mathrm{T}}^{\mathsf{P}}$ *and the relation* $\leq_{\mathrm{btt}}^{\mathsf{P}}$ *by a stronger one such as* $\leq_{\mathrm{m}}^{\mathsf{P}}$. *To some extent we can also take the opposite direction. For example it should be obvious from its proof that Corollary 20 remains valid if we simultaneously replace* $\leq_{\mathrm{tt}}^{\mathsf{P}}$ *with truth-table reducibility restricted to logarithmic space and replace* $\leq_{\mathrm{btt}}^{\mathsf{P}}$ *by the relation* $\leq_{\mathrm{btt}}$, *that is, the restriction of Turing reducibility to reductions of bounded truth-table type. Here we find in addition that for almost all oracles their* $\leq_{\mathrm{btt}}$*-lower cone is not contained in their lower* $\leq_{\mathrm{tt}}^{\mathsf{P}}$*-cone, i.e., the lower cones with respect to these two reducibilities are mutually not contained in each other. For a proof, it suffices to construct a recursive set* A *which is not in the "Almost" class of logarithmic space bounded btt-reducibility. In order to do so, choose for the latter reducibility an effective reduction cover* $\mathcal{R} = \{\Delta_0, \Delta_1, \ldots\}$ *which is closed under finite patching and then let* $A(e) = 0$ *iff the measure of* $\{X : \Delta_e(X, e) = 0\}$ *is at most* $1/2$. *If there were* Δ *in* $\mathcal{R}$ *such that the class* $\{X : \Delta(X) = A\}$ *had nonzero measure, by probability amplification according to the Lebesgue density theorem there would be a finite patch* Δ_α *of* Δ *in* $\mathcal{R}$ *such that* $\{X : \Delta_\alpha(X) = A\}$ *has measure strictly larger than* $1/2$, *thus contradicting the construction of* A.

Remark 22. *Observe the close resemblance between Propositions 11 and 18 and between their corresponding proofs. Intuitively speaking, given an honest reduction* Γ *and a reduction cover* $\mathcal{R}$ *for some generalized reducibility* $\leq_r$ *such that each reduction in* $\mathcal{R}$ *uses at infinitely many places* x *strictly less of the oracle than* Γ, *then the former proposition asserts that there is some set* A *where* $\Gamma(A)$ *is not* $\leq_r$*-reducible to* A, *while the latter proposition asserts that this is true for almost all* A *in case* Γ *in addition computes the parity of the bits it scans.*

4 Reducibilities of bounded truth-table-type

Reductions of finite norm. In Sect. 1.3 we have introduced the standard concepts of bounded truth-table and k-truth-table reducibility for effective reductions defined via oracle Turing machines. We will now extend these concepts to generalized reducibilities.

Definition 23. *The* NORM $\kappa(\Gamma)$ *of a reduction* Γ *is defined by*

$$\kappa(\Gamma) \;:=\; \max_{x \text{ in } \mathbb{N}} |u(\Gamma, x)|$$

in case the maximum exists and, otherwise, $\kappa(\Gamma)$ *is equal to* ∞.

Definition 24. *Given some* k *in* $\mathbb{N}$, *a generalized reducibility* $\leq_r$ *is of* k-TT-TYPE *iff it has a reduction cover in which every reduction has norm at most* k. *A generalized reducibility* $\leq_r$ *is of* BTT-TYPE *iff it has a reduction cover in which every reduction has finite norm.*

In general, given a function f from $\mathbb{N}$ to $\mathbb{N}$, a reduction Γ might be called $f(x)$ use bounded in case for all x in $\mathbb{N}$, the cardinality of $u(\Gamma, x)$ is at most $f(x)$, and given a class $\mathcal{F}$ of functions, a generalized reducibility might be called $\mathcal{F}$ use bounded iff it has a reduction cover in which every reduction is use bounded by some function in $\mathcal{F}$. In Sect. 5 we will consider generalized reducibilities with non-constant use bounds, while this section is devoted to generalized reducibilities of btt-type. In connection with the latter, we will frequently apply the the following concept of a normalized reduction.

Definition 25. *A reduction* Δ *is* NORMALIZED *iff there is an infinite set* J *such that, firstly, the reduction* Δ *is honest on* J *and, secondly, for all* x *in* J *we have*

$$|u(\Delta, x)| \;=\; \kappa(\Delta) \;,$$

that is, the generalized use of Δ *has maximum cardinality for all* x *in* J. *A reduction cover is* NORMALIZED *iff it contains only normalized reductions.*

Remark 26 states a useful equivalent characterization of normalized reductions.

Remark 26. *A reduction* Δ *of finite norm is* not *normalized iff there is a finite set* D *such that* $u(\Delta, x)$ *intersects* D *whenever* $u(\Delta, x)$ *has maximum cardinality* $\kappa(\Delta)$. *First, assume that* Δ *is normalized. Then* Γ *is honest on an infinite set where it attains its maximum use and thus there cannot be a set* D *as above. Next, assume that there is no set* D *as above. Then for every* z *in* $\mathbb{N}$ *there is an* $x > z$ *such that* $u(\Delta, x)$ *has cardinality* $\kappa(\Delta)$ *and does not intersect the set* $\{0, \ldots, z\}$. *For the scope of this remark, let the least such* x *be denoted by* $u(z)$ *and obtain infinitely many* $x_0 < x_1 < \ldots$ *as required in the definition of the concept of normalized reduction by defining* $x_0 = 0$ *and* $x_{i+1} = u(z)$ *where* z *is the maximum element in the union of* $\{x_i\}$ *and the sets* $u(\Delta, x_0)$ *through* $u(\Delta, x_i)$.

