Electronic Colloquium on Computational Complexity, Report No. 34 (1999)

ECCC

The global power of additional queries to p-random oracles

Wolfgang Merkle

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

Abstract. We consider separations of reducibilities in the context of resource-bounded measure theory. First, we show a result on polynomial-time bounded reducibilities: for every p-random set R, there is a set which is reducible to R with $k+1$ non-adaptive queries, but is not reducible to any other p-random set with at most k non-adaptive queries. This result solves an open problem stated in a recent survey paper by Lutz and Mayordomo [15]. 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 yields as a special case the main result of Book, Lutz, and Martin [7], who, by using different methods, showed a similar separation w.r.t. Martin-Löf-random sets. Moreover, in both settings we obtain a separation as above of truth-table versus bounded truth-table reducibility.

1 Introduction and related work

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 Sect. 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 w.r.t. 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 relations on Cantor space) if and only if they are separated by some oracle. Beyond this simple observation, the question which reducibilities are separated by what kind of oracles has been the object of intensive studies. Here, for a given pair of reducibilities, typical question are the following. Are there separating oracles of low complexity? How comprising is the class of separating oracles? What are sufficient properties for being a separating oracle?

Ladner, Lynch, and Selman [10] considered separations of the usual polynomial-time bounded reducibilities in the range between many-one and Turing reducibility. They showed that for every distinct pair of such reducibilities, there is a separating oracle which can be computed in exponential time. Subsequently, in their seminal paper [5], Bennett and Gill obtained results about separations

ISSN 1433-8092

by almost all or by random oracles, i.e., they showed that for certain pairs of reducibilities the class of separating oracles has measure 1 w.r.t. uniform measure on Cantor space. In fact, for every $k > 0$, every pair of distinct reducibilities chosen among p-T-, p-tt, p-btt, p-btt$(k+1)$, and p-btt(k)-reducibility can be separated by random oracles, see [14] and [17], as well as [9] for a separation of p-btt$(k+1)$- and p-btt(k)-reducibility by almost all tally oracles.

A separation by random oracles can be expressed equivalently by saying that the class of oracles which do not separate the reducibilities under consideration has uniform measure 0. Lutz and Mayordomo [14] could show for certain pairs of polynomial-time bounded reducibilities of truth-table type that the class of separating oracles does not just have uniform measure 0 but is in fact covered by a polynomial-time computable martingale. 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 polynomial-time computable martingale which covers all oracles which do not separate p-btt$(k+1)$- and p-btt(k)-reducibility, whence, 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 a nonempty class $\mathbf{C}$ locally separates two given reducibilities iff for every set A in $\mathbf{C}$, the lower spans of A w.r.t. these reducibilities are different, whereas $\mathbf{C}$ globally separates the reducibilities in case for every set A in $\mathbf{C}$ there is a set B which is reducible to A w.r.t. one of the reducibilities but B is not reducible to any set in $\mathbf{C}$ w.r.t. 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. In distinguishing local and global separations we follow Book, Lutz, and Martin [7], who discuss such separations for the classes of Martin-Löf-random, tally, and sparse sets.

Remark 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 which 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.

In Theorem 4, we extend Lutz and Mayordomo's local separation of p-btt$(k+1)$- and p-btt(k)-reducibility to a global separation. This, together with Remark 6, solves Problem 7 in the recent survey article [15], 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 Sect. 6, then we obtain by basically the same proof as for Theorem 4, that for every natural number k, the class of rec-random sets globally separates p-btt$(k+1)$-reducibility from btt(k)-reducibility, i.e., from the reducibility restricted to at most k non-adaptive queries where the reductions have to be effective but might run in arbitrary time and space. By Remark 1, this yields as a special case the main result of Book,

