Electronic Colloquium on Computational Complexity, Report No. 65 (2002)

Measure on P Revisited

Olivier Powell *

Abstract

We revisit the problem of generalising Lutz's resource bounded measure ($\mathcal{RBM}$) to small complexity classes. We propose a definition of a *perfect* $\mathcal{RBM}$ on P, and give sufficient and necessary conditions for such a measure to exist. We also revisit μ_τ, an $\mathcal{RBM}$ for P defined in [Str97], and correct an erroneous claim concerning the relations between μ_τ and random sets. The interest of generalising Lutz's $\mathcal{RBM}$ to small complexity classes, such as P, is that the theory of $\mathcal{RBM}$ has proven itself a useful tool in understanding the structure of big complexity classes such as E or EXP, and that small complexity classes are perhaps those of higher interest. Generalising $\mathcal{RBM}$ to small complexity classes has been studied in [May94b] for PSPACE, and in [AS94], [AS95] and [Str97] for P. We merely revisit the measure on P defined in [Str97], and besides correcting an erroneous claim concerning the relations between this $\mathcal{RBM}$ and random sets, construct a *better* $\mathcal{RBM}$, which we argue as being a *perfect* generalisation of Lutz's $\mathcal{RBM}$ to P, but which we can only prove to exist under the hypothesis of the *existence of random sets.*

1 Introduction

Resource bounded measure ($\mathcal{RBM}$) was introduced by Lutz in [Lut92]. Roughly speaking, $\mathcal{RBM}$ introduces a notion of big and small sets in complexity classes. It has since been used successfully to illuminate the structure of complexity classes, notably E and EXP. The theory of $\mathcal{RBM}$ is a parametrised tool, which permits to obtain an $\mathcal{RBM}$ for many complexity classes: one just adapts the parameters in order to obtain an $\mathcal{RBM}$ at the desired scale. One of the major limitations of $\mathcal{RBM}$ is that, for technical reasons, there seem to be no obvious ways of generalising it to so-called small complexity classes, such as P, or even PSPACE, which do not (or are not known to) contain E. Various attempts to remedy this flaw can be found in the literature, all of which make some compromise with what would be an intuitively perfect generalisation of Lutz's $\mathcal{RBM}$ to small complexity classes. In [May94b], an $\mathcal{RBM}$ is defined on PSPACE, using a concept of *on line* Turing machines. This definition yields a notion of $\mathcal{RBM}$ in PSPACE, which is interesting but sadly fails to extend to P. Further attempts to construct $\mathcal{RBM}$s for P can be found in the series of papers [AS94], [AS95] and [Str97]. These constructions give rise to consistent notions of measure for P, and also extend upwards to PSPACE. They are interesting from the theoretical point of view, and also permit certain results concerning the structure of small complexity classes: in [AS94] it is shown that almost every set in SUBEXP is hard for BPP, and that this cannot be improved without showing that BPP is a proper subset of E. In [CSS97], it is shown that the Lutz hypothesis, stating that NP has a non-null measure in E, and under which many conditional results are obtained (c.f. [May94a], [AS94], [LM94], [JL95a], [LM96], [Lut96] or, for a survey of the previous results, [Lut97a]), does not hold when translated to P. Nevertheless, these constructions all make compromises with the ideal generalisation of Lutz's $\mathcal{RBM}$ to small complexity classes, which consists of extending Lutz's $\mathcal{RBM}$ to small complexity classes by modifying only the parameters (which for example, permit to obtain an $\mathcal{RBM}$ on E or EXP). It is interesting to note that such an *ideal generalisation* of Lutz's $\mathcal{RBM}$ to small complexity classes is not proven to be impossible: it just happens that when plugging into the theory the parameters that would give an $\mathcal{RBM}$ for P (or PSPACE), the proofs of the consistency of the mathematical object thus defined cannot be obtained through simple downwards translation of the proofs in "big" complexity classes. Therefore the compromises conceded in order to obtain $\mathcal{RBM}$s in small complexity classes are unsatisfactory from a theoretical point of view, since it

* Université de Genève, Centre Universitaire d'Informatique, rue du Général Dufour 24, CH-1211 Genève 4, Switzerland, olivier.powell@cui.unige.ch

ISSN 1433-8092

is unknown whether simply extending Lutz's $\mathcal{RBM}$ to small complexity classes by adapting the parameters is impossible. Also, from a more practical point of view, these flaws are an obstacle to downward translation of results obtained in big complexity classes. For example, some results on almost and weak completeness, such as those from [Lut95], [ASMZ96], [ASTZ97], [AS00], [Jue95], [JL95b],[ASMRT00], could perhaps be adapted to small complexity classes if the ideal generalisation of Lutz's $\mathcal{RBM}$ were indeed a consistent $\mathcal{RBM}$, but it seems much more difficult to adapt these results with only a weaker notion of measure for small complexity classes. Our contribution to the mending of these flaws in the theory of $\mathcal{RBM}$ on small complexity classes is to define what a *perfect* generalisation on P of Lutz's $\mathcal{RBM}$ is and, most importantly, to give two sufficient conditions for such a measure to exist, one of theme, namely the *existence of random sets*, being also a necessary condition.

2 Preliminaries

The goal of this section is to define the concepts of a measuring system ($\mathcal{MS}$) and a resource bounded measure ($\mathcal{RBM}$). These concepts are used to obtain the results of this article. Although not as general as $\mathcal{RBM}$s, $\mathcal{MS}$s have the advantage of allowing the definition of what a *perfect* generalisation of Lutz's $\mathcal{RBM}$ should be. Intuitively, $\mathcal{RBM}$s and $\mathcal{MS}$s are the following: an $\mathcal{RBM}$ on a fixed class of languages $\mathcal{C}$ separates the subsets of $\mathcal{C}$ into small sets: those of null measure, and large sets: those of measure one. An $\mathcal{MS}$ is a structure that induces an $\mathcal{RBM}$, whereas the converse is not true. Thus there are "more" $\mathcal{RBM}$s than $\mathcal{MS}$s. Exact definitions follow.

Definition 2.1. *Let $\mathcal{C} \subseteq \{0,1\}^\infty$. An $\mathcal{RBM}$ on $\mathcal{C}$ is a partial function $\mu : \mathcal{P}(\mathcal{C}) \dashrightarrow \{0,1\}$, where $\mathcal{P}(\mathcal{C})$ is the power set of $\mathcal{C}$, and such that* [1]

M1 Points are of null measure: $\forall L \in \mathcal{C}\ \mu(L) = 0$
M2 The whole space is of measure one: $\mu(\mathcal{C}) = 1$
M3 A "suitable" union of null measure sets is a null measure set too.
M4 $A \subseteq B$ *and* $\mu(B) = 0 \Rightarrow \mu(A) = 0$
M5 $\mu(A) = 0$ *iff* $\mu(\overline{A}^{\mathcal{C}}) = 1$, *where* $\overline{A}^{\mathcal{C}} = \mathcal{C} \setminus A$

One could argue that any reasonable definition of an $\mathcal{RBM}$ should imply that some intuitively small sets such as sparse languages, or "slices", [2] are of null measure. However this is intentionally not included in the general definition of an $\mathcal{RBM}$. The intuition behind this choice is the following: it is noticeable that different attempts to define $\mathcal{RBM}$s in P or PSPACE have produced different notions of small sets. Typically, sentences of the following form can be found in the literature: "[...]our notion of $\mathcal{RBM}$ captures such intuitively small sets, which could not be done with previous $\mathcal{RBM}$s, but fails to capture such other intuitively small sets, whereas some previous $\mathcal{RBM}$s could[...]". As an alternative solution to obtain "reasonable" $\mathcal{RBM}$s, we propose, in definition 2.5, the introduction of a partial ordering relation *is better* on $\mathcal{RBM}$s. A good $\mathcal{RBM}$ will then be one that *is better* than many other $\mathcal{RBM}$s.

