

THE GLOBAL POWER OF ADDITIONAL QUERIES TO P-RANDOM ORACLES*

WOLFGANG MERKLE†

Abstract. We consider separations of reducibilities by random sets. First, we show a result on polynomial time-bounded reducibilities that query their oracle nonadaptively: for every p-random set R , there is a set that is reducible to R with $k + 1$ queries but is not reducible to any other p-random set with at most k queries. This result solves an open problem stated in a recent survey paper by Lutz and Mayordomo [*EATCS Bulletin*, 68 (1999), pp. 64–80]. Second, we show that the separation result above can be transferred from the setting of polynomial time-bounds to a setting of rec-random sets and recursive reducibilities. This extends the main result of Book, Lutz, and Martin [*Inform. and Comput.*, 120 (1995), pp. 49–54] who, by using different methods, showed a similar separation with respect to Martin-Löf-random sets. Moreover, in both settings we obtain similar separation results for truth-table versus bounded truth-table reducibility.

Key words. separation of reducibilities, random sets, resource-bounded measure, effective measure, resource-bounded reducibilities, effective reducibilities, bounded truth-table reducibility, truth-table reducibility

AMS subject classifications. 03D15, 03D30, 68Q15, 68Q30

PII. S0097539700366711

1. Introduction and related work. We consider separations of reducibilities in the context of resource-bounded measure theory. In the following, we use the symbol \leq with appropriate sub- or superscripts to denote binary relations on Cantor space, the class of all sets of natural numbers. These binary relations are meant as reducibilities and, in particular, we will consider polynomial time-bounded reducibilities of the following types: Turing (p-T), truth-table (p-tt), bounded truth-table (p-btt), and bounded truth-table restricted to at most k queries (p-btt(k)); see section 2 for more precise definitions. We say two reducibilities \leq_r and \leq_s are *separated by an oracle* A if the lower spans of A with respect to these reducibilities, i.e., the classes $\{X : X \leq_r A\}$ and $\{X : X \leq_s A\}$, differ. It is easy to see that two reducibilities are different (as binary relations on Cantor space) iff they are separated by some oracle. Beyond this simple observation, the question of which reducibilities are separated by what kind of oracles has been the object of intensive studies. Here, for a given pair of reducibilities, typical questions are the following. Are there separating oracles of low complexity? How comprising is the class of separating oracles? Which properties are sufficient for being a separating oracle?

Ladner, Lynch, and Selman [12] considered separations of the usual polynomial time-bounded reducibilities in the range between many-one- (p-m-) and p-T-reducibility. They showed that for every distinct pair of such reducibilities, there is a separating oracle that can be computed in exponential time. In their seminal paper [6], Bennett and Gill then obtained results about *separations by random oracles*, i.e., they showed that certain pairs of reducibilities are separated by almost all oracles in the sense that the class of separating oracles has measure 1 with respect to uniform measure on Cantor space. Subsequently, for any $k > 0$ it was shown for p-T-, p-

*Received by the editors February 4, 2000; accepted for publication (in revised form) January 30, 2001; published electronically September 26, 2001.

<http://www.siam.org/journals/sicomp/31-2/36671.html>

†Universität Heidelberg, Mathematisches Institut, Im Neuenheimer Feld 294, D-69120 Heidelberg, Germany (merkle@math.uni-heidelberg.de).

tt-, p-btt-, p-btt($k + 1$)-, and p-btt(k)-reducibility that the two latter reducibilities are separated by almost all tally oracles [10] and that in fact every pair of distinct reducibilities chosen from this list can be separated by random oracles [16, 21].

A separation by random oracles can be expressed equivalently by saying that the class of oracles that do not separate the reducibilities under consideration has uniform measure 0. Lutz and Mayordomo [16] could show for certain pairs of polynomial time-bounded reducibilities of truth-table type that the class of nonseparating oracles does not just have uniform measure 0 but can in fact be covered by a martingale that is computable in polynomial time. Typically, their results are derived from the assumption that for both reducibilities the number of queries is bounded by a function in the input length and that the two bounding functions are related in a specific way, say, one is growing faster than the square of the other. In the special case where the bounding functions are constant, they showed that for every natural number k , there is a martingale computable in polynomial time that covers all oracles that do not separate p-btt($k + 1$)- and p-btt(k)-reducibility; hence, in particular, these reducibilities are separated by every p-random oracle. The latter can be rephrased by saying that these reducibilities are locally separated by the class of p-random oracles. Here, formally, a nonempty class \mathbf{C} *locally separates* two given reducibilities if and only if for every set A in \mathbf{C} , the lower spans of A with respect to these reducibilities are different.

We say a class \mathbf{C} *globally separates* two given reducibilities in case for every set A in \mathbf{C} there is a set B that is reducible to A with respect to one of the given reducibilities but B is not reducible to any set in \mathbf{C} with respect to the other reducibility. Moreover, in case such a set B exists not for all but just for some sets A in \mathbf{C} , we say that \mathbf{C} yields a weak global separation of the reducibilities under consideration.

The definitions of the concepts of separations given above are meant for being applied with pairs of reducibilities \leq_r and \leq_s where $X \leq_r Y$ implies $X \leq_s Y$. In this situation, the definitions are no more symmetric in the sense that for example sets A and B witnessing a global separation by a class \mathbf{C} must satisfy $B \leq_s A$ and $B \not\leq_r Z$ for all Z in \mathbf{C} . In distinguishing local and global separation we follow Book, Lutz, and Martin [8], who discuss such separations for the classes of Martin-Löf-random, tally, and sparse sets.