Lutz, and Martin [7], who showed, by using different methods, a corresponding global separation w.r.t. 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 [4], [6], and [13]. All strings are over the alphabet $\Sigma = \{0,1\}$. We identify strings with natural numbers via the isomorphism which takes the length-lexicographical ordering on $\{\lambda, 0, 1, 00, \ldots\}$ 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 some set I is denoted by $\beta|I$, whence in particular for a 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 $\{0, \ldots, n-1\}$, whence in particular strings can be viewed as prefixes of sets. For a partial characteristic function α with domain $\{z_0 < \ldots < z_{n-1}\}$, the string associated with α is the (unique) string β where $\beta(j) = \alpha(z_j)$ for $j = 0, \ldots, n-1$. For a set X and a partial characteristic function σ we write $\langle X, \sigma \rangle$ for the set which agrees with σ for all arguments in the domain of σ and which agrees with X, otherwise.

We will consider the following variants of polynomial-time bounded reducibility: Turing reducibility (p-T), truth-table reducibility (p-tt), where the queries have to be asked non-adaptively, bounded truth-table reducibility (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 some natural number k. The relation symbol $\leq^{\mathrm{p}}_{\mathrm{btt}}$ refers to p-btt-reducibility, and relation symbols for other reducibilities are defined in a similar fashion. Expressions such as p-T-reduction and $\leq^{\mathrm{p}}_{\mathrm{T}}$-reduction will be used interchangeably. We will represent p-btt-reductions by a pair of polynomial time computable functions g and h 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 which specifies how the answers to the queries in the set $g(x)$ are evaluated. Here we assume, firstly, via introducing dummy variables, that the cardinality of $g(x)$ is always exactly k and, secondly, by convention, that in order to assign the queries in $g(x)$ to the arguments of the Boolean function $h(x)$, the queries are ordered by the length-lexicographical ordering.

3 Resource-Bounded Measure

We give a brief introduction to resource-bounded measure which focusses 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 [13].

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, bets on A, for short. The betting proceeds in rounds $i = 1, 2, \ldots$ where during round i, the player receives the length $i-1$ prefix of A and then, firstly, decides whether to bet on the ith bit being 0 or 1 and, secondly, determines the stake by specifying the fraction of the current capital which shall be bet. Formally, a player can be identified with a betting strategy $b : \{0,1\}^* \to [-1,1]$ 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

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

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

$$d(w) \ = \ \frac{d(w0) + d(w1)}{2} \ , \tag{1}$$

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 (1) for all strings w.

By the preceding discussion it follows for gambles as described above that the possible payoff functions are exactly the martingales and that in fact there is a one-to-one correspondence between martingales and betting strategies. 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.

Fix a martingale d. We say d succeeds on a set A if d is unbounded on the prefixes of A, i.e., if $\limsup_{n \text{ in } \omega} d(A|\{0,\ldots,n\}) = \infty$. The success set $S^\infty[d]$ of the martingale d is the class of sets on which d succeeds. We say d succeeds on or covers a class iff this class is contained in $S^\infty[d]$.

Every countable class $\boldsymbol{C} = \{C_1, C_2, \ldots\}$ 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 (and abstain from betting if such an index does not exist), then bet half of the current capital on the next bit agreeing with the corresponding bit of C_i. As a consequence, most of the classes considered in complexity and recursion theory can be covered by martingales, whence 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 $\boldsymbol{C}$ one is interested in finding a class of martingales which allows the covering of large subclasses of $\boldsymbol{C}$, but not of $\boldsymbol{C}$ itself. In the context of recursion theory, this led to the consideration of recursive martingales, see [19], [20], whereas in connection with complexity classes one has to impose additional resource-bounds, see [11], [13], [1]. Here an effective martingale d is always confined to rational values and it is assumed that there is a Turing machine which on input w outputs an appropriate finite representation of $d(w)$.

Recall the definition of the uniform (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, see [22] and [4]. The latter result justifies the following notation: a class has measure 0 w.r.t. a given class of martingales iff it is covered by some martingale in the class. The aim stated above can then be rephrased: for given $\boldsymbol{C}$, we want to specify a class of admissible martingales such that large subclasses of $\boldsymbol{C}$ have measure 0, but not $\boldsymbol{C}$ itself.