Definition 2.2. *Let $\mathcal{C} \subseteq \{0,1\}^\infty$. A measuring system ($\mathcal{MS}$) R for $\mathcal{C}$ is $\{R_i\}_{i\in\mathbb{N}}$, a family of subsets of $\mathcal{C}$ such that*

A1 $R_i \supseteq R_j$ *for* $j \geq i$
A2 $\cap_{i\in\mathbb{N}} R_i = \emptyset$
A3 $\forall i \in \mathbb{N}\ R_i \neq \emptyset$

The $\mathcal{RBM}$ associated to R is the following a partial function $\mu_R : \mathcal{P}(\mathcal{C}) \dashrightarrow \{0,1\}$ such that $\mu_R(A) = 0$ if $\exists k$ such that $A \subseteq \overline{R_k}^{\mathcal{C}}$, and $\mu_R(A) = 1$ if $\exists k$ such that $R_k \subseteq A$.

[1] The meaning of *suitable* in point 3 is informal, but it should definitely include finite unions.
[2] The term "slice" is used informally. For example, the k-th slice of P could be defined as $\mathtt{DTIME}(n^k)$.

Definition 2.3. *If a family R satisfies A1 only, it is called a pre-measuring system (pre-$\mathcal{MS}$).*

In the definition above, the terminology suggests a first relation between $\mathcal{MS}$s and $\mathcal{RBM}$s, since an $\mathcal{RBM}$ μ_R is defined from any given $\mathcal{MS}$ R, although at this point it remains to be shown that the function associated to an $\mathcal{MS}$ is an $\mathcal{RBM}$ in the sense of definition 2.1. The latter fact is the object of lemma 2.4, but before proving this it needs to be shown that the function associated to an $\mathcal{MS}$ is a well defined partial function.

Claim. The above partial function μ_R is well defined.

The above claim is easy, and can be shown to hold in this way. Suppose on the contrary, that for some fixed class $\mathcal{C}$ and for some fixed $\mathcal{MS}$ R on $\mathcal{C}$ there exists a set $A \subseteq \mathcal{C}$ such that "$\mu_R(A) = 1$ and $\mu_R(A) = 0$", i.e. μ_R is not well defined. Therefore there exist two integers k and k' such that $R_k \subseteq A$ and $A \subseteq \overline{R_{k'}}^{\mathcal{C}}$. Suppose that $k \leq k'$. Thus using $A1$, it holds that $R_{k'} \subseteq R_k$ and $\overline{R_k}^{\mathcal{C}} \subseteq \overline{R_{k'}}^{\mathcal{C}}$. The combination of the two previous formulae yields the following: $R_{k'} \subseteq R_k \subseteq A \subseteq \overline{R_{k'}}^{\mathcal{C}} \Rightarrow R_{k'} \subseteq A \subseteq \overline{R_{k'}}^{\mathcal{C}} \Rightarrow R_{k'} = \emptyset$, which is a contradiction to $A3$. A contradiction is obtained similarly if one supposes that $k' \leq k$, and thus the claim is substantiated. In the next lemma, we show that the function associated to an $\mathcal{MS}$ is indeed an $\mathcal{RBM}$ in the sense of definition 2.1.

Lemma 2.4. *If R is an $\mathcal{MS}$ on $\mathcal{C}$, then μ_R is an $\mathcal{RBM}$.*

Proof. We prove the five points separately. To show that $M1$ holds, let $\{L\}$ be a point in $\mathcal{C}$. By $A2$, it holds that $\cap_{i\in\mathbb{N}} R_i = \emptyset$, and thus $\exists i \in \mathbb{N}$ such that $L \notin R_i$. To conclude: $L \notin R_i \Rightarrow L \in \overline{R_i}^{\mathcal{C}} \Rightarrow \{L\} \subseteq \overline{R_i}^{\mathcal{C}} \overset{\text{def of } \mu_R}{\Rightarrow} \mu_R(\{L\}) = 0$. To show that $M2$ holds, recall that by $A1$ we have that $R_0 \subseteq \mathcal{C}$. Thus by definition of μ_R we have $\mu_R(\mathcal{C}) = 1$. For $M3$, let $\{A_i\}_{i\in I}$ be a collection of null sets for μ_R. This is equivalent to stating that $\forall i \in I\ \exists k \in \mathbb{N} \quad A_i \subseteq \overline{R_k}^{\mathcal{C}}$. Now we want the informal claim "if $\{A_i\}_{i\in\mathbb{N}}$ is a suitable family of null sets, then $\mu_R(\cup_{i\in\mathbb{N}} A_i) = 0$" to hold, where "suitable" definitely includes the case where I is finite. Suppose that $\{A_i\}_{i\in I}$ is a family of null sets such that the previous formula still holds when we invert the two quantifiers and thus obtain the following equation: $\exists k \in \mathbb{N}\ \forall i \in I \in \mathbb{N} \quad A_i \subseteq \overline{R_k}^{\mathcal{C}}$, then it is easy to show that $\mu(\cup_{i\in I} A_i) = 0$. So we shall adopt the convention that a family $\{A_i\}_{i\in I}$ of null sets, which thus satisfies the universal-existential formula above is a "suitable" union if it also satisfies the existential-universal formula obtained by inverting the universal and existential quantifiers from the previous formula. It is trivial that with this convention, finite unions of null sets are "suitable" unions. $M4$ is shown by noticing: if $\mu_R(B) = 0$, then $\exists k \in \mathbb{N}\ B \subseteq \overline{R_k}^{\mathcal{C}}$. Now if $A \subseteq B$, then also $\exists k \in \mathbb{N}\ A \subseteq \overline{R_k}^{\mathcal{C}}$. But by definition of μ_R, this latter fact implies that $\mu_R(A) = 0$. Finally, to prove that $M5$ holds, let $A \subseteq \mathcal{C}$, then the following holds: $\mu_R(A) = 0 \Leftrightarrow \exists k \in \mathbb{N}\ A \subseteq \overline{R_k}^{\mathcal{C}} \Leftrightarrow \exists k \in \mathbb{N}\ R_k \subseteq \overline{A}^{\mathcal{C}} \Leftrightarrow \mu_R(\overline{A}^{\mathcal{C}}) = 1$. □

The first use of the concept of $\mathcal{MS}$ is to permit to define the partial ordering relation *is better* on $\mathcal{RBM}$s discussed earlier in this section.