In the sequel we will consider global separations by various classes of random sets. Such investigations can be viewed as part of a more comprising research project where one asks which types of reductions are able to transform random objects into what types of far from random objects. For results in this direction and for further discussion and references see Juedes, Lathrop, and Lutz [11] as well as Lutz and Schweizer [18].

Remark 1.1. By definition, every local or global separation by a class \mathbf{C} extends trivially to every nonempty subclass of \mathbf{C} . This is false in general, however, for weak global separations. For example given an oracle A that separates p-btt(2)- and p-btt(1)-reducibility, the class $\{A, \emptyset\}$, but not its subclass $\{\emptyset\}$, yields a weak global separation of these two reducibilities.

Remark 1.2. By definition, global separations always imply the corresponding local separation. A similar remark for weak global separations in place of global separations, however, is false. In order to obtain a counterexample, consider the class \mathbf{C} that consist of all p-random sets plus a single set A that is computable in polynomial time. Then \mathbf{C} does not locally separate p-btt(1)- and p-btt(2)-reducibility because A does not separate these reducibilities. On the other hand, \mathbf{C} yields a weak

global separation of these reducibilities. The latter fact follows from Theorem 4.1 and the observation that none of the sets that witness a global separation by the class of p -random sets will be p - $btt(1)$ -reducible to A .

In Theorem 4.1, we show that the class of p -random oracles yields a global separation of p - $btt(k+1)$ - and p - $btt(k)$ -reducibility. This, together with Remark 4.3, solves Problem 7 in a recent survey article by Lutz and Mayordomo [17], where it has been asked to prove or disprove that, in our terms, the class of p -random oracles yields a weak global separation of these reducibilities. In section 5, we obtain by basically the same proof as for Theorem 4.1 that for every natural number k and any rec-random set R , there is a set that is p - $btt(k+1)$ -reducible to R but is not $btt(k)$ -reducible to any rec-random set, where $btt(k)$ -reductions are restricted to at most k nonadaptive queries and are computed by total Turing machines that might run in arbitrary time and space. Thus in particular, the class of rec-random sets globally separates $btt(k+1)$ -reducibility from $btt(k)$ -reducibility. By an easy argument similar to the one given in Remark 1.1, this yields as a special case the main result of Book, Lutz, and Martin [8], who showed, by using different methods, a corresponding separation result with respect to the class of Martin-Löf-random sets, which is a proper subclass of the class of rec-random sets. Moreover, we will argue that in both settings, i.e., for polynomial time-bounded, as well as for recursive reductions and martingales, the corresponding random sets globally separate the corresponding notions of truth-table and bounded truth-table reducibility.

2. Notation. The notation used in the following is mostly standard, for unexplained notation refer to the surveys and textbooks cited in the bibliography [4, 7, 15]. All strings are over the alphabet $\Sigma = \{0, 1\}$. We identify strings with natural numbers via the isomorphism that takes the length-lexicographical ordering on $\{\lambda, 0, 1, 00, \dots\}$ to the usual ordering on ω , the set of natural numbers. If not explicitly stated differently, the terms *set* and *class* refer to sets of natural numbers and to sets of sets of natural numbers, respectively.

A *partial characteristic function* is a (total) function from some subset of the natural numbers to $\{0, 1\}$. A partial characteristic function is *finite* iff its domain is finite. The restriction of a partial characteristic function β to a set I is denoted by $\beta|I$ and thus, in particular, for any set X , the partial characteristic function $X|I$ has domain I and agrees there with X . We identify strings of length n in the natural way with a partial characteristic function with domain $\{0, \dots, n-1\}$ and hence strings can be viewed as prefixes of sets. For a partial characteristic function α with domain $\{z_0 < \dots < z_{n-1}\}$, the *string associated with α* is the (unique) string β with domain $\{0, \dots, n-1\}$ defined by $\beta(j) = \alpha(z_j)$. For a set X and a partial characteristic function σ we write $\langle X, \sigma \rangle$ for the set that agrees with σ for all arguments in the domain of σ and agrees with X , otherwise.

We will consider the following polynomial time-bounded reducibilities: p -T, p -tt, where the queries have to be asked nonadaptively, p -btt, where for each reduction the number of queries is bounded by a constant, and, even more restrictive, p - $btt(k)$ -reducibility, where for all reductions this constant is bounded by the natural number k . The relation symbol \leq_{btt}^P refers to p -btt-reducibility, and relation symbols for other reducibilities are defined in a similar fashion. Expressions such as *p -T-reduction* and \leq_T^P -reduction will be used interchangeably. We represent p -btt-reductions by a pair of functions g and h computable in polynomial time where $g(x)$ gives the set of strings queried on input x and $h(x)$ is a truth-table of a Boolean function over k variables that specifies how the answers to the queries in the set $g(x)$ are evaluated. Here we

assume, first, via introducing dummy variables, that the cardinality of $g(x)$ is always exactly k and, second, by convention, that for $i = 1, \dots, k$, the i th argument of the Boolean function $h(x)$ is assigned the i th query in $g(x)$ where the queries are ordered by length-lexicographical ordering. All reducibilities mentioned above can be defined by specifying an appropriate sequence of total oracle Turing machines that compute the corresponding reductions. For any total oracle Turing machine M there is a corresponding functional Γ where $\Gamma(B) = A$ iff M computes the set A on oracle B . Equivalently, the functional Γ can be viewed as a binary function from pairs of sets and strings to $\{0, 1\}$ such that $\Gamma(B, x) = 1$ iff M accepts x on oracle B .

Given a reducibility r , the *lower r -span of a set A* is the class $\{X : X \leq_r A\}$ of sets that are r -reducible to A , and the *lower r -span of a class \mathcal{C}* is the class of all sets that are r -reducible to some set in \mathcal{C} .