In Remark 27 we argue that usually the concepts of k-tt and btt type for generalized reducibilities introduced in Definition 24 are consistent with the corresponding standard notation for bounded reducibilities. In Proposition 28 this claim is made more precise in the case of reducibilities of k-tt type.

Remark 27. In Section 1.3 we have introduced the usual concept of bounded reducibilities of btt-type, where it is required that the reducibility can be defined by an effective listing of oracle Turing machines which all have a constant bound on the number of queries that might be asked on a single input. Now the latter concept coincides with the concept of generalized reducibilities of btt-type as introduced in Definition 24 for virtually all reducibilities to be found in the literature (and a similar assertion holds for for reducibilities of k-tt type). Obviously, every bounded reducibility of btt-type is also of btt-type if viewed as a generalized reducibility, while on the other hand, given a bounded reducibility $\leq_s$ which is not of btt-type in the standard sense, then usually there is an honest $\leq_s$-reduction Γ such that the cardinality of the generalized use of Γ is unbounded, whence Proposition 11 shows that $\leq_s$ is not a generalized reducibility $\leq_r$ of btt-type in the sense of Definition 24.

Observe in connection with Proposition 28 that the requirement on the existence of a least set holds also for a generalized reducibility of many-one type if, as usual, it is defined in such a way that for example in the case of $\leq_{\mathrm{m}}^{\mathrm{P}}$ all sets computable in polynomial time are reducible to the sets $\emptyset$ and $\mathbb{N}$.

Proposition 28. *Let $\leq_r$ be a generalized reducibility which is closed under finite variation and which possesses a least set A_0, that is, $A_0 \leq_r B$ for all sets B. Furthermore, let there be an effective reduction cover for $\leq_r$ which contains only reductions of norm at most k_0 for some natural number k_0.*

Then for all natural numbers k, the relation $\leq_r$ has a reduction cover which contains only reductions of norm at most k iff it has an effective reduction cover which contains only reductions of norm at most k.

Proof. For $k \geq k_0$ there is nothing to prove. So it suffices to show inductively for $k = k_0 - 1, \dots, 0$ that if $\leq_r$ has a reduction cover which contains only reductions of norm at most k, then $\leq_r$ actually has an effective reduction cover of the latter type. So fix $k < k_0$ and assume that $\leq_r$ has a reduction cover which contains only reductions of norm at most k. By induction we obtain that $\leq_r$ has an effective reduction cover $\mathcal{R}$ which contains only reductions of norm at most $k+1$.

Fix an arbitrary reduction Γ in $\mathcal{R}$ which has norm $k+1$. If Γ were normalized, this would contradict the variant of Proposition 11 stated in Remark 12. Thus by Remark 26 there is some finite set D which intersects $u(\Gamma, x)$ whenever the latter set has maximum cardinality $k+1$. Now for all sets B, with $\beta = B|I_\delta$ the sets $\Gamma(B)$ and $\Gamma_\beta(B)$ are the same while, by choice of β, the reduction Γ_β is k use bounded. Now $\leq_r$ is closed under finite variation, whence we can assume that $\mathcal{R}$ is closed under finite patching, and as Γ was an arbitrary reduction in $\mathcal{R}$ with norm $k+1$, every fact $A \leq_r B$ is witnessed by a reduction in $\mathcal{R}$ which has norm at most k. As a consequence we obtain an effective reduction cover for $\leq_r$ which contains only reductions of norm at most k if we alter every reduction Γ in $\mathcal{R}$ such that for all x and all oracles B, we change $\Gamma(B,x)$ to $A_0(x)$ in case $|u(\Gamma, y)| = k+1$ for some $y \leq x$ (and $\Gamma(B,x)$ remains unchanged, otherwise). □

It is immediate from the definition of normalized reduction cover that if a generalized reducibility has a normalized reduction cover, then it is of btt-type. Lemma 29 shows that for generalized reducibilities which are upwards closed under finite variation this implication can be reversed.

Lemma 29. *Every generalized reducibility of btt-type which is upwards closed under finite variation has a normalized reduction cover.*

Proof. We let $\mathcal{R}$ be some reduction cover for $\leq_s$ which witnesses that $\leq_s$ is of btt-type. By $\leq_r$ being upwards closed under finite variation we can assume that $\mathcal{R}$ is closed under finite patching. We show by induction on $\kappa(\Delta)$ that for every reduction Δ in $\mathcal{R}$ one of the following cases applies

(i) The reduction Δ is normalized.
(ii) Every fact $A \leq_s B$ which is witnessed by Δ is also witnessed by some reduction in $\mathcal{R}$ with norm strictly smaller than the norm of Δ.

As a consequence, by eliminating all reductions for which Case (ii) applies, we obtain a reduction cover as required. More precisely, if we denote by $\mathcal{R}'$ the reduction cover obtained by this elimination, then by an easy induction on k we infer that for all k in $\mathbb{N}$, for all Δ in $\mathcal{R}$ with norm at most k, and for every given set B there is some reduction Δ_0 in $\mathcal{R}'$ with norm at most k such that Δ and Δ_0 agree on B.