Definition 2.5. *Let R and μ be respectively an $\mathcal{MS}$ and an $\mathcal{RBM}$ on a single fixed class $\mathcal{C}$, then R is said to be an $\mathcal{MS}$ for μ if $\mu = \mu_R$. An $\mathcal{RBM}$ μ_1 is* better *than an $\mathcal{RBM}$ μ_2, which is denoted $\mu_1 \prec \mu_2$, if they both admit an $\mathcal{MS}$ and if μ_1 extends μ_2.* [3]

The idea behind the choice of comparing $\mathcal{RBM}$s that admit an $\mathcal{MS}$ only, is that it is considered nice for an $\mathcal{RBM}$ to admit an $\mathcal{MS}$, and therefore an $\mathcal{RBM}$ which does not admit an $\mathcal{MS}$ should *not* be considered better than one that does. In order to get interesting results on $\mathcal{RBM}$s on $\mathtt{P}$, we need to increase the technical tools at our disposal by continuing our investigations of the relations between $\mathcal{MS}$s and $\mathcal{RBM}$s. Lemma 2.4 shows that the concept of $\mathcal{MS}$ is stronger than that of $\mathcal{RBM}$, since it proves that each $\mathcal{MS}$ has an $\mathcal{RBM}$ associated with it. The reverse implication, stating that every $\mathcal{RBM}$ admits an $\mathcal{MS}$, can be shown to hold under certain conditions, as stated in the next lemma. Intuitively, it says that an $\mathcal{RBM}$ admits an $\mathcal{MS}$ if it is "consistent" with a pre-$\mathcal{MS}$. It can also be seen as a sufficient condition for a pre-$\mathcal{MS}$ to be an $\mathcal{MS}$.

[3] A partial function f extends a partial function g if $\mathcal{D}(g) \subseteq \mathcal{D}(f)$ and $f_{|\mathcal{D}(g)} = g$.

Lemma 2.6. *Let $\mathcal{C} \subseteq \{0,1\}^\infty$. Let $R = \{R_k\}_{k\in\mathbb{N}}$ and μ be respectively a pre-$\mathcal{MS}$ and an $\mathcal{RBM}$ on $\mathcal{C}$. If $[\mu(A) = 0 \Leftrightarrow \exists k \in \mathbb{N}\ A \subseteq \overline{R_k}^{\mathcal{C}}]$ then $[R$ is an $\mathcal{MS}$ on $\mathcal{C}$ and $\mu = \mu_R]$.*

Proof. We have to show that R is an $\mathcal{MS}$, and that $\mu = \mu_R$. Let us start by showing that under the assumptions R is an $\mathcal{MS}$. Since R is by hypothesis a pre-$\mathcal{MS}$, it only remains to be shown that R satisfies $A2$ and $A3$. To prove that $A2$ holds, suppose on the contrary that it does not. Then the following implications lead to a contradiction to $M1$: $\exists L \in \bigcap_{i\in\mathbb{N}} R_i \Rightarrow \exists L \in \mathcal{C}\ \forall i \in \mathbb{N}\ \{L\} \not\subseteq \overline{R_i}^{\mathcal{C}} \Rightarrow \exists L \in \mathcal{C}\ \mu(\{L\}) \neq 0$. To show that $A3$ holds, suppose on the contrary that it does not hold. Then there exists $i \in \mathbb{N}$ such that $R_i = \emptyset$. The following implications then lead to a contradiction to $M2$: $R_i = \emptyset \Rightarrow \mathcal{C} \subseteq \overline{R_i}^{\mathcal{C}} \Rightarrow \mu(\mathcal{C}) = 0$. Since at this point R is shown to be an $\mathcal{MS}$, one can consider μ_R its associated $\mathcal{RBM}$, and conclude using the following implication, which holds since μ satisfies $M5$ and by definition of μ_R: $[\mu(A) = 0 \Leftrightarrow \exists k\ A \subseteq \overline{R_k}^{\mathcal{C}}] \Rightarrow \mu = \mu_R$. □

Before using the mainframe described in this section to define and discuss, in section 4, the existence of *perfect measures*, we devote the next section to a reminder to the reader of the main result of [Str97], which is the construction of an $\mathcal{RBM}$ for P. This $\mathcal{RBM}$ will be analysed and compared to the definition of *perfect* $\mathcal{RBM}$ proposed.

3 A Previous Resource Bounded Measure on P

In this section, we summarise the construction of μ_τ, an $\mathcal{RBM}$ for P that emerged from the series of papers [AS94], [AS95] and [Str97]. The main mathematical concept used is that of a betting strategy [4], which is a function satisfying certain properties (see below), and being computable within certain resource bounds. We slightly change the way the original definition of μ_τ was given in [Str97] by introducing a topology, whereas this was done in [Str97] by means of a hierarchy of sub-basic null sets, basic null sets and null sets. We find that the definition gains in clarity by doing it this way, especially it is easier to then compare this $\mathcal{RBM}$ to its potential related $\mathcal{MS}$s. Nevertheless, this definition is equivalent to that of [Str97].

Definition 3.1. *A betting strategy is $\beta : \{0,1\}^* \to \mathbb{R}$ such that the three following points hold: first $\beta(\lambda) = 1$, where λ is the empty word. Second, $\forall \omega \in \{0,1\}^*\ \beta(\omega 0) = -\beta(\omega 1)$, where $\omega 0$ is the word ω concatenated with the symbol 0. Finally, $\forall \omega \in \{0,1\}^*\ \sum_{x \sqsubseteq \omega} \beta(x) \geq 0$, where $x \sqsubseteq \omega$ means that x is a prefix of ω.*

As its name suggests it, a betting strategy can be used to bet money when playing a particular game, called the *casino game* (c.f. for example [ASMRT00] for a description of this game). The next definition formalises the concept of a "win" for a betting strategy.

Definition 3.2. *Let $L \subseteq \{0,1\}^*$, let $\chi_L[i]$ be the unique prefix of length i of the characteristic sequence of L under the canonical ordering of $\{0,1\}^*$. Let β be a betting strategy. The success set of β, denoted $S^\infty[\beta]$, is defined to be: $S^\infty[\beta] := \{L \in \{0,1\}^\infty |\ \limsup_{N\to\infty} \sum_{i=0}^{N} \beta(\chi_L[i]) = \infty\}$.*

It is now time to turn our attention to the algorithmic resources needed to compute betting strategies. The two following definitions permit to suitably bound resources used by algorithms computing betting strategies, enabling the definition of an $\mathcal{RBM}$ for P.