In connection with measure on complexity classes, most attention has been received by measure concepts for the exponentially time-bounded classes $\mathbf{E} = \mathbf{DTIME}(2^{\mathrm{lin}})$ and $\mathbf{EXP} = \mathbf{DTIME}(2^{\mathrm{poly}})$. For example, in the case of the class $\mathbf{E}$, Lutz proposed to use martingales which 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 $2^{\mathcal{O}(|x|)}$ 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 $\mathbf{DTIME}(2^{c \cdot n})$ 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, there is a one-to-one correspondence between polynomial-time computable martingales and betting strategies (however, in general, the polynomial bounding the running time might not be preserved in the transition from a betting strategy to the corresponding martingale, see [3]). Furthermore, there is a similar correspondence between martingales and betting strategies in the case of martingales used to define measure on $\mathbf{EXP}$ and in the case of recursive martingales, see [3] and [20], respectively.

Intuitively speaking, a martingale can only succeed on a set which has certain regularities known to the martingale and, conversely, if none of the martingales in a given class succeeds on a set R then, relative to the martingales under consideration, the set R is essentially irregular or random. Formally, we call a set random w.r.t. a given class of martingales iff none of these martingales succeeds on this set. Now, the success set of a single martingale always has uniform measure 0, and by σ-additivity, the same holds for every countable union of success sets. Thus for every countable class of martingales, the corresponding class of random sets has uniform measure 1. In this situation, random sets can also be viewed as typical sets.

We say a set is p-random if the set cannot be covered by a polynomial-time computable martingale, and we write p-RAND for the class of all 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 polynomial-time computable ones. Moreover, we will consider Martin-Löf-random sets, which have been introduced in [16] and have been characterized equivalently in terms of martingales in [20]: a set is Martin-Löf-random if and only if it cannot be covered by a subcomputable martingale. Here a martingale d is subcomputable iff there is a recursive function g in two arguments such that for all strings w, the sequence $g(w,0), g(w,1), \ldots$ is nondecreasing and converges to $d(w)$. Schnorr [20] has implicitly shown that the class of Martin-Löf-random sets is a proper subclass of rec-RAND.

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

Remark 2. Let a finite set D be given, as well as a list $\langle D_1, \ldots, D_m \rangle$ of pairwise disjoint subsets of D which 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

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

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 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 $1/2^k$. It is suggestive to assume that for large m, only for a small fraction of all partial characteristic functions with domain D the frequency of w will deviate significantly from the expected value. Using Chernoff bounds (see for example Lemma 11.9 in [18]), one can indeed 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 $D_1, \ldots, D_m$ as above we have

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

Remark 3. 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 which 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 Separating p-btt($k+1$)- and p-btt(k)-reducibility

In connection with Theorem 4, recall that given a reducibility $\leq$, the lower $\leq$-span of a set A is the class $\{X : X \leq A\}$ of sets which are $\leq$-reducible to A, and the lower $\leq$-span of a class $\boldsymbol{C}$ is the class of all sets which are $\leq$-reducible to some set in $\boldsymbol{C}$.

Theorem 4. *Let R be a p-random set and let k be a natural number. Then the lower p-btt$(k+1)$-span of R is not contained in the lower p-btt(k)-span of* p-RAND.