Now, concerning our induction on the norm $\kappa(\Delta)$, in case Δ has norm 0, the set $J = \mathbb{N}$ witnesses that Δ is normalized. In the induction step, given some reduction Δ in $\mathcal{R}$ where $\kappa(\Delta) > 0$, there is nothing to prove in case Δ is normalized. So we can assume that Δ is not normalized and that consequently by Remark 26 there is some finite set D where $u(\Delta, x)$ intersects D for all x where the cardinality of $u(\Delta, x)$ is equal to $\kappa(\Delta)$. Then, given some set B, if we let β be the restriction of B to D, the reductions Δ and Δ_β agree on B. But, the reduction Δ_β has norm strictly smaller than Δ because for every place x where cardinality of $u(\Delta, x)$ is maximal, the set $u(\Delta, x)$ intersects the domain of β. □

Proposition 30. *Let $\leq_r$ be a generalized reducibility of btt-type which is upwards closed under finite variation. Then* Almost_r *coincides with the class* L_r *of least sets.*

Proof. The set L_r is always a subset of Almost_r, so it remains to show that every given set A in Almost_r is also in L_r. By Lemma 29, we can choose a normalized reduction cover $\mathcal{R}$ for $\leq_r$. By σ-additivity of μ, there is some reduction Δ in $\mathcal{R}$ where the class

$$\Delta^{-1}(A) \ := \ \{B : A \leq_r B\}$$

has measure different from 0. We first assume for a contradiction that Δ has norm strictly larger than 0. By choice of $\mathcal{R}$ the reduction Δ is normalized. We choose a set J_Δ which witnesses the latter fact and infer by Remark 10 that there is an infinite subset J of J_Δ such that Δ has disjoint use on J. As a consequence, firstly, for all x in J the probability that $\Delta(B, x)$ differs from $A(x)$ is at least $1/2^{\kappa(\Delta)}$, and secondly, these errors are stochastically independent. As a consequence, the probability that there occurs no error for all x in J below y becomes arbitrarily small for sufficiently large y. Now, the class $\Delta^{-1}(A)$ contains only sets where there occurs no error at all, and thus, contrary to our assumption, has measure 0.

So Δ has norm 0, that is, Δ maps all sets to the same set. But $\Delta^{-1}(A)$ has measure strictly greater than 0, whence Δ maps some set, and then in fact all sets, to A, i.e., A is in L_r. □

From Proposition 30 the following corollaries are immediate.

Corollary 31. $\mathsf{Almost}^{\mathsf{P}}_{\mathrm{m}} = \mathsf{Almost}^{\mathsf{P}}_{\mathrm{btt}} = \mathsf{P}$.

Corollary 32. $\mathsf{Almost}_{\mathrm{m}} = \mathsf{Almost}_{\mathrm{btt}} = REC$.

Corollary 31 is due to Ambos-Spies [1, 2] and Book and Tang [7]. Concerning Corollary 32, in fact a stronger result is known: even for Turing reducibility $\leq_{\mathrm{T}}$ we have $\mathsf{Almost}_{\mathrm{T}} = \mathrm{REC}$, see [18, Sect. 10, Theorem 1].

We will use Lemma 33 together with Lemma 29 while showing separations by random oracles for reducibilities of btt-type, that is, when reductions with a constant use bound are involved.

Lemma 33. *Let $\leq_r$ be a generalized reducibility of btt-type which is upwards closed under finite variation. Let Γ be some reduction of finite norm such that for all finite partial characteristic functions α, the functional Γ_α is not an $\leq_r$-reduction. Then for almost all sets A, the set $\Gamma(A)$ is not contained in $\leq_r(A)$.*

Proof. We let $\mathcal{R}$ be some reduction cover for $\leq_r$ which witnesses that $\leq_r$ is of btt-type. Given Δ in $\mathcal{R}$ we fix k in $\mathbb{N}$ such that Δ and Γ both have norm at most k. Then given a finite partial characteristic functions α, consider the reductions Δ_α and Γ_α. Both have norm at most k and by assumption they differ for some set B and some number argument x. But then the disagreement at x has probability at least $\varepsilon := 1/2^{2k}$ because it occurs for all sets which agree with B on the union of $u(\Gamma, x)$ and $u(\Delta, x)$. Now the assertion of the lemma is immediate by Lemma 17 because we have shown for an arbitrary reduction Δ in $\mathcal{R}$ and for all finite partial characteristic functions α that the reductions Γ_α and Δ_α differ with probability at least $\varepsilon > 0$. □

Proposition 34. *Let $\leq_r$ and $\leq_s$ be generalized reducibilities which are upwards closed under finite variation. Let k be in $\mathbb{N}$ where $\leq_r$ is of k-tt-type, while $\leq_s$ is of btt-type, but not of k-tt-type. Then $\leq_r$ and $\leq_s$ can be separated by random oracles. More precisely, for almost all oracles A, the lower cone $\leq_s(A)$ is not contained in $\leq_r(A)$.*

Proof. We choose a reduction cover for $\leq_s$ according to Lemma 29. The relation $\leq_s$ is by assumption not of k-tt-type, and consequently this reduction cover contains a reduction Γ with norm strictly larger than k. Now, given some finite partial characteristic function α, also the norm of Γ_α is strictly larger than k because by choice of Γ the reduction Γ attains its maximal use on some infinite set J_Γ on which Γ is honest. But then Remark 12 shows that for all finite partial characteristic functions α the functional Γ_α is not an $\leq_r$-reduction. Thus the relation $\leq_r$ and the reduction Γ satisfy the assumption of Lemma 33, and we are done. □

Corollary 35 contains an easy consequence of Lemma 33. In fact, the corollary follows already directly from Proposition 18. The way Corollary 35 is shown here, however, has the advantage that the proof carries over to reducibilities of btt-type which do not allow to compute parity functions as it is required in the assumption of Proposition 18. In particular, Corollary 35 extends to polynomial-time bounded btt-type-reducibility where the truth-table is either required to be a disjunction or a conjunction of the queries made.