3. Resource-bounded measure. We give a brief introduction to resource-bounded measure, which focuses on the concepts that will be used in subsequent sections. For more comprehensive accounts of resource-bounded measure theory see the recent survey papers by Ambos-Spies and Mayordomo [4] and by Lutz [15].

The theory of resource-bounded measure is usually developed in terms of *martingales*, which can be viewed as payoff functions of gambles of the following type. A player successively places bets on the individual bits of the characteristic sequence of an unknown set A or, for short, the player bets on A . The betting proceeds in rounds $i = 1, 2, \dots$, where during round i , the player receives the length $i - 1$ prefix of A and then, first, decides whether to bet on the i th bit being 0 or 1 and, second, determines the stake by specifying the fraction of the current capital that shall be bet. Formally, a player can be identified with a *betting strategy* $b : \{0, 1\}^* \rightarrow [-1, 1]$ where the bet is placed on the next bit being 0 or 1 depending on whether $b(w)$ is negative or nonnegative, respectively, and where the absolute value of the real $b(w)$ is the fraction of the current capital that shall be at stake.

The player starts with strictly positive, finite capital. At the end of each round, in case the current guess has been correct, the capital is increased by this round's stake and, otherwise, is decreased by the same amount. So given a betting strategy b , we can inductively compute the corresponding *payoff function* d by applying the equations

$$d(w0) = d(w) - b(w) \cdot d(w), \quad d(w1) = d(w) + b(w) \cdot d(w).$$

Intuitively speaking, the payoff $d(w)$ is the capital the player accumulates till the end of round $|w|$ by betting on a set that has the string w as a prefix. Conversely, any function d from strings to nonnegative reals that for all strings w satisfies the fairness condition

$$(3.1) \quad d(w) = \frac{d(w0) + d(w1)}{2}$$

induces canonically a betting function b , where

$$b(w) = \frac{d(w1) - d(w0)}{2} \cdot \frac{1}{d(w)}$$

in case $d(w)$ differs from 0 and $b(w) = 0$ otherwise. We call a function d from strings to nonnegative reals a *martingale* iff $d(\lambda) > 0$ and d satisfies the fairness condition (3.1) for all strings w .

By the preceding discussion it follows for gambles as described above that for any martingale there is an equivalent betting strategy and vice versa. We will frequently

identify martingales and betting strategies via this correspondence and, if appropriate, notation introduced for martingales will be extended to the induced betting strategies.

We say a martingale d *succeeds* on a set A if d is unbounded on the prefixes of A , i.e., if

$$\limsup_{n \in \omega} d(A| \{0, \dots, n\}) = \infty,$$

and d *succeeds* on or *covers* a class iff d succeeds on every set in the class.

It is easy to see that every countable class $\mathbf{C} = \{C_1, C_2, \dots\}$ is covered by the following betting strategy. On input w , let i be the minimal index such that w is a prefix of C_i , then bet half of the current capital on the next bit agreeing with the corresponding bit of C_i (and abstain from betting if such an index does not exist). As a consequence, most of the classes considered in complexity and recursion theory can be covered by martingales. In order to distinguish such classes in terms of coverability, one has to restrict the class of admissible martingales. Here, in general, for a given class \mathbf{C} we want to specify a class of admissible martingales that allows the covering of interesting subclasses of \mathbf{C} , but not of \mathbf{C} itself. In the context of recursion theory, this led to the consideration of recursive martingales [23, 24, 25, 27], whereas in connection with complexity classes one has to impose additional resource-bounds [1, 4, 14, 15, 20]. An effective martingale d is always confined to rational values and there is a Turing machine that on input w outputs some appropriate finite representation of $d(w)$.

Recall the definition of the *uniform measure* (or *Lebesgue measure*) on Cantor space, which describes the distribution obtained by choosing the individual bits of a set by independent tosses of a fair coin. It has been shown by Ville that a class has uniform measure 0 iff the class can be covered by some martingale [4, 26]. The latter result justifies the following notation: a class has *measure* 0 with respect to a given class of martingales iff it is covered by some martingale in the class. The aim stated above can then be rephrased: for a given class \mathbf{C} , we want to specify a class of admissible martingales such that interesting subclasses of \mathbf{C} have measure 0, but not \mathbf{C} itself.

In connection with measure on complexity classes, most attention has been received by measure concepts for the exponential time-bounded classes

$$\mathbf{E} = \mathbf{DTIME}(2^{\text{lin}}) \quad \text{and} \quad \mathbf{EXP} = \mathbf{DTIME}(2^{\text{poly}}).$$

For example, in the case of the class \mathbf{E} , Lutz proposed to use martingales that on input w are computable in time polynomial in the length of w . Observe that the latter time-bound yields the same class of martingales as the time-bound $2^{O(|x|)}$ where x is the minimal string not in the domain of w ; i.e., if w is viewed as prefix of a set A , then x is the minimal string y such that $A(y)$ is not encoded in w . Lutz could show that for every constant c , the subclass $\mathbf{DTIME}(2^{c \cdot n})$ of \mathbf{E} can be covered by such a martingale, but not \mathbf{E} itself. The class of polynomial time-bounds used to define measure on \mathbf{E} is so robust that, similar to the case of unrestricted martingales, martingales and betting strategies that can be computed in polynomial time are essentially equivalent. (However, in general, a fixed polynomial bound on the running time might not be preserved in the transition from a betting strategy to the corresponding martingale [3].) Furthermore, there is a similar correspondence between martingales and betting strategies in the case of martingales used to define measure on \mathbf{EXP} [3] and in the case of recursive martingales [24].