Proof. In order to define a set A and a p-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

$$g_0(x) \;:=\; \{x0^1 1^{k+1}, x0^2 1^k, \ldots, x0^{k+1}1^1\} \;, \qquad A \;:=\; \{x : g_0(x) \subseteq R\} \;.$$

We are done if we can show that if A is p-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-btt(k)-reduction (g, h). We will construct a polynomial-time computable martingale d which succeeds on B. To this end, we define a sequence $n_0, n_1, \ldots$ with

$$n_0 = 0 \;, \qquad n_{i+1} > 2^{n_i} \;, \qquad \log n_{i+1} > m(k+1, \frac{1}{2^{i+1}}) \tag{3}$$

(here $m(.,.)$ is the function defined in Remark 2) and such that given x of length n, we can compute in time $\mathcal{O}(n^2)$ the maximal i with $n_i \leq n$. Such a sequence can be obtained by standard methods. For example we can first define a sufficiently fast growing time-constructible function $r : \omega \to \omega$ and then let n_i be the i-fold iteration of r applied to 0 (for details, refer to the chapter on uniform diagonalization and gap languages in [6]).

It is helpful to view the betting strategy of the martingale d as being performed in stages $i = 0, 1, \ldots$ 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 which have length strictly less than

$$l_i \quad := \quad \left\lfloor \frac{n_i}{2k} \right\rfloor \tag{4}$$

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

$$(i)\ h(x) = h(y)\ , \qquad (ii)\ \{z \text{ in } g(x) : |z| < l_i\} = \{z \text{ in } g(y) : |z| < l_i\}\ , \quad (5)$$

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 and for all sufficiently large i, the number of equivalence classes of strings of length n_i is bounded by

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

As a consequence, there is some i_o such that for all $i \geq i_0$, 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

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

(In fact 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. Our actual choice of the m_i has the advantage that most of the current proof can be reused in the proof of Theorem 7.) We show now that due to A being p-random, almost all α_i are close to $1/2^{k+1}$.

Claim 1. For almost all i,

$$\frac{1}{2} \cdot \frac{1}{2^{k+1}} \quad < \quad \alpha_i \quad < \quad \frac{3}{2} \cdot \frac{1}{2^{k+1}}\ . \qquad (6)$$

Proof. Fix an index i and assume that (6) is false. Let $z_1 < \ldots < z_{m_i}$ be the elements of J_i, let $D_j = g_0(z_j)$ for $j = \{1, \ldots, m_i\}$, and let D be the union of D_1 through D_{m_i}. If we let $w = 1^{k+1}$, then by definition of g_0 we have $\alpha_i = \alpha(R|D, w)$, whence (6) remains false with α_i replaced by $\alpha(R|D, w)$. On the other hand, (6) is false with α_i replaced by $\alpha(\sigma, w)$ for at most a $1/2^i$-fraction of all partial characteristic functions σ with domain D because by (3) and the choice of the m_i, we have $m_i \geq m(k+1, 1/2^i)$. Remark 3 then shows that while betting on R, a martingale can increase its capital by a factor of 2^i by betting for all places in D on the $1/2^i$-fraction of partial characteristic functions for which (6) is false.

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 $c_1, c_2, \ldots$ where $c_i = 1/2^i$ is exclusively used to place bets on the strings in the set D which corresponds to the index i, i.e., the strings which 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 such that (6) is false. 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. □

By Claim 1, the set A has comparatively low density on J_i. We will show now that this fact gives us enough information on the set B to construct a polynomial-time computable martingal which succeeds on B. Let Γ be the functional which corresponds to the btt(k)-reduction given by (g, h) (whence for example A is equal to $\Gamma(B)$) and for all $i \geq i_0$, let

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

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 such low density on J_i. Formally, for every $i > i_0$ and for every partial characteristic function σ with domain H_i, we let

$$\beta_i(\sigma) \ = \ \frac{|\Gamma(\langle B, \sigma \rangle) \cap J_i|}{|J_i|} \ , \qquad \rho \ = \ \frac{3}{2} \cdot \frac{1}{2^{k+1}} \ ,$$

and, further,

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

Then by Claim 1 for almost all i, the restriction of B to H_i must be contained in Θ_i. Moreover, we will argue 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 martingal 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 as follows: compute $h(x)$ and for every short query z in $g(x)$ hard-wire $B(z)$ into τ_x. Then for equivalent strings x and y, the Boolean functions τ_x and τ_y are identical. As a consequence, for every i, 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, whence in particular all 0-placed 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, whence Claim 1 implies that this is the case for at most finitely many indices i. □