Corollary 35. *[Book and Tang] For every fixed k in $\mathbb{N}$, the bounded reducibilities $\leq^{\mathsf{P}}_{(k+1)-\mathrm{tt}}$ and $\leq^{\mathsf{P}}_{k-\mathrm{tt}}$ can be separated by random oracles. More precisely, for almost all oracles the lower cone with respect to the first relation is not contained in the lower cone with respect to to the second one.*

Proof. The proof of Corollary 35 is an immediate consequence of Propositions 11 and 34 where as diagonalizing reduction we can for example use a reduction Γ such that $\Gamma(B, x)$ is always 0, except when x has the form 0^n and B does not contain any of the strings $0^n1, \ldots, 0^n1^{k+1}$. □

Corollary 35 extends to other reducibilities and in particular it can be shown by virtually the same proof with $\leq^{\mathsf{P}}_{k-\mathrm{tt}}$ replaced by $\leq_{k-\mathrm{tt}}$. The latter form of the corollary is an immediate consequence of the main result of Book, Lutz, and Martin in [5]. They show that for every Martin-Löf-random language A and for every fixed $k \geq 0$, the lower cone $\leq^{\mathsf{P}}_{k+1-\mathrm{tt}}(A)$ is not contained in $\leq_{k-\mathrm{tt}}(A)$, whence the latter assertion holds for almost all oracles A because the class of Martin-Löf-random languages has measure 1.

The next proposition shows that generalized reducibilities of btt-type can be separated by random oracles from a wide class of generalized reducibilities which are not of btt-type.

Proposition 36. *Let $\leq_r$ and $\leq_s$ be generalized reducibilities. Let $\leq_r$ be of btt-type and let there be an $\leq_s$-reduction Γ such that Γ is honest and there are arbitrarily large k in $\mathbb{N}$ where the set $\{x \in \mathbb{N} : |u(\Gamma, x)| = k\}$ is infinite. Then for almost all oracles A, the lower cone $\leq_s(A)$ is not contained in $\leq_r(A)$.*

Proof. We choose some reduction cover which witnesses that $\leq_r$ is of btt-type. Then, given some reduction Δ in $\mathcal{R}$ there is some k_0 in $\mathbb{N}$ where Δ is k_0 use bounded. We choose some $k > k_0$ in $\mathbb{N}$ where there are arbitrarily large x such that the cardinality of $u(\Gamma, x)$ is k. We infer as in the proof of Lemma 33 that for all finite partial characteristic functions α the α-patches of Γ and Δ differ with probability at least $1/2^{k_0+k}$, which then finishes the proof by Lemma 17. □

We have already seen in Corollary 19 that $\leq^{\mathsf{P}}_{f(x)-\mathrm{tt}}$ and $\leq^{\mathsf{P}}_{g(x)-\mathrm{tt}}$ can be separated by random oracles in case f is easy to compute and is infinitely often strictly greater than g. While the proof of Corollary 19 worked by a diagonalizing reduction which computes the parity of $f(x)$ places of the oracle, we will now derive from Proposition 36 a separation by random oracles between $\leq^{\mathsf{P}}_{f(x)-\mathrm{tt}}$ and $\leq^{\mathsf{P}}_{\mathrm{btt}}$ where the diagonalizing reduction can be defined in terms of Boolean functions other than the parity function. This way we obtain in particular that $\leq^{\mathsf{P}}_{\mathrm{btt}}$ can be separated by random oracles from the reducibilities $\leq^{\mathsf{P}}_{f(x)-\mathrm{ctt}}$ and $\leq^{\mathsf{P}}_{f(x)-\mathrm{dtt}}$, i.e., the restrictions of $\leq^{\mathsf{P}}_{f(x)-\mathrm{tt}}$ where the truth-table is always a conjunction and a disjunction, respectively, of the queries asked.

Corollary 37. *Let g be an unbounded function from $\mathbb{N}$ to $\mathbb{N}$ which is computable in time polynomial in $\max\{|x|, f(x)\}$. Then the relations $\leq^{\mathsf{P}}_{f(x)-\mathrm{tt}}$, $\leq^{\mathsf{P}}_{f(x)-\mathrm{ctt}}$, and $\leq^{\mathsf{P}}_{f(x)-\mathrm{dtt}}$ can all be separated by random oracles from $\leq^{\mathsf{P}}_{\mathrm{btt}}$. More precisely, given one of the former relations then for almost all oracles X, the lower cone of X with respect to the given relation is not contained in the lower $\leq^{\mathsf{P}}_{\mathrm{btt}}$-cone of X.*

Proof. We show the assertion for the relation $\leq^{\mathsf{P}}_{f(x)-\mathrm{ctt}}$ and leave the almost identical considerations for the remaining cases to the interested reader. Fix a Turing machine M and a polynomial p such that M computes $f(x)$ in $p(\max\{|x|, f(x)\})$ steps. Then for all x, by simulating $p(|x|)$ many steps of the computation of M on input x, we will either be able to compute $f(x)$ or, in case of timeout, to verify $f(x) > |x|$. Thus if we let $k_0(x) = f(x)$ in the former case and let $k_0(x) = |x|$ in case of timeout, the function k_0 is computable in polynomial time and we have $k_0(x) \leq f(x)$ for all x.