We say a set is *p-random* if the set cannot be covered by a martingale that is computable in polynomial time, and we write $\mathbf{p-RAND}$ for the class of all \mathbf{p} -random

sets. The notion *rec-random set* and the class *rec-RAND* of all *rec-random sets* are defined likewise with recursive martingales in place of martingales that are computable in polynomial time. Moreover, we will consider Martin-Löf-random sets [19]. These have been characterized in terms of martingales by Schnorr [24]. A set is *Martin-Löf-random* if and only if it cannot be covered by a subcomputable martingale. A martingale d is *subcomputable* iff there is a recursive function g in two arguments such that for all strings w , the sequence $g(w, 0), g(w, 1), \dots$ is nondecreasing and converges to $d(w)$.

The classes of *p-random*, *rec-random*, and *Martin-Löf random sets* all have uniform measure 1 because the class of sets on which a single martingale succeeds always has uniform measure 0 and, by σ -additivity, the same holds for every countable union of such classes. By definition, any *rec-random set* is *p-random* but the reverse implication is false as one can construct a recursive *p-random set* by diagonalizing against an appropriate weighted sum of all *p-betting strategies*. By the characterization of *Martin-Löf-random sets* stated above, it is immediate that the class of *Martin-Löf-random sets* is a subclass of *rec-RAND*. Schnorr [24] has implicitly shown that this containment is proper. For a proof, it suffices to recall that the prefixes of a *Martin-Löf-random set* can not be compressed by more than a constant while a corresponding statement for *rec-random sets* is false [13, Theorem 3.6.1 and Exercise 2.5.13].

We conclude this section by two remarks in which we describe standard techniques for the construction of martingales.

Remark 3.1. Let a finite set D be given, as well as a list $\langle D_1, \dots, D_m \rangle$ of pairwise disjoint subsets of D that all have the same cardinality $k > 0$. Then for a partial characteristic function σ with domain D and a string w of length k we might ask for the frequency

$$\alpha(\sigma, w, \langle D_1, \dots, D_m \rangle) := \frac{|\{j : w \text{ is the associated string of } \sigma|_{D_j}\}|}{m}$$

with which w occurs in σ as associated string at the positions specified by the D_i . In case the sets D_i are clear from the context, we suppress mentioning them and we write $\alpha(\sigma, w)$ for short.

If we choose the bits of σ by independent tosses of a fair coin, then for every w of length k , the expected value of $\alpha(\sigma, w)$ is $1/2^k$. For large m , only for a small fraction of all partial characteristic functions with domain D will the frequency of w deviate significantly from the expected value, as can, for example, be shown by using Chernoff bounds [22, Lemma 11.9]. By using such bounds it is indeed straightforward to show that given k and a rational $\varepsilon > 0$, we can compute a natural number $m(k, \varepsilon)$ such that for all $m \geq m(k, \varepsilon)$ and for all D and D_1, \dots, D_m as above we have

$$(3.2) \quad \frac{|\{\sigma : D \rightarrow \{0, 1\} : \frac{1}{2} \cdot \frac{1}{2^k} < \alpha(\sigma, w, \langle D_1, \dots, D_m \rangle) < \frac{3}{2} \cdot \frac{1}{2^k}\}|}{2^{|D|}} \geq 1 - \varepsilon.$$

Remark 3.2. Let I be a finite set and let Θ be a subset of all partial characteristic functions with domain I . We can easily construct a martingale that by betting on places in I , increases its capital by a factor of $2^{|I|}/|\Theta|$ for all sets B where $B|I$ is in Θ . Here the martingale takes the capital available when betting on the minimal element of I and distributes it evenly among the elements of Θ , then computing values upwards according to the fairness condition for martingales.

4. Separations by p-random oracles. Lutz and Mayordomo [16] have shown that for any *p-random set* R , the lower *p-btt(k)*-span of R is strictly contained in the

lower $p\text{-btt}(k+1)$ -span of R , i.e., the class $p\text{-RAND}$ yields a local separation of these reducibilities. In Theorem 4.1, we extend this local separation to a global separation, i.e., we show that for any p -random set R there is a set that is $p\text{-btt}(k+1)$ -reducible to R but is not $p\text{-btt}(k)$ -reducible to any p -random set.

THEOREM 4.1. *Let R be a p -random set and let k be a natural number. Then the lower $p\text{-btt}(k+1)$ -span of R is not contained in the lower $p\text{-btt}(k)$ -span of $p\text{-RAND}$.*

Proof. In order to define a set A and a $p\text{-btt}(k+1)$ -reduction (g_0, h_0) from A to R , we let $h_0(x)$ be the truth-table of the $(k+1)$ -place conjunction and we let

$$(4.1) \quad g_0(x) := \{x0^11^{k+1}, x0^21^k, \dots, x0^{k+1}1^1\}, \quad A := \{x : g_0(x) \subseteq R\}.$$

We are done if we can show that if A is $p\text{-btt}(k)$ -reducible to a set, then this set cannot be p -random. So let B be an arbitrary set and assume that A is reducible to B via the $p\text{-btt}(k)$ -reduction (g, h) . We will construct a martingale d that is computable in polynomial time and succeeds on B . To this end, let $m(., .)$ be the function defined in Remark 3.1 and define a sequence n_0, n_1, \dots with

$$(4.2) \quad n_0 = 0, \quad n_{i+1} > 2^{n_i}, \quad \log n_{i+1} > m\left(k+1, \frac{1}{2^{i+1}}\right)$$

such that given x of length n , we can compute in time $O(n^2)$ the maximal i with $n_i \leq n$. Such a sequence can be obtained by standard methods as described in the chapter on uniform diagonalization and gap languages in Balcázar, Díaz, and Gabarró [7]. For example, we can first define a sufficiently fast growing time-constructible function $r : \omega \rightarrow \omega$ and then let n_i be the value of the i -fold iteration of r applied to 0.