Definition 3.3. *Let M be an algorithm. Let $\omega = \omega_0 \cdots \omega_N \in \{0,1\}^{N+1}$ for some $N \in \mathbb{N}$. The oriented graph $G_{M,\omega}$ with vertexes $V(G_{M,\omega}) \subseteq \{v_0, \cdots, v_N\}$ and edges $E(G_{M,\omega})$ is called the* graph of recursive queries *of the algorithm M on input ω, and is inductively thus defined: first, $\forall 0 \leq i \leq N$, v_i is added to $V(G_{M,\omega})$ if the algorithm M queries the ith bit of its input, during its computation on input $\omega = \omega_0 \cdots \omega_N$. Then, $\forall v_i$ previously added to $V(G_{M,\omega})$ and for all $j < i$, v_j is added to $V(G_{M,\omega})$ and (v_j, v_i) is added to $E(G_{M,\omega})$ iff M queries the jth bit of its input during its computation on input $\omega_0 \cdots \omega_i$.*

[4] A betting strategy is a generalisation of a martingale, which is the type of function traditionally used in the context of Lutz's RBM. The two concepts are transparent at the level of Lutz's RBM in "big" complexity classes.

Intuitively, the aim of defining such a graph is the following. Suppose that one wants to simulate the execution of the algorithm M on input ω, and each time the simulation of the algorithm M needs to read a bit of its input, it is required to simulate M on the prefix of ω of length equal to the index of the bit queried, and so on, recursively. This is roughly what needs to be done when computing a language L that diagonalises against a betting strategy computed by an algorithm M. Thus imposing size or depth restriction on the size of the graph of recursive queries permits to limit respectively the time or space complexity of the language L, c.f. [Str97] for more details.

Definition 3.4. *Let β be a betting strategy and t be a complexity function. β is a $\Gamma(t(n))$ betting strategy if there exists M, an algorithm such that $\forall \omega \in \{0,1\}^*$: $M(\omega) = \beta(\omega)$, $M(\omega)$ computes in $\mathtt{DTIME}(\mathcal{O}(t(|\omega|)))$ and $|V(G_{M,\omega})| = \mathcal{O}(t(|\omega|))$.*

As explained above, the idea behind this definition is that if a betting strategy is both efficiently computable *and* has a small graph of recursive queries, it will be possible to construct an efficiently computable language L that diagonalises against the given betting strategy. Notice that the condition on the size of the graph becomes void when the time-bound becomes at least linear (because the graph may then contain every possible node, i.e. the algorithm has enough time to read all its input), and that the notion of efficiently computable betting strategy then comes back to the traditional definition of efficiently computable betting strategy in the context of Lutz's $\mathcal{RBM}$ for complexity classes containing $\mathtt{E}$; c.f. [ASMRT00] for more details. In order to be able to state the definition of μ_τ, the $\mathcal{RBM}$ on $\mathtt{P}$ defined in [Str97], we also need to introduce a topology on the Cantor set. To define this topology, the notion of quotient of a language by a word is needed.

Definition 3.5. *Let $L \subseteq \{0,1\}^*$ be a language. Let $x \in \{0,1\}^*$ be a word. The language $L_{/x}$ of L quotiented by x is defined to be $L_{/x} := \{y \in \{0,1\}^* | \; yx \in L\}$.*

The following operation on language, called a direct product of languages, is useful in constructing a single language with many properties. Roughly speaking, in certain conditions which we are interested in, if a family of languages $\{R_i\}$ is such that each R_i has a property, depending on i, then $\bigotimes L_i$ will be a single language combining the properties of all the R_is. This fact is used in [Str97] and will also be used in the next section.

Definition 3.6. *Let $\{L_i\}_{i\in\mathbb{N}}$ be a family of languages. Their direct product is defined to be: $\bigotimes_{i\in\mathbb{N}} L_i := \{x10^i | \; x \in L_i\}$.*

Notice that *direct product* and *quotient* are complementary operations, as suggested by the following example: $(\bigotimes_{i\in\mathbb{N}} L_i)_{/10^i} = L_i$. By using the definition of the quotient of a language, open balls and the associated topology τ are defined.

Definition 3.7. *Let $L \subseteq \{0,1\}^*$. The open ball B_L centred on L is defined to be $B_L := \{L_{/x} | \; x \in \{0,1\}^*\}$. The topology τ is defined by: $\tau := \{O | \; L \in O \Rightarrow B_L \subseteq O\}$.*

The proof of the fact that τ is a topology (which is closed even under intersection) is easy, and left to the reader. Intuitively, a set belongs to the topology if it is closed under the operation consisting of constructing a new language L' from another language L, by defining the characteristic sequence of L' to be a regular subsequence of the characteristic sequence of L. For what we are interested in, that is considering betting strategies on languages, winning on every language of an open covering of a given set A is much harder then winning on A only, since it means that not only the betting strategy needs to cover every language in A, but also every language whose characteristic sequence is a "regular" substring of any language in A. Next comes the definition of μ_τ, and the theorem from [Str97], stating that it is an $\mathcal{RBM}$.

Definition 3.8. *Let $\mu_\tau : \mathcal{P}(\mathtt{P}) \dashrightarrow \{0,1\}$ be the following partial function: $\forall A \subseteq \mathtt{P}$, $\mu_\tau(A) = 0$ iff there exists $k \in \mathbb{N}$ and $\{\beta_i\}_{i\in\mathbb{N}}$ a family of $\Gamma(\log(N)^k)$ betting strategies such that $A \subseteq \cup_{i\in\mathbb{N}} \overset{\circ}{S^\infty}[\beta_i]$, [5] and $\forall A \subseteq \mathtt{P}$, $\mu_\tau(A) = 1$ iff $\mu_\tau(\overline{A}^{\mathcal{C}}) = 0$.*

[5] The notation $\overset{\circ}{A}$ denotes the interior (with respect to the topology τ) of the set A.

Theorem 3.9 ([Str97]). *μ_τ is well defined, and it satisfies M1 to M5, thus it is an $\mathcal{RBM}$ on* P.

In [Str97], some properties of this measure are demonstrated, such as the fact that some intuitively small sets are of null measure. It is also shown that this measure admits an equivalent measure for PSPACE, and it is then compared to the measure on PSPACE of [May94b]. An alternative definition of μ_τ in terms of random sets was also proposed, but this definition is erroneous, as we prove in the next section

4 Perfect Measures on P and Random Sets

In this section we revisit the problem of generalising Lutz's $\mathcal{RBM}$ to small complexity classes, and more precisely, to the class of time efficient solvable problems: P. We give a definition of perfection for an $\mathcal{RBM}$ on P, which is based on the idea that a perfect measure for P is one that generalises Lutz's $\mathcal{RBM}$, together with a necessary and sufficient condition, in terms of random sets, for such a perfect measure to exists. The guideline followed in this section is the revisiting of μ_τ, the $\mathcal{RBM}$ for P from [Str97] recalled in the last section, and more particularly, the discussion of a result from the same article, which is erroneous, and that we correct. It is while following this guideline, that we try our best to present the results of this section in a way that makes them look as intuitive as possible. We start by reminding the reader of the definition, central to this section, of random sets in the context of $\mathcal{RBM}$ at the scale P, and define the associated pre-$\mathcal{MS}$ at the same time.