By a standard looking back construction we obtain a polynomial time computable function k_1 such that $k_1(x) \leq k_0(x)$ for all x in $\mathbb{N}$ and k_1 attains every natural number infinitely often. Here we let $k_1(x)$ be equal to the first component of a coded pair $\langle k, j\rangle$ which is selected as follows. First we use a total of $|x|$ steps in order to list successively the coded pairs which have been selected on inputs $0, 1, \ldots$; then we select the least pair $\langle k, j\rangle$ with $k \leq k_0(x)$ which has not been listed. Now we are done, because the functional Γ where $\Gamma(A, x)$ is the conjunction of $A(x0), A(x0^2), \ldots, A(x0^{k_1(x)})$ is a $\leq^{\mathsf{P}}_{f(x)-\mathrm{ctt}}$-reduction and, by construction of k_1, satisfies the assumption of Proposition 36. □

Remark 38. *Given a generalized reducibility $\leq_r$ of btt-type which is closed under finite variation, we can construct a generalized reducibility $\leq_s$ which is not of btt-type, but which cannot be separated by random oracles from $\leq_r$. In order to define a reduction cover for $\leq_s$, we pick some reduction cover for $\leq_r$ and we let Δ be some arbitrary reduction in $\mathcal{R}$. We define a diagonalizing reduction Γ which is equal to Δ, except that for all strings x of the form 0^n, in case the set argument A does not contain any string of length n, we let Γ differ from the nth reduction in $\mathcal{R}$ at x. Then adding Γ to $\mathcal{R}$ yields a new reducibility which is not of btt-type according to Proposition 11. However, the probability that Γ differs at some string 0^n from Δ is $1/2^n$ and the sum of these error probabilities over all n is bounded. Thus we infer from the Borel-Cantelli lemma that the class of sets where Γ differs from Δ for infinitely many places has measure 0, that is, for almost all oracles A the set $\Gamma(A)$ is equal to a finite variation of $\Delta(A)$ and, by $\leq_r$ being closed under finite variation, is contained in $\leq_r(A)$.*

5 Reducibilities not of bounded truth-table-type

In the proofs of their results on separations by random oracles, Bennett and Gill use reductions Γ of a special form which can informally be described as follows:

In order to compute $\Gamma(B, x)$, first we query non-adaptively the strings in some finite set D which might depend on x, followed by a single adaptive query $q(B, x)$ which is not in D. Then we let

$$\Gamma(B, x) \ := \ B(q(B, x)) \ .$$

Here the adaptive query depends on the non-adaptive queries in such a way that in case B_0 and B_1 differ for some argument in D, then $q(B_0, x)$ differs from $q(B_1, x)$.

Observe that while for each single set argument B and for each place x exactly $|D| + 1$ queries are made, the size of the generalized use of Γ at x is equal to $|D| + 2^{|D|}$. In Definition 39, we try to capture the essential features of such reductions in terms of generalized use.

Definition 39. *Let Γ be a reduction and let x be in $\mathbb{N}$. The reduction Γ is (single adaptive query)* USE BOOSTING AT *x iff there is some finite subset D of $\mathbb{N}$ such that for all partial characteristic functions α and β with domain D we have*

- $|u(\Gamma_\alpha, x)| \ = \ 1$,
- *if α differs from β, then $u(\Gamma_\alpha, x)$ and $u(\Gamma_\beta, x)$ are disjoint.*

The reduction Γ is (single adaptive query) USE BOOSTING *iff Γ is use boosting at every x in $\mathbb{N}$.*

Proposition 40. *Let $\leq_r$ and $\leq_s$ be generalized reducibilities, and let $\mathcal{R}$ be a reduction cover for $\leq_r$. Let Γ be a $\leq_s$-reduction which is honest and use boosting and where for all Δ in $\mathcal{R}$ we have*

$$\liminf_{x \to \infty} \frac{|u(\Delta, x)|}{|u(\Gamma, x)|} \ < \ 1 \ . \tag{6}$$

Then $\leq_r$ and $\leq_s$ can be separated by random oracles. More precisely, for almost all sets A, the set $\Gamma(A)$ is not contained in $\leq_r(A)$.

Proof. By Lemma 17, it is sufficient to show that for every Δ in $\mathcal{R}$ there is some $\varepsilon > 0$ such that for all finite partial characteristic functions α the α-patch of Δ and Γ differ with probability at least ε. For all x in $\mathbb{N}$, we choose some set $D(x)$ which witnesses that Γ is use boosting at x, and we let $n(x)$ be equal to the cardinality of $D(x)$, that is, we have for all x in $\mathbb{N}$

$$|u(\Gamma, x)| \ = \ 2^{n(x)} + n(x) \ .$$

Then, given some reduction Δ in $\mathcal{R}$, by (6) we choose some rational $\delta_0 < 1$ where the set

$$I := \{x \text{ in } \mathbb{N} : \frac{|u(\Delta, x)|}{|u(\Gamma, x)|} \leq \delta_0\}$$

is infinite. In case $|u(\Gamma, x)|$ is bounded by some constant for all x in I, then for all these x it must be strictly larger that $|u(\Delta, x)|$ and we are done by an argument similar to the one used in the proof of Lemma 33. On the other hand, if $|u(\Gamma, .)|$ is not bounded on I, then neither is $n(x)$, and consequently for every rational $\varepsilon > 0$ there is an infinite subset J of I where for all x in J we have

$$2^{n(x)} + n(x) \leq (1+\varepsilon)\, 2^{n(x)} .$$

By definition of I and because Γ is assumed to be use boosting, we then have for all x in J

$$\delta_0 \geq \frac{|u(\Delta, x)|}{|u(\Gamma, x)|} = \frac{|u(\Delta, x)|}{2^{n(x)} + n(x)} \geq \frac{1}{(1+\varepsilon)} \cdot \frac{|u(\Delta, x)|}{2^{n(x)}} .$$