It is helpful to view the betting strategy of the martingale d as being performed in stages $i = 0, 1, \dots$ where the bets of stage i depend on the g -images of the strings of length n_i . While considering the queries made for strings of length n_i with $i > 0$, we will distinguish short queries with length strictly less than

$$(4.3) \quad l_i := \left\lfloor \frac{n_i}{2k} \right\rfloor$$

and long queries, i.e., queries of length at least l_i . We call two strings x and y equivalent iff, for some i , both have identical length n_i and in addition we have

$$(4.4) \quad h(x) = h(y) \quad \text{and} \quad g(x) \cap \{z : |z| < l_i\} = g(y) \cap \{z : |z| < l_i\},$$

i.e., two strings of length n_i are equivalent iff they have the same truth-table and the same set of short queries. Then for some constant c , the number of equivalence classes of strings of length n_i can be bounded from above by

$$2^{2^k} \sum_{j=0}^k \binom{2^{l_i} - 1}{j} \leq 2^{2^k} (k+1) \cdot 2^{l_i \cdot k} \leq c \cdot 2^{\frac{n_i}{2k} \cdot k} = c \cdot 2^{\frac{n_i}{2}}.$$

So the 2^{n_i} strings of length n_i are partitioned into at most $c \cdot 2^{\frac{n_i}{2}}$ equivalence classes, hence there is i_0 such that for all $i > i_0$, there is an equivalence class of cardinality at least $m_i := \lfloor \log n_i \rfloor$. For all such i , among all equivalence classes of strings of length n_i we choose one with maximal cardinality (breaking ties by some easily computable but

otherwise arbitrary rule), we let J_i contain the first m_i strings in this equivalence class, and we let

$$(4.5) \quad \alpha_i = \frac{|A \cap J_i|}{|J_i|}.$$

We show now that due to R being p -random, almost all α_i are close to $1/2^{k+1}$.

CLAIM 1. *For almost all i , α_i is contained in the open interval K defined by*

$$(4.6) \quad K := \left(\frac{1}{2} \cdot \frac{1}{2^{k+1}}, \frac{3}{2} \cdot \frac{1}{2^{k+1}} \right).$$

Proof. Fix any index $i > i_0$. Let $z_1 < \dots < z_{m_i}$ be the elements of J_i , let D_j be equal to $g_0(z_j)$ for $j = \{1, \dots, m_i\}$, and let D be the union of D_1 through D_{m_i} . Recall from Remark 3.1 the definition of the function α . For any partial characteristic function σ with domain D and any string w of length $k + 1$, $\alpha(\sigma, w)$ is equal to the fraction of all indices i among $1, \dots, m_i$ such that the string associated with $\sigma|D_i$ is equal to w . Now the truth table h_0 is just the conjunction of the queries given by g_0 and thus by construction, z_i is in A iff all strings in D_i are in R . Hence by the definitions of α_i and α , we obtain $\alpha_i = \alpha(\sigma_i, v)$ where $v = 1^{k+1}$ and σ_i is the restriction of R to places in D .

On the other hand, by choice of the m_i and by (4.2), we know that $m_i = \lfloor \log n_i \rfloor$ is larger than $m(k + 1, 1/2^i)$. By definition of the function m in Remark 3.1, it is then immediate that for all but a $1/2^i$ -fraction of all partial characteristic functions σ with domain D the value $\alpha(\sigma, v)$ is in K . If α_i , and hence also $\alpha(\sigma_i, v)$, is not in K , then $\sigma_i = R|D$ belongs to this exceptional fraction. Remark 3.2 shows that in this situation, by betting on the places in D , a martingale can increase its capital by a factor of 2^i when betting against the unknown set R .

Now consider the following martingale, where we leave it to the reader to show that the martingale can be computed in polynomial time. The initial capital 1 is split into infinitely many parts c_1, c_2, \dots where $c_i = 1/2^i$ is exclusively used to place bets on the strings in the set D that corresponds to the index i , i.e., the strings that are in $g_0(x)$ for some x in J_i . By the preceding discussion, the martingale can increase the capital c_i to at least 1 for all $i > i_0$ such that α_i is not in K . But if this were the case for infinitely many values of i , the martingale would succeed on R , thus contradicting the assumption that R is p -random. \square

By Claim 1 for almost all i , the density of the set A on J_i is confined to the small interval K with center $1/2^{k+1}$. While constructing the martingale d that is meant to succeed on B , we will exploit that thus in particular for almost all i , this density differs from 0 and is less than

$$(4.7) \quad \rho = \frac{3}{2} \cdot \frac{1}{2^{k+1}}.$$

Recall from the introduction that one can view reductions as functionals and let Γ be the functional that corresponds to the $\text{btt}(k)$ -reduction given by (g, h) , hence for example A is equal to $\Gamma(B)$. For all $i \geq i_0$, let

$$H_i = \bigcup_{x \in J_i} \{z : z \text{ in } g(x) \text{ and } |z| \geq l_i\},$$

i.e., H_i is the set of all long queries made by strings in J_i . Then we can argue that only for a fraction of all partial characteristic functions σ with domain H_i the

set $\Gamma(\langle B, \sigma \rangle)$ has density less than ρ on J_i . Formally, for every $i > i_0$ and for every partial characteristic function σ with domain H_i , we let

$$\beta_i(\sigma) = \frac{|\Gamma(\langle B, \sigma \rangle) \cap J_i|}{|J_i|}$$

and, further,

$$\Theta_i = \{\sigma : \sigma \text{ partial characteristic function with domain } H_i \text{ and } \beta_i(\sigma) < \rho\}.$$

By Claim 1 for almost all i , the density α_i of the set $A = \Gamma(B)$ on J_i is less than ρ , hence the restriction of B to H_i must be contained in Θ_i by definition of Θ_i .