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 given i 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 $\widehat{\sigma}$ with domain H_i. Then all

partial characteristic functions of the latter type occur with the same probability, whence 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, moreover, define a random variable γ_i with rational values in the closed interval $[0,1]$ by

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

Consider an arbitrary string x in J_i. By assumption, τ_i is not constant, whence there is at least one choice of σ such that b_x is 1. Moreover such a σ 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

$$E(\gamma_i) \quad = \quad \frac{1}{|J_i|} \sum_{x \text{ in } J_i} E(b_x) \quad \geq \quad \frac{1}{|J_i|} \sum_{x \text{ in } J_i} \frac{1}{2^k} \quad = \quad \frac{1}{2^k} \ . \qquad (7)$$

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

$$\frac{1}{2^k} \leq E(\gamma_i) \leq p \cdot \rho + (1-p) \cdot 1 \leq \rho + (1-p) = \frac{3}{4} \cdot \frac{1}{2^k} + (1-p) \ , \qquad (8)$$

where the relations follow, from left to right, by (7), by definition of p and by $\gamma_i \leq 1$, because the probability p is bounded by 1, and by definition of ρ. But (8) is obviously false in case $(1-p)$ is strictly less than $1/2^{k+2}$, whence p can be bounded from above by $\delta := 1 - 1/2^{k+2}$. □

For all i, let $I_i = \{x : l_i \leq |x| < l_{i+1}\}$. The 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 and all $i > i_2$, there is a set Θ_i of partial characteristic functions with domain H_i where, firstly, Θ_i contains only a δ-fraction of all such partial characteristic functions, and, secondly, Θ_i 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 which succeeds on B. On 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 and 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 a betting strategy as described in Remark 3, 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 which are not in Θ_i. Here all necessary computations can be performed in time $2^{\mathcal{O}(n_i)}$ and hence, by $|x| \geq l_i = \lfloor n_i/8 \rfloor$, in time $2^{\mathcal{O}(|x|)}$. It follows that this betting strategy induces a polynomial-time computable martingale which 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. □

Remark 5. The proof of Theorem 4 shows in fact that the theorem is valid for some small constant c and all n^c-random sets R, i.e., for all sets R which cannot be covered by a martingale which is computable in time $\mathcal{O}(n^c)$. Indeed, the theorem is even valid for n-random R. This can be shown by essential the same proof where, however, during stage i, we will not consider the queries made for all strings of length n_i, but just the queries for the first $2^{n_i}/3$ strings of this length, while adapting appropriately the values of the n_i and the l_i.

Remark 6. Theorem 4 states that the lower p-btt$(k+1)$-span of every p-random set R contains a set A which is not in the lower p-btt(k)-span of any p-random set. As already noted in [7], for a set R which is not just p-random but is even Martin-Löf-random, such a set A cannot be recursive. This follows from a result by Book, Lutz, and Wagner [8]. They have shown for a quite comprising class of bounded reducibilities that every recursive set which is reducible to a Martin-Löf-random set must be contained in the corresponding Almost-class, i.e. in the class of sets which have an upper span of uniform measure 1. Now, firstly, their result applies to p-btt(k)-reducibility for all $k \geq 0$ and, secondly, for these reducibilities it has been shown in [2] that the corresponding Almost classes are all equal to the class of sets computable in polynomial time. As a consequence, every recursive set A in the lower p-btt$(k+1)$-span of a Martin-Löf-random set is computable in polynomial time and is hence in the lower p-btt(k)-span of every Martin-Löf-random set.

5 Separating p-tt- and p-btt-reducibility

The proof of Theorem 4 can be adjusted such that it yields a global separation of the polynomial-time bounded versions of truth-table and bounded truth-table reducibility.

Theorem 7. *For every p-random set R, the lower p-tt-span of R is not contained in the lower p-btt span of* p-RAND.