Definition 4.1. *Let $L \in \mathtt{P}$ be a language. L is n^k-random if there is no $\Gamma(\log(N)^k)$ betting strategy covering L. Let $R^P_k := \{L \in \mathtt{P} \mid L \text{ is } n^k\text{-random}\}$. R^P is the following pre-$\mathcal{MS}$ on* P*: $R^P := \{R^P_k\}_{k\in\mathbb{N}}$.*

The question of whether this pre-$\mathcal{MS}$ is also an $\mathcal{MS}$ will be raised, and shown to have interesting implications. But before we come to this, let us enter the heart of the subject by stating a result from [Str97], which is the mistake that we correct later in this section.

Claim (erroneous). $\mu_\tau(A) = 0$ iff $\exists k \in \mathbb{N}$ such that $A \cap R^P_k = \emptyset$

In the rest of this article, we refer to this claim as the "erroneous claim". This claim may seem very plausible at first sight, and in fact only a subtle detail in the (pseudo) proof of it, which is in [Str97] too, is inconsistent. What makes this claim not so likely, is when its consequences are analysed with the insight of the concept of $\mathcal{MS}$s. To come to the point, let us start by using lemma 2.6 to obtain two easy consequences that would follow should the erroneous claim hold: the first consequence is named <u>$C1$</u> and is the following: $R^P$is an $\mathcal{MS}$ for P. The second is <u>$C2$</u>: $\mu_{R^P} = \mu_\tau$. The following result of [ASTZ97], restated in our notations, permits an interesting interpretation of the two previous statements.

Lemma 4.2 ([ASTZ97]). *Let R^E_k=$\{L \in E \mid$ there exists a $\Gamma(N^k)$ betting strategy covering $L\}$. Let $R^E = \{R^E_k\}_{k\in\mathbb{N}}$. R^E is an $\mathcal{MS}$ for* E *and $\mu_{R^E} = \mu_{Lutz}$, where μ_{Lutz} is Lutz's $\mathcal{RBM}$ for* E.

The main observation is that the pre-$\mathcal{MS}$ R^P is the P analogous of $R^{\mathtt{E}}$ in E. Pushing further the idea behind this observation, and supposing that $C1$ holds, lemma 2.4 implies that μ_{R^P} is an $\mathcal{RBM}$ for P, which is thus the P analogous of μ_{R^E}, and thus of μ_{Lutz}. Adopting the terminology of calling perfect a measure that is analogous to (or better then) Lutz's $\mathcal{RBM}$, we define:

Definition 4.3. *An $\mathcal{RBM}$ μ for* P *is said to be perfect if it admits $\tilde{R} = \{\tilde{R}_j\}_{j\in\mathbb{N}}$ an $\mathcal{MS}$ such that $\forall k \in \mathbb{N} \exists j \in \mathbb{N} \mid \tilde{R}_j \subseteq R^P_k$.*

Notice that it is immediate that if there exists a perfect measure μ, then μ_{R^P} is a well defined measure such that μ is better than μ_{R^P}. With this definition of perfection for an $\mathcal{RBM}$, it is easy to see that the statements $C1$ and $C2$ imply that *there exists a perfect $\mathcal{RBM}$ for* P and *μ_τ is a perfect $\mathcal{RBM}$ for* P respectively. The following figure sums up the discussion pursued so far.

$$\text{Erroneous claim} \overset{\text{lemma 2.6}}{\Rightarrow} \begin{cases} C1 \text{ holds} \Rightarrow \text{There exists a perfect measure for } \mathtt{P} \\ C2 \text{ holds} \Rightarrow \mu_\tau \text{ is a perfect measure for } \mathtt{P} \end{cases}$$

This sets the general context in which the following results are obtained. The first result is the fact that μ_τ admits an $\mathcal{MS}$, which is composed of a family of a special kind of random sets, a result that can be seen as an alternative to the erroneous claim. Second is the fact that the *existence of random sets* is a necessary and sufficient condition for the existence of a perfect measure. Third is the exhibition of another sufficient condition, called the *unique betting strategy hypothesis*, to the existence of a perfect measure. Finally, it is shown that μ_τ is *not* a perfect measure, which implies that the erroneous claim is false. These results are now given in full detail in the following three subsections.

4.1 Alternative Random sets to Characterise μ_τ

Starting with the first point of the scheme given above, we show that μ_τ admits an $\mathcal{MS}$, consisting of a parametrised family of an alternative definition of random sets for $\mathtt{P}$, which also defines a pre-$\mathcal{MS}$.

Definition 4.4. *Let $L \in \mathtt{P}$ be a language. L is n^k_τ-random if there is no $\Gamma(\log(N)^k)$ betting strategy covering B_L. Let $R^P_{k,\tau} := \{L \in \mathtt{P} \,|\, L \text{ is } n^k_\tau\text{-random}\}$. R^P_τ is the following pre-$\mathcal{MS}$ on $\mathtt{P}$: $R^P_\tau := \{R^P_{k,\tau}\}_{k\in\mathbb{N}}$.*

Lemma 4.5. *Let $A \subseteq \mathtt{P}$, then $\mu_\tau(A) = 0$ iff $\exists k \in \mathbb{N}$ such that $A \cap R^P_{k,\tau} = \emptyset$.*

Proof. Let us start with the (easy) direct implication. If $A \subseteq \mathtt{P}$ is such that $\mu_\tau(A) = 0$, then there exist $k \in \mathbb{N}$ and $\{\beta_i\}_{i\in\mathbb{N}}$, a family of $\Gamma(\log(N)^k)$ betting strategies, such that $A \subseteq \cup_{i\in\mathbb{N}} \overset{\circ}{S^\infty}[\beta_i]$. Therefore $\forall L \in A$, $\exists\beta$ a $\Gamma(\log(N)^k)$ betting strategy such that $L \in \overset{\circ}{S^\infty}[\beta]$. Now observe the following: if $L \in \overset{\circ}{S^\infty}[\beta]$ and $\overset{\circ}{S^\infty}[\beta] \in \tau$, then $B_L \subseteq \overset{\circ}{S^\infty}[\beta]$, and hence $L \in \overline{R^P_{k,\tau}}^{\mathcal{C}}$. Since this is true for any language $L \in A$, it implies that $A \subseteq \overline{R^P_{k,\tau}}^{\mathcal{C}}$, which proves the first implication. Now let us prove the reverse implication. Suppose that $A \subseteq \mathtt{P}$ is such that for some fixed integer k, it holds that $A \subseteq \overline{R^P_{k,\tau}}^{\mathcal{C}}$. First consider $\{\beta_i\}_{i\in\mathbb{N}}$ an enumeration of all $\Gamma(\log(N)^k)$ betting strategies. Such an enumeration exists, since all $\Gamma(\log(N)^k)$ betting strategies admit an algorithm computing them, and since algorithms are enumerable. Since $A \subseteq \overline{R^P_{k,\tau}}^{\mathcal{C}}$, it holds that $\forall L \in A \quad \exists i \in \mathbb{N}$ *such that* $B_L \subseteq S^\infty[\beta_i]$. The last formula implies that $B_L \subseteq \overset{\circ}{S^\infty}[\beta_i]$, and that $L \in \overset{\circ}{S^\infty}[\beta_i]$. Since for any $L \in A$ this is true for some $i \in \mathbb{N}$, then $A \subseteq \cup_{i\in\mathbb{N}} \overset{\circ}{S^\infty}[\beta_i]$. Now the following observation permits to conclude: If $A \subseteq \cup_{i\in\mathbb{N}} \overset{\circ}{S^\infty}[\beta_i]$ and $\{\beta_i\}_{i\in\mathbb{N}}$ *is a family of $\Gamma(\log(N)^k)$ betting strategies*, then by definition of μ_τ, $\mu_\tau(A) = 0$. □