In particular, if we choose $\varepsilon > 0$ so small that $\delta := (1+\varepsilon)\delta_0$ is strictly less than 1, then for all x in J we have

$$|u(\Delta, x)|/2^{n(x)} \leq \delta < 1 .$$

Recall that we want to apply Lemma 17. So, given some finite partial characteristic function α, by honesty of Γ we choose x in J such that $u(\Gamma, x)$ does not intersect dom(α). Then by definition of J and because $u(\Delta_\alpha, x)$ is contained in $u(\Delta, x)$, a fraction of at least $1 - \delta$ of the $2^{n(x)}$ "adaptive queries" of Γ is *not* contained in $u(\Delta_\alpha, x)$. So Γ_α and Δ_α differ at place x with probability greater or equal to $(1-\delta) \cdot (1/2)$ because each of the adaptive queries is "selected" with equal probability, and in case the selected adaptive query is not in $u(\Delta_\alpha, x)$, then with probability $1/2$ the two reductions will differ at x. □

In Corollary 41, we state some sample applications of Proposition 40. Recall in this connection that the relations $\leq_{\mathrm{T}}^{\mathsf{E}}$ and $\leq_{\mathrm{T}}^{\mathsf{PSPACE}}$ are Turing reducibility restricted to time bounds of the form $2^{c|x|+c}$ and to polynomial space, respectively.

Corollary 41. *The following pairs of reducibilities can be separated by random oracles:*

- *the relations* $\leq_{\mathrm{T}}^{\mathsf{P}}$ *and* $\leq_{\mathrm{tt}}^{\mathsf{P}}$*,*
- *the relations* $\leq_{\mathrm{T}}^{\mathsf{P}}$ *and* $\leq_{\mathrm{T}}^{\log}$ *[Bennett and Gill],*
- *the relations* $\leq_{\mathrm{T}}^{\mathsf{E}}$ *and* $\leq_{\mathrm{T}}^{\mathsf{PSPACE}}$ *[Bennett and Gill].*

Here in each case for almost all oracles the lower cone with respect to the first relation is not contained in the lower cone with respect to the second one.

Proof. The first assertion is immediate from Proposition 40 because there is a use boosting $\leq_{\mathrm{T}}^{\mathsf{P}}$-reduction with polynomially many non-adaptive queries for each x in $\mathbb{N}$.

The remaining assertions follow by the crucial observation due to Bennett and Gill that the number of potential queries of an oracle Turing machine T, and therefore the size of the generalized use of the reduction computed by T, is bounded by the number of configurations of T. Here we assume as usual a machine model where the query tape is erased after a query has been answered, that is, the configuration after each query determines the next query. By this argument, the reductions computed by oracle Turing machines which use logarithmic and polynomial space are polynomially and $2^{c \cdot |x|}$ use bounded, respectively. Now the second and third assertion follow by Proposition 40 because there are honest and use boosting $\leq_{\mathrm{T}}^{\mathsf{P}}$ - and $\leq_{\mathrm{T}}^{\mathsf{E}}$-reductions where the cardinality of the generalized use exceeds $2^{|x|}$ and $2^{2^{|x|}}$, respectively. □

A bounded-error probability operator based on oracles. According to Proposition 30, for a generalized reducibility $\leq_r$ of btt-type which is closed under finite variation, the class L_r of least sets coincides with Almost_r. Concerning reducibilities which are not of btt-type, the situation is apparently less simple, for example, $\mathsf{Almost}_{\mathrm{T}}^{\mathsf{P}}$ is equal to BPP and is not known to be equal to $\mathsf{L}_{\mathrm{T}}^{\mathsf{P}} = \mathsf{P}$. In the remainder of this section, we consider characterizations of the class Almost_r for generalized reducibilities which are not necessarily of btt-type. Note that the techniques used in this section are standard and have mostly, at least implicitly, been used before.

For a start, we consider upper and lower bounds for Almost_r. While for all relations $\leq_r$ the class L_r is a trivial lower bound, the oracle-based version of the BP operator introduced in Definition 42 yields an upper bound.

Definition 42. *The* ORACLE-BASED BOUNDED-ERROR PROBABILITY CLASS *with respect to a generalized reducibility $\leq_r$, which we denote by $\mathsf{BP}_{\mathrm{o}}(\leq_r)$, contains exactly the sets A where there is some $\leq_r$-reduction Γ and some rational $\varepsilon > 0$ such that we have for all x in $\mathbb{N}$*

$$\mu[\ \{B : A(x) = \Gamma(B, x)\}\ ] \ \geq\ 1/2 + \varepsilon\ . \tag{7}$$

The main difference between the operator BP_{o} and the usual BP operator is that for BP_{o}, the random bits are given via some oracle, that is, by a set argument, and not by some advice string which is part of the number input, and that consequently in the case of BP_{o} the number of available random bits is not bounded in advance by some polynomial, but by the reduction Γ itself. Using the BP_{o} operator, we obtain an upper bound for the class Almost_r.

Proposition 43. *If the generalized reducibility $\leq$ is upwards closed under finite variation, then we have*

$$\mathsf{L}_r \subseteq \mathsf{Almost}_r \subseteq \mathsf{BP}_{\mathrm{o}}(\leq_r)\ . \tag{8}$$

Proof. The first inclusion is immediate from the observation that for every set A in L_r the functional Γ defined by $\Gamma(X, x) = A(x)$ is an $\leq_r$-reduction. In order to show the second inclusion, let A be in Almost_r. By σ-additivity of the measure μ, each reduction cover for $\leq_r$ contains some $\leq_r$-reduction Γ such that we have $\mu[\ \{B : A = \Gamma(B)\}\ ] > 0$. By probability amplification according to the

Lebesgue density theorem there is a partial characteristic function α with finite domain such that we have

$$\mu[\{B : A = \Gamma_\alpha(B)\}] \;>\; 3/4 \;.$$

But then Γ_α witnesses that A is in $\mathsf{BP_o}(\leq_r)$ because, firstly, Γ_α is an $\leq_r$-reduction due to $\leq_r$ being upwards closed under finite variation and, secondly, for every x in $\mathbb{N}$ the probability for a disagreement between Γ_α and A at x cannot exceed the probability $1/4$ for a disagreement somewhere. □