Proof. The proof of Theorem 7 is rather similar to the proof of Theorem 4. Here the main difference is that now, while reducing A to R, we will use an increasing number of queries. In the definition of the sequence $n_0, n_1, \ldots$ we replace (3) by

$$n_0 = 0 \ , \qquad n_{i+1} > 2^{n_i} \ , \qquad \log n_{i+1} > m(i+1, \frac{1}{2^{i+1}}) \ , \tag{9}$$

i.e, the first argument of the function m is changed from the constant $k+1$ to i. This relates to the fact that now the set A is defined by

$$A \quad := \quad \bigcup_{i \text{ in } \omega} \{x : |x| = n_i \text{ and } \{x0^1 1^i, x0^2 1^{i-1}, \ldots, x0^i 1^1\} \subseteq R\} \ ,$$

i.e., the canonical p-tt-reduction from A to R will ask i queries for arguments of length n_i. The set A is indeed reducible to B in polynomial time because the

n_i have been chosen such that given a string x of length n, in polynomial time, firstly, we can compute the largest index i with $n_i \leq |x|$ and, secondly, we can check whether n is in fact equal to some n_i by comparing the corresponding indices for x and 0^{n-1}.

Now let S be an arbitrary set and assume that A is reducible to S via the p-btt-reduction (g, h), where this reduction is in fact a p-btt(k)-reduction for some k. Then if we define the J_i and the α_i in the same way as in the proof of Theorem 4, we can show again that for almost all i, the α_i are close to their expected value, i.e., for almost all i, we have

$$\frac{1}{2} \cdot \frac{1}{2^i} \quad < \quad \alpha_i \quad < \quad \frac{3}{2} \cdot \frac{1}{2^i} \ , \tag{10}$$

In the proof we exploit that by the choice of the n_i, now we have $m_i > m(i, 1/2^i)$, and not just $m_i > m(k, 1/2^i)$. In the argument we construct a martingal which again considers all partial characteristic functions domain equal to H_i, where the sets H_i are defined like in the proof of Theorem 4. Now we cannot bound the cardinality of the sets H_i by $k \cdot m_i$, as before, but just by $i \cdot m_i$. However, the latter bound is still less than n_i for almost all i, whence the constructed martingal is again computable in polynomial time. The remainder of the proof is almost literally the same as for Theorem 4 and is left to the reader. □

6 Separations by rec-random oracles

Lutz [11] 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 (see [21] for a comparison of measure concepts for the class of recursive sets). Next we state two results on rec-random sets which correspond rather closely to Theorems 4 and 7 on p-random sets.

In connection with Theorems 8 and 9, recall from the introduction that rec-RAND is the class of sets which cannot be covered by a recursive martingale. Moreover, let btt-reducibility be defined like p-btt-reducibility, except that a btt-reduction can run in arbitrary time and space, and let btt(k)-reducibility be the restriction of btt-reducibility where the number of queries is bounded by k.

Theorem 8. *Let the set R be in* rec-RAND *and let k be a natural number. Then the lower* p-$(k+1)$-tt*-span of R is not contained in the lower btt(k)-span of* rec-RAND*.*

Theorem 9. *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*.*

We omit the proofs of Theorems 8 and 9, which are basically 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 recursive reductions from A to B we cannot compute an apriori bound

on the size of the queries, whence we cannot choose the n_i such that the sets H_i are disjoint from some index i on. However, as a set H_i will never contain short strings, i.e., strings of length less than l_i, each string x will be contained in at most finitely many of the sets H_i. Furthermore, each of the local betting strategies related to the various sets H_i uses its own share of the initial capital, whence we can apply a recursive betting strategy which at each string x bets according to the sum of the finitely many local betting strategies which are relevant for x.