We will argue next that there is some $\delta < 1$ such that for almost all i , the set Θ_i comprises at most a δ -fraction of all partial characteristic functions with domain H_i . We will then exploit the latter fact in the construction of the martingale d by betting against the $(1 - \delta)$ -fraction of partial characteristic functions outside of Θ_i , which have already been ruled out as possible restriction of B to H_i .

For the moment, let τ_x be the Boolean function obtained from $h(x)$ by hard-wiring $B(z)$ into $h(x)$ for all short queries z in $g(x)$. By definition for all x , the queries in $g(x)$ are assigned to the variables of $h(x)$ in length-lexicographical order, hence for equivalent strings x and y , the Boolean functions τ_x and τ_y are identical. Thus for every $i > i_0$, all strings in J_i are mapped to the same Boolean function, which we denote by τ_i . We call a Boolean function constant iff it evaluates to the same truth value for all assignments to its arguments (and hence in particular all 0-place Boolean functions are constant).

CLAIM 2. *For almost all i , τ_i is not constant.*

Proof. If τ_i is constant, then the value $A(x)$ must be the same for all x in J_i . But then α_i is either 0 or 1, while Claim 1 implies that this is the case for at most finitely many i . \square

CLAIM 3. *There is a constant $\delta < 1$ such that for almost all i , the set Θ_i comprises at most a δ -fraction of all partial characteristic functions with domain H_i .*

Proof. For a given $i > i_0$ such that τ_i is not constant, consider the random experiment where we use independent tosses of a fair coin in order to choose the individual bits of a random partial characteristic function $\hat{\sigma}$ with domain H_i . Then all partial characteristic functions of this type occur with the same probability; hence the fraction we want to bound is just the probability of picking an element in Θ_i .

For every string x in J_i , define a 0-1-valued random variable b_x , and define a random variable γ_i with rational values in the closed interval $[0, 1]$ by

$$b_x(\hat{\sigma}) := \Gamma(\langle B, \hat{\sigma} \rangle, x), \quad \gamma_i(\hat{\sigma}) := \frac{1}{|J_i|} \sum_{x \in J_i} b_x(\hat{\sigma}).$$

Consider an arbitrary string x in J_i . By assumption, τ_i is not constant, hence there is at least one assignment to $\hat{\sigma}$ such that $b_x(\hat{\sigma})$ is 1. Moreover such an assignment occurs with probability at least $1/2^k$ because $h(x)$, and thus also τ_i , has at most k variables. Thus the expected value of b_x is at least $1/2^k$ and by linearity of expectation we obtain

$$(4.8) \quad \mathbf{E}(\gamma_i) = \frac{1}{|J_i|} \sum_{x \in J_i} \mathbf{E}(b_x) \geq \frac{1}{|J_i|} \sum_{x \in J_i} \frac{1}{2^k} = \frac{1}{2^k}.$$

If we let p be the probability of the event “ $\gamma_i < \rho$,” we have

$$(4.9) \quad \frac{1}{2^k} \leq \mathbf{E}(\gamma_i) \leq p \cdot \rho + (1-p) \cdot 1 \leq \rho + (1-p) = \frac{3}{4} \cdot \frac{1}{2^k} + (1-p),$$

where the relations follow, from left to right, by (4.8), by definition of p and by $\gamma_i \leq 1$, because the probability p is bounded by 1, and by the choice of ρ in (4.7). By comparing the first and last term in (4.9) we then obtain that p is bounded from above by $\delta := 1 - 1/2^{k+2}$. \square

For all i , let $I_i = \{x : l_i \leq |x| < l_{i+1}\}$. The values of n_i grow sufficiently fast such that for some i_1 and for all $i > i_1$, the set H_i is contained in I_i . Moreover, by Claim 3, for some $i_2 > i_0$ and all $i > i_2$, there is a set Θ_i of partial characteristic functions with domain H_i where Θ_i contains only a δ -fraction of all such partial characteristic functions and contains the restriction of B to H_i . Let i_3 be the maximum of i_1 and i_2 .

Now we are in a position to describe a betting strategy that succeeds on B . For a given input w , let x be the $(|w| + 1)$ th string, i.e., the string on which we might bet. We first compute the index i such that x is in I_i , together with the corresponding set H_i . In case $i \leq i_3$ or if x is not in H_i , we abstain from betting. Otherwise, we place a bet on x according to the betting strategy as described in Remark 3.2, which, while placing bets on the strings in H_i , increases the capital by a factor of at least $1/\delta$ by betting against the partial characteristic functions that are not in Θ_i . Here all necessary computations can be performed in time $2^{O(n_i)}$ and hence, by $|x| \geq l_i = \lfloor n_i/2k \rfloor$, in time $2^{O(|x|)}$. It follows that this betting strategy induces a martingale computable in polynomial time that on interval I_i preserves its capital in case $i \leq i_3$ and increases its capital by a factor of at least $1/\delta$ for all $i > i_3$.