Corollary 4.6. *The two following points hold. <u>$C'1$</u>: R^P_τ is an $\mathcal{MS}$ for $\mathtt{P}$. <u>$C'2$</u>: $\mu_{R^P_\tau} = \mu_\tau$.*

The last corollary is obtained using lemmas 2.6 and 4.5 in conjunction. The first point of this corollary, $C'1$, says that R^P_τ is an $\mathcal{MS}$. The open problem discussed earlier in this section asking whether R^P is an $\mathcal{MS}$, which implies [6] that there exists a perfect measure for $\mathtt{P}$, seems very similar. Since we managed to prove that $C'1$ holds, i.e. that R^P_τ is an $\mathcal{MS}$, it is natural to enthusiastically hope to prove, using the same techniques, that R^P is an $\mathcal{MS}$, and the existence of a perfect $\mathcal{RBM}$ for $\mathtt{P}$ at the same time. This cannot be done, so if $C1$ has to be proven to hold, it will be in another way. The reason is the following: $C'1$ is a corollary of lemma 4.5. Thus proving that $C1$ holds, adapting the proof that $C'1$ does, would require an analogue of lemma 4.5, with the family R^P_τ replaced by the family R^P: but this is precisely the erroneous claim, and as we are going to prove in subsection 4.2, the erroneous claim does *not* hold. Therefore the problem of proving or disproving $C1$, i.e. whether there exists a perfect measure for $\mathtt{P}$, remains open. Now that we have a characterisation of μ_τ in terms of (an alternative kind of) random sets, let us turn to the relation between random sets and perfect measures.

[6] In fact, as shown in lemma 4.7, not only does this condition imply, but it is even equivalent to the existence of a perfect measure.

4.2 Conditional Existence of Perfect Measures

This subsection is devoted to discussing sufficient (and necessary) conditions for the existence of perfect $\mathcal{RBM}$s. The main result is to prove that there exist perfect $\mathcal{RBM}$s iff there exist random sets. This will be obtained as a corollary of the next lemma, which shows that the existence of a perfect measure is equivalent to the fact that the pre-$\mathcal{MS}$ of random sets is also an $\mathcal{MS}$.

Lemma 4.7. *There exists a perfect $\mathcal{RBM}$ iff the pre-$\mathcal{MS}$ R^P is also an $\mathcal{MS}$*

Proof. We only prove the direct implication, since the reverse implication is easy, and therefore left to the reader. Since R^P is a pre-$\mathcal{MS}$, we only need to show that the assumptions imply that R^P satisfies points $A2$ and $A3$ of definition 2.2 Let us start with $A2$, which can be proved to hold unconditionally. We need to prove that $\cap_{i\in\mathbb{N}} R^P_i = \emptyset$. It is easy to see from the definitions of R^P_τ and R^P that it holds that $R^P_k \subseteq R^P_{k,\tau}$ for any $k \in \mathbb{N}$. Now since corollary 4.6 insures that R^P_τ is an $\mathcal{MS}$, it holds that $\cap_{i\in\mathbb{N}} R^P_{i,\tau} = \emptyset$, and thus $A2$ follows. We now prove $A3$, that is the fact that $R^P_i \neq \emptyset$ for any $i \in \mathbb{N}$, using the assumption that there exists a perfect $\mathcal{RBM}$. By definition of the existence of a perfect measure, there exists $\tilde{R} = \{\tilde{R}_i\}_{i\in\mathbb{N}}$ an $\mathcal{MS}$ such that $\forall k \in \mathbb{N} \exists i \in \mathbb{N}$ such that $\tilde{R}_i \subseteq R^P_k$. Since $\tilde{R}$ is an $\mathcal{MS}$, $\forall i\ \tilde{R}_i \neq \emptyset$, and thus $\forall k\ R^P_k \neq \emptyset$. □

Since $A2$ in the proof above is shown to hold unconditionally, the next corollary follows.

Corollary 4.8. *There exists a perfect $\mathcal{RBM}$ iff there are random sets, i.e. if $R^P_i \neq \emptyset$ for all i.*

Next comes the discussion of another condition, sufficient for the existence of a perfect $\mathcal{RBM}$. As explained in the literature, one of the main technical difficulties in defining an $\mathcal{RBM}$ for small complexity classes comes from the fact that it cannot be proved that the following assertion (or a variation of it) holds:

Definition 4.9. *We call the following assertion the* unique betting strategy *hypothesis:* $\forall k \in \mathbb{N}\ \forall \{\beta_i\}_{i\in\mathbb{N}}$ *family of* $\Gamma(n^k)$ *betting strategies* $\exists k' \in \mathbb{N}\ \exists \beta$ *a* $\Gamma(n^{k'})$ *betting strategy such that* $\cup_{i\in\mathbb{N}} S^\infty[\beta_i] \subseteq S^\infty[\beta']$.

The fact that this hypothesis cannot be shown to hold (nor its negation) is the main difference with $\mathcal{RBM}$ at the level of $\mathtt{E}$, where the equivalent assertion is true indeed. It is easy to see that if this condition was to hold, the following function, which is the transposition of Lutz's $\mathcal{RBM}$ on $\mathtt{E}$, would define an $\mathcal{RBM}$ on $\mathtt{P}$: $\mu_L : \mathcal{P}(\mathtt{P}) \dashrightarrow \{0,1\}$, where $\mu_L(A) = 0$ if $\exists k \exists \beta$ a $\Gamma(n^k)$ betting strategy such that $A \subseteq S^\infty[\beta]$, and $\mu_L(A) = 1$ if $\mu_L(\mathtt{P} \setminus A) = 0$. Next comes a lemma comparing the *unique betting strategy hypothesis* and the *existence of random sets.* It shows two things:

- The *unique betting strategy hypothesis* is stronger then that of the *existence of random sets.*
- Although it is not obvious and is unknown to us whether the reverse is true, i.e. whether the *existence of random sets* implies that the *unique betting strategy hypothesis* holds, the hypothesis of the existence of random sets is as as strong as the unique betting strategy when it comes to defining measures.

We consider this latter fact as strong evidence that the definition chosen for a *perfect* measure does indeed capture the essence of an ideal generalisation of Lutz's $\mathcal{RBM}$.

Lemma 4.10. *If the unique betting strategy hypothesis holds, then there exist random sets. Furthermore, in this configuration,* $\mu_{R^P} = \mu_L$.