Remark 10. Recall from Remark 1, that a global separation by a class $\boldsymbol{C}$ extends to all nonempty subclasses of $\boldsymbol{C}$. As a consequence, the global separation by the class rec-RAND stated in Theorem 8 yields as a corollary the main result of Book, Lutz, and Martin in [7], who used different methods to show that for all k, the class of Martin-Löf-random sets globally separates p-btt$(k+1)$- and btt(k)-reducibility.

7 Acknowledgements

We would like to thank Klaus Ambos-Spies and Jan Reimann for helpful discussion on resource-bounded measure.

References

1. E. Allender and M. Strauss. Measure on small complexity classes, with applications for BPP. In: *Proceedings of the 35th Annual IEEE Symposium an Foundations of Computer Science*, pages 807–818, IEEE Computer Society Press, 1994.
2. K. 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.
3. K. Ambos-Spies, E. Mayordomo, Y. Wang, X. Zheng. Resource-bounded balanced genericity, stochasticity and weak randomness. In C. Puech, R. Reischuk (Eds.), 13th Annual Symposium on Theoretical Aspects of Computer Science 1996, Lecture Notes in Computer Science 1046, pages 63–74, Springer-Verlag, 1996.
4. K. Ambos-Spies and E. Mayordomo. Resource-bounded measure and randomness. In: A. Sorbi, editor, *Complexity, logic, and recursion theory*, p.1-47. Dekker, New York, 1997.
5. Ch. H. Bennett and J. 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.
6. J. L. Balcázar, J. Díaz, and J. Gabarró. *Structural Complexity*, volume I and II. Springer-Verlag, 1995 and 1990.
7. 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.
8. R. V. Book, J. H. Lutz, and K. W. Wagner. An observation on probability versus randomness with applications to complexity classes. *Mathematical Systems Theory* 27:201–209, 1994, .

9. R. V. Book and S. Tang. Polynomial-time reducibilities and "almost all" oracle sets. *Theoretical Computer Science* 81:35–47, 1991.
10. R. E. Ladner, N. A. Lynch, and A. L. Selman. A comparison of polynomial time reducibilities. *Theoretical Computer Science* 1:103–123, 1975.
11. J. H. Lutz. Almost everywhere high nonuniform complexity. *Journal of Computer and System Sciences*, 44:220–258, 1992.
12. J. H. Lutz. Weakly hard problems. *SIAM Journal on Computing* 24:1170–1189, 1995.
13. J. H. Lutz. The quantitative structure of exponential time. In: Hemaspaandra, Lane A. et al., editors, *Complexity theory retrospective* II, pages 225–260, Springer-Verlag, 1997.
14. 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.
15. J. H. Lutz, E. Mayordomo. Twelve problems in resource-bounded measure. *EATCS Bulletin* 68:64–80, 1999.
16. P. Martin-Löf. The definition of random sequences. *Information and Control* 9:602–619, 1966.
17. W. Merkle and Y. Wang. Random separations and "Almost" classes for generalized reducibilities. In J. Wiedermann and P. Hájek, editors, *Mathematical Foundations of Computer Science*, Lecture Notes in Computer Science 969, pages 179–190. Springer-Verlag, 1995. Submitted for further publication.
18. C. H. Papadimitriou. *Computational Complexity.* Addison-Wesley Publishing Company, 1994.
19. C. P. Schnorr. A unified approach to the definition of random sequences. *Mathematical Systems Theory*, 5:246–258, 1971 .
20. C. P. Schnorr. *Zufälligkeit und Wahrscheinlichkeit.* Lecture Notes in Mathematics 218, Springer-Verlag, 1971.
21. S. A. Terwijn. *Computability and Measure.* Doctoral dissertation, Universiteit van Amsterdam, Amsterdam, Netherlands, 1998.
22. J. Ville. *Étude Critique de la Notion de Collectif.* Gauthiers-Villars, 1939.

ECCC ISSN 1433-8092
http://www.eccc.uni-trier.de/eccc
ftp://ftp.eccc.uni-trier.de/pub/eccc
ftpmail@ftp.eccc.uni-trier.de, subject 'help eccc'