This finishes the proof of Theorem 4.1. Observe that the current proof would for example also go through if we had chosen the cardinality m_i of J_i to be equal to n_i . The actual choice of the m_i emphasizes that for given k , the complexity of the martingale d covering the set B in the upper p -btt(k)-span of A is dominated by the complexity of computing the sets J_i , whereas the complexity of handling the assignments on the sets H_i can be neglected. \square

Remark 4.2. The assertion of Theorem 4.1 remains valid if we simply require the set R to be n -random instead of p -random, (i.e., if we require that there is no martingale computable in time $O(n)$ that succeeds on R). For a proof, note that Ambos-Spies, Terwijn, and Zheng [5] have shown that for every n^2 -random set R , there is a p -random set R_0 that is p - m -reducible to R while, in fact, the latter assertion is true for n -random R . Now the relaxed version of Theorem 4.1 follows because the existence of a separating set A as required in the theorem extends directly from R_0 to R .

Remark 4.3. Theorem 4.1 states that the lower p -btt($k + 1$)-span of every p -random set R contains a set A that is not in the lower p -btt(k)-span of any p -random set. As already noted by Book, Lutz, and Martin [8], for a set R that is not just p -random but is even Martin-Löf-random, such a set A cannot be recursive. This follows from the fact that every recursive sets that is p -btt($k + 1$)-reducible to a Martin-Löf-random set is in fact computable in polynomial time. The latter fact is attributed to folklore by Lutz and Schweizer [18] and can be obtained as a special case of a result of Book, Lutz, and Wagner [9]. They have shown from rather general assumptions on the reducibility under consideration that every recursive set that is reducible to a Martin-Löf-random set must be contained in the corresponding almost-class, i.e., in the class of sets that have an upper span of uniform measure 1. Their assumptions are satisfied for most bounded reducibilities considered in the literature

and, in particular, their result applies to $p\text{-btt}(k)$ -reducibility for all $k \geq 0$. Moreover, for the latter reducibilities it was shown by Ambos-Spies [2] that the corresponding almost-classes are all equal to the class of sets computable in polynomial time. As a consequence, any recursive set A in the lower $p\text{-btt}(k + 1)$ -span of a Martin-Löf-random set is computable in polynomial time and is hence in the lower $p\text{-btt}(k)$ -span of every Martin-Löf-random set.

From the proof of Theorem 4.1 we obtain the following corollary.

COROLLARY 4.4. *For every p -random set R , the lower p -tt-span of R is not contained in the lower p -btt span of $p\text{-RAND}$.*

Proof. For a given p -random set R and for every k , let the set A_{k+1} be defined in the same way as the set A has been defined in (4.1) in the proof of Theorem 4.1. Then A_{k+1} is $p\text{-btt}(k + 1)$ -reducible to R , but is not $p\text{-btt}(k)$ -reducible to any p -random set. Moreover, the set

$$B = \{x : x = 1^k 0y \text{ and } y \text{ in } A_k\}$$

is $p\text{-tt}$ -reducible to R by construction of the sets A_k . On the other hand, if B were $p\text{-btt}$ -reducible to some p -random set R_0 , then B would be in fact $p\text{-btt}(k)$ -reducible to R_0 for some k . Hence, in particular, A_{k+1} were $p\text{-btt}(k)$ -reducible to R_0 , thus contradicting the choice of A_{k+1} . \square

5. Separations by rec-random oracles. Lutz [14] showed that recursive martingales yield a reasonable measure concept for the class of recursive sets, where in particular the class of all recursive sets cannot be covered by a recursive martingale.¹ Recall from the introduction that a set is recursively random iff it cannot be covered by a recursive martingale and that rec-RAND denotes the class of all such sets. Next we state two results on recursively random sets that correspond rather closely to Theorem 4.1 and Corollary 4.4 on p -random sets.

THEOREM 5.1. *Let the set R be in rec-RAND and let k be a natural number. Then the lower $p\text{-}(k + 1)\text{-tt}$ -span of R is not contained in the lower $btt(k)$ -span of rec-RAND .*

COROLLARY 5.2. *For every set R in rec-RAND , the lower p -tt-span of R is not contained in the lower btt -span of rec-RAND .*

In connection with Theorem 5.1 and Corollary 5.2, recall that *btt-reducibility* is defined like $p\text{-btt}$ -reducibility, except that a btt -reduction is required to be computed by a total Turing machine that might run in arbitrary time and space and that *btt(k)-reducibility* is the restriction of btt -reducibility where the number of queries is bounded by k .

We omit the proofs of Theorem 5.1 and Corollary 5.2, which are almost literally the same as in the case of p -random sets. Besides the fact that now we consider effective martingales and reductions instead of polynomial time-bounded ones, the main difference is that for arbitrary recursive reductions from A to B we cannot compute an a priori bound on the size of the queries. Hence in order to ensure that the sets H_i are pairwise disjoint, the definition of the n_i will now depend on the given reduction (g, h) . Here we choose n_{i+1} so large that all strings queried on inputs of length n_i are short queries with respect to n_{i+1} , i.e., have length strictly less than $\lfloor n_{i+1}/2k \rfloor$.

Remark 5.3. Recall from the discussion preceding Remark 3.1 that the class of Martin-Löf-random sets is a proper subclass of rec-RAND . As a consequence,

¹For further discussion of measure concepts for the class of recursive sets see for example Schnorr [24], Terwijn [25], and Wang [27].

by an easy argument similar to the one used in Remark 1.1, from the separation by the class rec-RAND stated in Theorem 5.1 we obtain the main result of Book, Lutz, and Martin [8], who showed that for all k , the lower $\text{p-btt}(k+1)$ -span of a Martin-Löf-random set is never contained in the lower $\text{btt}(k)$ -span of the class of all Martin-Löf-random sets.

Acknowledgments. We are grateful to Elvira Mayordomo for several useful corrections and suggestions, where the latter include a significant simplification of the argument in Remark 4.2 via referring to the cited result of Ambos-Spies, Terwijn, and Zheng [5]. Furthermore, we would like to thank Klaus Ambos-Spies, Jack Lutz, and Jan Reimann for helpful discussions. Finally, we are grateful for the detailed comments of the anonymous referees of ICALP 2000 and of the *SIAM Journal on Computing*.