Proof. Suppose that the unique betting strategy hypothesis holds. We want to prove that for any $k \in \mathbb{N}$, there exists an n^k-random set, i.e. there exists a language $L \in \mathtt{P}$ such that $L \notin \cup_{\beta\in\{\Gamma(n^k)\text{betting strategies}\}} S^\infty[\beta]$. By hypothesis, there exists k' and γ a $\Gamma(n^{k'})$ betting strategy such that $\cup_{\beta\in\{\Gamma(n^k)\text{betting strategies}\}} S^\infty[\beta] \subseteq S^\infty[\gamma]$. Since the definition of Γ betting strategies was given in order to enable the construction of a language $L \in \mathtt{P}$ that diagonalises against a single betting strategy, it is easy to construct a language of $\mathtt{P}$ which is not in $S^\infty[\gamma]$, and thus not in $\cup_{\beta\in\{\Gamma(n^k)\text{betting strategies}\}} S^\infty[\beta]$ either. Such a language L is by definition an n^k-random set, and thus the fact that the hypothesis implies the existence of random sets follows. To prove that under the assumption of the lemma, $\mu_L = \mu_{R^P}$, it only needs to be shown that for any $A \subseteq \mathtt{P}$, $\mu_L(A) = 0$ iff $\mu_{R^P}(A) = 0$. Suppose that $\mu_L(A) = 0$, then there exists $k \in \mathbb{N}$ and γ a $\Gamma(n^k)$ betting strategy, such that $A \subseteq S^\infty[\gamma]$. Thus $A \cap \{n^k\text{-random}\} = \emptyset$, and by definition $\mu_{R^P}(A) = 0$. On the other hand, suppose that $A \subseteq \mathtt{P}$ is such that $\mu_{R^P}(A) = 0$. Therefore there exists k such that $A \cap \{n^k\text{-random}\} = \emptyset$. Thus $A \subseteq \cup_{\beta \in \{\Gamma(n^k)\text{betting strategies}\}} S^\infty[\beta]$. By hypothesis, there exists k' and γ a $\Gamma(n^k)$ betting strategy such that $A \subseteq S^\infty[\gamma]$, and thus $\mu_L(A) = 0$. □

Remark 4.11. In [Str97], as well as in this article, it is ensured that no "good" betting strategy covers the whole space P, thanks to the third point of definition 3.4 which forces a condition on the graph of recursive queries. It ensures that for any $\Gamma(n^k)$ betting strategy, there exists a language $L \notin S^\infty[\beta]$ which is computable in $\mathtt{DTIME}(n^{(2k+1)})$, c.f. [Str97] for more details. This restriction imposed to the size of the graph of recursive queries of "good" betting strategies could be replaced by the following: *for any $\Gamma(n^k)$ betting strategy β, there has to exist a language L in $\mathtt{DTIME}(n^{f(k)})$ such that $L \notin S^\infty[\beta]$*, where f is some arbitrary computable function. It would enable the definition of measures $\mu_\tau{}'$ "à la Strauss", generalising μ_τ, but this is probably of little interest, at least from a theoretical point of view, since it would not add much to the concepts and the ideas of [Str97]. On the other hand, the choice of ensuring that no "good" betting strategy covers the whole space P by imposing a restriction on the graph of recursive queries, or any generalisation of this concept, as proposed above, is an arbitrary choice, and therefore unpleasant regarding our claim of having defined a "perfect measure". This can be solved by the following remark. If one replaces the third point of definition 3.4 by the following: *a $\Gamma(n^k)$ betting strategy β must not cover the whole of* P, then all the proofs of this subsection go unchanged. The definition of a perfect measure thus obtained has the advantage of being free of any arbitrary choice .

4.3 Previous Relations between μ_τ and Randomness

The main result of this subsection is the proof that μ_τ is not perfect. This latter fact implies that the erroneous claim does not hold. First of all, we state and prove a technical lemma.

Lemma 4.12. $\exists \mathcal{A} \subseteq \mathtt{P}\ \exists k \in \mathbb{N}$ *such that* $\mathcal{A} \subseteq \overline{R_k^P}^{\mathcal{C}}$ *but* $\mu_\tau(\mathcal{A}) \neq 0$

Proof. Suppose on the contrary that the lemma is false, then the following implication holds for any $\mathcal{A} \in \mathtt{P}$: $\forall k \in \mathbb{N} \quad \mathcal{A} \subseteq \overline{R_k^P}^{\mathcal{C}} \;\Rightarrow\; \mu_\tau(\mathcal{A}) = 0$. If $\exists K \in \mathbb{N}$ such that $\forall k \geq K\ R_k^P = \emptyset$,then the previous equation implies that $\mu_\tau(\mathtt{P}) = 0$. This is a contradiction to theorem 3.9, which states that μ_τ satisfies $M2$, and thus $\mu_\tau(\mathtt{P}) = 1$. Thus $\forall k \in \mathbb{N}$, $R_k^P \neq \emptyset$, and there exists $\{L_i\}_{i \in \mathbb{N}}$ a family of languages such that $\forall i \in \mathbb{N}\ L_i \in R_i^P$. Let L be the empty language, and consider the following class of languages: $\mathcal{A} := \bigcup_{i \in \mathbb{N}} \{L \otimes L_i\} = \bigcup_{i \in \mathbb{N}} \{\tilde{L}_i\}$, where $\tilde{L}_i := \{x10 | x \in L\} \cup \{x100 | x \in L_i\} = \{x100 | x \in L_i\}$. Now we need the three following claims, for which we also give a short idea of the demonstration. *Claim 1:* $\mathcal{A} \subseteq \mathtt{P}$. *Claim2:* $\exists k \in \mathbb{N}$ such that $\mathcal{A} \cap R_k^P = \emptyset$. *Claim 3:* $\mu_\tau(\mathcal{A}) \neq 0$. To show that the first claim holds, it is sufficient to show that $\forall i \in \mathbb{N}\ \tilde{L}_i \in \mathtt{P}$. But this is an easy consequence of the fact that $\forall i \in \mathbb{N}\ L_i \in \mathtt{P}$. To be convinced that the second claim holds, notice that it is easy to construct a $\Gamma(\log(N))$ betting strategy that wagers on words of the form 0^*10 only, and that covers $\mathcal{A}$. For the third claim, suppose the contrary, i.e. $\mu_\tau(\mathcal{A}) = 0$. Therefore there would exist $k \in \mathbb{N}$ and $\{\beta_i\}_{i \in \mathbb{N}}$ a family of $\Gamma(\log(N)^k)$ betting strategies such that $\mathcal{A} \subseteq \bigcup_{i \in \mathbb{N}} \overset{\circ}{S^\infty}[\beta_i]$. Together with the fact that $\forall j\ \tilde{L}_j \in \mathcal{A}$, it implies that $\forall j \in \mathbb{N}\ \exists i \in \mathbb{N}$ *such that* $\tilde{L}_j \in \overset{\circ}{S^\infty}[\beta_i]$. Now since $\overset{\circ}{S^\infty}[\beta_i] \in \tau$, it must also be that $\forall j \in \mathbb{N}\ \exists i \in \mathbb{N}$ *such that* $B_{\tilde{L}_j} \subseteq \overset{\circ}{S^\infty}[\beta_i]$. Finally, in conjunction with the fact that $\forall j\ L_j \in B_{\tilde{L}_j}$, it implies that $\forall j \in \mathbb{N}\ \exists i \in \mathbb{N}$ *such that* $L_j \in \overset{\circ}{S^\infty}[\beta_i]$. Since for all $i \in \mathbb{N}$, β_i is by assumption a $\Gamma(\log(N)^k)$ betting strategy, it thus also holds that for all $j \in \mathbb{N}$, $L_j \notin R_k^P$, which yields a contradiction when $j \geq k$, (since by construction $\{L_j\}_{j \in \mathbb{N}}$ is a family of languages such that $L_j \in R_j^P \subseteq R_k^P$). The three claims above give rise to the following contradiction: the first two claims show that the set $\mathcal{A}$ (constructed using the absurd hypothesis that the lemma does not hold) satisfies $\mathcal{A} \subseteq \mathtt{P} \cap \overline{R_k^P}^{\mathcal{C}}$. Since by the absurd hypothesis, the lemma is false, then necessarily $\mu_\tau(\mathcal{A}) = 0$, which is a contradiction to the third claim. □