Definition 44. *A generalized reducibility allows* PROBABILITY AMPLIFICATION *(more precisely: oracle based probability amplification of order $1 - 1/2^{c|x|}$) iff for every A in $\mathsf{BP_o}(\leq_r)$ and every c in $\mathbb{N}$ there is some $\leq_r$-reduction Γ such that we have for all x in $\mathbb{N}$*

$$\mu[\{B : A(x) = \Gamma(B, x)\}] \;\geq\; 1 - \frac{1}{2^{c|x|+c}} \;.$$

By the standard technique of first iterating the computation, while using independent parts of the random oracle for the different iterations, and then applying a majority vote, we obtain that reducibilities such as $\leq_{\mathrm{T}}^{\mathsf{P}}$ or $\leq_{\mathrm{tt}}^{\mathsf{P}}$ allow probability amplification, for details see [3, Vol. II, Sect. 11]. Here the corresponding techniques can be transferred to the abstract setting and we leave it to the reader to formulate sufficient conditions for a generalized reducibility to allow probability amplification.

Proposition 45. *Let $\leq_r$ be a generalized reducibility, which is upwards closed under finite variation and allows probability amplification. Then Almost_r coincides with $\mathsf{BP_o}(\leq_r)$.*

Proof. By Proposition 40, it remains to show that $\mathsf{BP_o}(\leq_r)$ is contained in Almost_r. Assuming that A is in $\mathsf{BP_o}(\leq_r)$, by definition of probability amplification, there is some reduction Γ such that the probability that $\Gamma(B)$ differs from A at some place x is at most $1/2^{2|x|+2}$. Now the probability that a reduction makes an error somewhere cannot be larger than the sum of the probabilities for an error at some x in $\mathbb{N}$. In case of Γ, the latter sum is strictly below 1 and consequently the reduction Γ maps a class of non-zero measure to A, that is, the upper cone of A has measure different from 0. Now the upper cone of A is closed under finite variation, and hence has measure 1 by the Kolmogorov 0-1 law. □

Remark 46. *Book, Vollmer and Wagner independently have introduced an operator BP^2 which is very close to our $\mathsf{BP_o}$-operator and have shown analogs of Propositions 43 and 45 where in particular in the assertion $\mathsf{BP_o}$ is replaced by BP^2, see [8, 9] and [13]. The main difference between the two operators is that the BP^2-operator is applied to, in our terms, an effective reduction cover $\mathcal{R}$ and in its definition it is required that (7) holds for some reduction in $\mathcal{R}$, whereas in Definition 42 equation (7) is required to hold for some arbitrary $\leq_r$-reduction* *where $\leq_r$ is the reducibility given by $\mathcal{R}$. The mentioned results in [8, 9] and Proposition 45 show that if appropriately defined concepts of closure under finite variation and probability amplification apply to $\mathcal{R}$ and $\leq_r$, then the classes $\mathsf{BP}^2(\mathcal{R})$ and $\mathsf{BP}_\mathrm{o}(\leq_r)$ are both equal to Almost_r, that is, both definitions yield the same concept.*

Note, however, that for contrived choices of $\mathcal{R}$ the BP^2-operator might yield unexpected results and similarly, it is not obvious what happens if the BP_o-operator is applied to a generalized reducibility which does not satisfy the assumption of Proposition 45. For example, there is an effective reduction cover $\mathcal{R}$ for $\leq_\mathrm{T}^\mathsf{P}$ such that $\mathsf{BP}^2(\mathcal{R})$ is empty. Here we take any effective reduction cover for $\leq_\mathrm{T}^\mathsf{P}$ and for each reduction Δ in this reduction cover, we let $\mathcal{R}$ contain two reductions Δ_0 and Δ_1 where for $i = 0, 1$ and for all sets X, the set $\Delta_i(X)$ is equal to $\Delta(X)$ in case $X(0) = i$ and, otherwise, $\Delta_i(X)$ is equal to the complement of $\Delta(X)$. Then for every reduction Γ in $\mathcal{R}$ and for all x, we find that for an oracle X chosen at random the value of $\Gamma(X, x)$ will be 1 with probability exactly $1/2$.

Corollary 47. *The class $\mathsf{Almost}_\mathrm{tt}^\mathsf{P}$ coincides with BPP. [Bennett and Gill]*

Proof. By Proposition 45, the class $\mathsf{Almost}_\mathrm{tt}^\mathsf{P}$ coincides with $\mathsf{BP}_\mathrm{o}(\leq_\mathrm{tt}^\mathsf{P})$. But given a $\leq_\mathrm{tt}^\mathsf{P}$-reduction Γ which witnesses that a set A is in $\mathsf{BP}_\mathrm{o}(\leq_\mathrm{tt}^\mathsf{P})$, it is easy to construct a polynomial time bounded Turing machine T which witnesses that A is in BPP. Here we construct T such that it simulates Γ while using its random string in place of its random oracle and consequently for all inputs x, the probability that Γ accepts x when given a random oracle is equal to the probability that T accepts when given a random string of polynomial length as additional input. Similarly, given a Turing machine which witnesses that a set A is in BPP we can construct a polynomial time bounded oracle Turing machine which witnesses that A is in $\mathsf{BP}_\mathrm{o}(\leq_\mathrm{tt}^\mathsf{P})$. □

6 Conclusion

For the sake of simplicity, assume for the scope of this conclusion that all reducibilities considered are closed under finite variation. In terms of generalized use, a concept which we consider to be of independent interest in complexity theory, we have given a formal account of the fact that standard diagonalization arguments employed for separating reducibilities ultimately do not rely on the effectivity of the reductions involved but instead exploit differences in the cardinality of the generalized use. This remark applies to separations with respect to single oracles in the style of Ladner, Lynch, and Selman [10] (Proposition 11) but also to separations by random oracles. Here we obtain a rather nice picture in the realm of reducibilities of btt-type: every pair of generalized reducibilities of btt-type where one reducibility is of k-tt-type but the other one is not can be separated by random oracles (Proposition 34). Furthermore, we obtain results for generalized reducibilities which are not of btt-type (Propositions 36 and 40) which easily imply for a large class of resource-bounded computation models that the corresponding Turing, truth table, and bounded truth table reducibilities pairwise can be separated by random oracles.