REFERENCES

- [1] E. ALLENDER AND M. STRAUSS, *Measure on small complexity classes, with applications for BPP*, in Proceedings of the 35th Annual IEEE Symposium on Foundations of Computer Science, IEEE Computer Society Press, Los Alamitos, CA, 1994, pp. 807–818.
- [2] K. AMBOS-SPIES, *Randomness, relativizations, and polynomial reducibilities*, in Proceedings First Structure in Complexity Theory Conference, Lecture Notes in Comput. Sci. 223, Springer-Verlag, 1986, pp. 23–34.
- [3] K. AMBOS-SPIES, E. MAYORDOMO, Y. WANG, AND X. ZHENG, *Resource-bounded balanced genericity, stochasticity and weak randomness*, in the 13th Annual Symposium on Theoretical Aspects of Computer Science, C. Puech and R. Reischuk, eds., Lecture Notes in Comput. Sci. 1046, Springer-Verlag, New York, 1996, pp. 63–74.
- [4] K. AMBOS-SPIES AND E. MAYORDOMO, *Resource-bounded measure and randomness*, in Complexity, Logic, and Recursion Theory, A. Sorbi, ed., Dekker, New York, 1997, pp. 1–47.
- [5] K. AMBOS-SPIES, S. A. TERWIJN, AND X. ZHENG, *Resource bounded randomness and weakly complete problems*, Theoret. Comput. Sci., 172 (1997), pp. 195–207.
- [6] C. H. BENNETT AND J. GILL, *Relative to a random oracle A , $P^A \neq NP^A \neq \text{co-}NP^A$ with probability 1*, SIAM J. Comput., 10 (1981), pp. 96–113.
- [7] J. L. BALCÁZAR, J. DÍAZ, AND J. GABARRÓ, *Structural Complexity*, Vol. I, Springer-Verlag, Berlin, 1995.
- [8] R. V. BOOK, J. H. LUTZ, AND D. M. MARTIN, JR., *The global power of additional queries to random oracles*, Informat. Comput., 120 (1995), pp. 49–54.
- [9] R. V. BOOK, J. H. LUTZ, AND K. W. WAGNER, *An observation on probability versus randomness with applications to complexity classes*, Math. Systems Theory, 27 (1994), pp. 201–209.
- [10] R. V. BOOK AND S. TANG, *Polynomial-time reducibilities and “almost all” oracle sets*, Theoret. Comput. Sci., 81 (1991), pp. 35–47.
- [11] D. W. JUEDES, J. I. LATHROP, AND J. H. LUTZ, *Computable depth and reducibility*, Theoret. Comput. Sci., 132 (1994), pp. 37–70.
- [12] R. E. LADNER, N. A. LYNCH, AND A. L. SELMAN, *A comparison of polynomial time reducibilities*, Theoret. Comput. Sci., 1 (1975), pp. 103–123.
- [13] M. LI AND P. VITÁNYI, *An Introduction to Kolmogorov Complexity and Its Applications*, 2nd ed., Springer-Verlag, New York, 1997.
- [14] J. H. LUTZ, *Almost everywhere high nonuniform complexity*, J. Comput. System Sci., 44 (1992), pp. 220–258.
- [15] J. H. LUTZ, *The quantitative structure of exponential time*, in Complexity Theory Retrospective II, L. A. Hemaspaandra and A. L. Selman, eds., Springer-Verlag, New York, 1997, pp. 225–260.
- [16] J. H. LUTZ AND E. MAYORDOMO, *Cook versus Karp-Levin: Separating completeness notions if NP is not small*, Theoret. Comput. Sci., 164 (1996), pp. 141–163.
- [17] J. H. LUTZ AND E. MAYORDOMO, *Twelve problems in resource-bounded measure*, Bull. Euro. Assoc. Theoret. Comput. Sci., 68 (1999), pp. 64–80.
- [18] J. H. LUTZ AND D. L. SCHWEIZER, *Feasible reductions to Kolmogorov–Loveland stochastic sequences*, Theoret. Comput. Sci., 225 (1999), pp. 185–194.
- [19] P. MARTIN-LÖF, *The definition of random sequences*, Informat. Control, 9 (1966), pp. 602–619.

- [20] E. MAYORDOMO, *Contributions to the Study of Resource-Bounded Measure*, Doctoral dissertation, Universitat Politècnica de Catalunya, Barcelona, Spain, 1994.
- [21] W. MERKLE AND Y. WANG, *Random separations and “almost” classes for generalized reducibilities*, *Math. Logic Quart.*, 47 (2001), pp. 249–269.
- [22] C. H. PAPADIMITRIOU, *Computational Complexity*, Addison-Wesley, Reading, MA, 1994.
- [23] C.-P. SCHNORR, *A unified approach to the definition of random sequences*, *Math. Systems Theory*, 5 (1971), pp. 246–258.
- [24] C.-P. SCHNORR, *Zufälligkeit und Wahrscheinlichkeit*, *Lecture Notes in Math.* 218, Springer-Verlag, Berlin, 1971.
- [25] S. A. TERWIJN, *Computability and Measure*, Doctoral dissertation, Universiteit van Amsterdam, Amsterdam, Netherlands, 1998.
- [26] J. VILLE, *Étude Critique de la Notion de Collectif*, Gauthiers-Villars, Paris, 1939.
- [27] Y. WANG, *Randomness and Complexity*, Doctoral dissertation, Universität Heidelberg, Mathematische Fakultät, INF 288, Heidelberg, Germany, 1996.