Concerning "Almost" classes, again the picture is easy for generalized reducibility of btt-type where the "Almost" class always collapses to the class of least sets (Proposition 30). For generalized reducibilities in general we could show that the corresponding "Almost" class is contained in the class obtained by applying the $\mathsf{BP}_\circ$ operator and that in fact both classes coincide in case the reducibility allows probability amplification.

7 Acknowledgement

We like to thank the anonymous referees of preliminary versions of this article for helpful suggestions and corrections.

References

[1] Klaus Ambos-Spies. Randomness, relativizations, and polynomial reducibilities. In *Proc. First Structure in Complexity Theory Conference*, Lecture Notes in Computer Science 223, pages 23–34. Springer-Verlag, 1986.

[2] Klaus Ambos-Spies. Randomness, relativizations, and polynomial reducibilities. Unpublished research paper, 1986.

[3] José Luis Balcázar, Josep Díaz, and Joaquim Gabarró. *Structural Complexity*, volumes I and II. Springer-Verlag, 1995 and 1990.

[4] Charles H. Bennett and John Gill. Relative to a random oracle A, $P^A \neq NP^A \neq co - NP^A$ with probability 1. *SIAM Journal on Computing*, 10:96–113, 1981.

[5] R. V. Book, J. H. Lutz, and D. M. Martin Jr. The global power of additional queries to random oracles. *Information and Computation*, 120:49-54, 1995. A preliminary version appeared in: P. Enjalbert, E. W. Mayr, and K W. Wagner, editors, *11th Annual on Symposium on Theoretical Aspects of Computer Science 1994*, Lecture Notes in Computer Science 775, pages 403–414. Springer-Verlag, 1994.

[6] Ronald V. Book, Jack H. Lutz, and Klaus W. Wagner. An observation on probability versus randomness with applications to complexity classes. *Mathematical Systems Theory*, 27:201–209, 1994.

[7] Ronald V. Book and Shouwen Tang. Polynomial-time reducibilities and "almost all" oracle sets. *Theoretical Computer Science*, 81:35–47, 1991.

[8] Ronald V. Book, Heribert Vollmer, and Klaus W. Wagner. On type-2 probabilistic quantifiers. In: Friedhelm Meyer auf der Heide and Burkhard Monien, editors, *23rd International Colloquium on Automata, Languages and Programming '96*, Lecture Notes in Computer Science 1099, pages 369–380, Springer-Verlag 1996. A preliminary version was published as Technical Report 123, Institut für Informatik, Julius-Maximilians-Universität, Würzburg, Germany, August 1995.

[9] Ronald V. Book, Heribert Vollmer, and Klaus W. Wagner. Probabilistic type-2 operators and "Almost"-classes. Computational Complexity 7:265-289, 1998. Preliminary versions have been published as [8] and as Technical Report TR96-035, Electronic Colloquium on Computational Complexity, 1996.

[10] Richard E. Ladner, Nancy Ann Lynch, and Alan L. Selman. A comparison of polynomial time reducibilities. *Theoretical Computer Science*, 1:103–123, 1975.

[11] J. H. Lutz, E. Mayordomo. Cook versus Karp-Levin: separating completeness notions if NP is not small. *Theoretical Computer Science* 164:141–163, 1996. A preliminary version appeared in: P. Enjalbert, E. W. Mayr, and K W. Wagner, editors, *11th Annual on Symposium on Theoretical Aspects of Computer Science 1994*, Lecture Notes in Computer Science 775, pages 415–426. Springer-Verlag, 1994.

[12] Wolfgang Merkle. *A Generalized Account of Resource Bounded Reducibilities.* Doctoral dissertation, Universität Heidelberg, Mathematische Fakultät, INF 288, Heidelberg, Germany, 1997.

[13] Wolfgang Merkle and Yongge Wang. Random separations and "Almost" classes for generalized reducibilities. In Jiří Wiedermann and Petr Hájek, editors, *Mathematical Foundations of Computer Science*, Lecture Notes in Computer Science 969, pages 179–190. Springer-Verlag, 1995.

[14] Noam Nisan and Avi Wigderson. Hardness vs randomness. *Journal of Computer and System Sciences*, **49** (1994), 149–167. An extended abstract was published in *Proceedings of the 29th Annual IEEE Symposium on Foundations of Computer Science*, pages 2–11, IEEE, 1988.

[15] Piergiorgio Odifreddi. *Classical Recursion Theory.* North-Holland, Amsterdam, 1989.

[16] John C. Oxtoby. *Maß und Kategorie (Measure and Category).* Springer-Verlag, 1971.

[17] Kenneth W. Regan and James S. Royer. On closure properties of bounded two-sided error complexity classes. *Mathematical Systems Theory*, 28:229–243, 1995.

[18] Gerald E. Sacks. *Degrees of Unsolvability.* Annals of Mathematics Studies 55, Princeton University Press, 1963.