This technical lemma enables one to compare μ_τ and μ_{R^P} in terms of the partial ordering relation *is better* defined in section 2.

Lemma 4.13. *If R^P is an $\mathcal{MS}$, then μ_{R^P} is strictly better than μ_τ*

Proof. Suppose that R^P is an $\mathcal{MS}$. Thus the function μ_{R^P} is defined, and is an $\mathcal{RBM}$. Now we need to prove the two following facts: $\mu_{R^P} \prec \mu_\tau$ and $\mu_\tau \not\prec \mu_{R^P}$. Let us prove the two things separately: for the first point, and by definition of the relation *is better*, we have to show that both $\mathcal{RBM}$s admit an $\mathcal{MS}$ and that μ_{R^P} extends μ_τ. The fact that μ_{R^P} admits an $\mathcal{MS}$ is trivial, and μ_τ admits an $\mathcal{MS}$ too, as follows from corollary 4.6. The assertion that μ_{R^P} extends μ_τ is substantiated by showing that for any $A \subseteq \mathtt{P}$, if A is μ_τ measurable, then A is μ_{R^P} measurable, and $\mu_\tau(A) = \mu_{R^P}(A)$: first suppose that μ_τ is defined on A and that $\mu_\tau(A) = 0$. Together with lemma 4.5, it implies that $\exists k \in \mathbb{N}$ *such that* $A \cap R_{k,\tau}^P = \emptyset$. Now since by definition of R^P and R_τ^P, it holds that $\forall k \in \mathbb{N}\ R_k^P \subseteq R_{k,\tau}^P$, we also have that $\exists k \in \mathbb{N}$ *such that* $A \subseteq \overline{R_k^P}^{\mathcal{C}}$. Now using the hypothesis that R^P is an $\mathcal{MS}$ and definition 2.2, the last equation implies in turn that A is μ_{R^P} measurable and that $\mu_{R^P}(A) = 0$. A similar proof holds if one starts with the case where A is μ_τ measurable with $\mu_\tau(A) = 1$, and thus μ_{R^P} extends μ_τ. This also finishes the proof that $\mu_{R^P} \prec \mu_\tau$. We now turn to proving that $\mu_\tau \not\prec \mu_{R^P}$. Suppose on the contrary that $\mu_\tau \prec \mu_{R^P}$. If this were so, then we would have the following implications: $\mu_\tau \prec \mu_{R^P} \Rightarrow [\forall A \subseteq \mathtt{P}\ \mu_{R^P}(A) = 0 \Rightarrow \mu_\tau(A) = 0] \Rightarrow \forall A \subseteq \mathtt{P}$ *such that* $\exists k \in \mathbb{N}\ A \subseteq \overline{R_k^P}^{\mathcal{C}}$, $\mu_\tau(A) = 0$. But the last implication is a contradiction to lemma 4.12, thus the absurd hypothesis that $\mu_\tau \prec \mu_{R^P}$ is false. □

The next corollary follows from the easy claim that if a measure μ is perfect, then necessarily $\mu \prec \mu_{R^P}$. Together with corollary 4.5, it makes a correction to the erroneous claim.

Corollary 4.14. *μ_τ is not a perfect measure, C2 does not hold and the erroneous claim does not hold.*

5 Conclusion

We have proposed a definition of a perfect $\mathcal{RBM}$ in small complexity classes, which is intuitively an $\mathcal{RBM}$ that reproduces truly, at the level of $\mathtt{P}$, Lutz's $\mathcal{RBM}$ in $\mathtt{E}$. The question of whether such a measure exists, which is central to this line of research, is not answered, but it is shown that the existence of such a perfect measure admits a sufficient and necessary condition: the *existence of random sets* (in the context of resource bounded measure, and with suitable parameters). It was shown in lemma 4.10 that the *unique betting strategy* hypothesis, which holds in the context of Lutz's $\mathcal{RBM}$, is stronger then the hypothesis of the *existence of random sets*, but that surprisingly, it yields the same notion of measure. This could be due to the fact that both hypotheses are equivalent: we have not proven that the *unique betting strategy* is *strictly* better than the hypothesis of the *existence of random sets*; so this is left as an open problem. We also revisited the measure for $\mathtt{P}$ that was developed in [Str97], and corrected a mistake concerning the relation of this measure to random sets.

References

[AS94] E. Allender and M. Strauss. Measure on small complexity classes, with applications for BPP. In *Proceedings of the 35th IEEE Annual Symposium on Foundations of Computer Science*, volume 35, pages 807–818, 1994.

[AS95] E. Allender and M. Strauss. Measure on P: Robustness of the notion. In *Proceedings of the 20th Mathematical Foundations of Computer Science*, volume 969, pages 129–138. Springer, 1995.

[AS00] K. Ambos-Spies. Measure theoretic completeness notions for the exponential time classes. In *Mathematical Foundations of Computer Science*, volume 1893 of *Lecture Notes in Computer Science*, pages 152–161. Springer, 2000.

[ASLM98] K. Ambos-Spies, S. Lempp, and G. Mainhardt. Randomness vs. completeness: on the diagonalisation strength of resource bounded random sets. In *Mathematical Foundations of Computer Science*, volume 1450 of *Lecture Notes in Computer Science*, pages 465–473. Springer, 1998.

[ASMRT00] K. Ambos-Spies, W. Merkle, J. Reimann, and S. Terwijn. Almost complete sets. *Preliminary version in Symposium on Theoretical Aspects of Computer Science*, 1770:419–430, 2000. To appear in Theoretical Computer Science.

[ASMZ96] K. Ambos-Spies, E. Mayordomo, and X. Zheng. A comparison of weak completeness notions. In *Proceedings of the 11th Annual Comference on Computational Complexity*, pages 171–178. IEEE Computer Society Press, 1996.

[ASTZ97] K. Ambos-Spies, S.A. Terwijn, and X. Zheng. Resource bounded randomness and weakly complete problems. *Theoretical Computer Science*, 168:195–207, 1997.

[BC94] D.P. Bovet and P. Crescenzi. *Introduction to the Theory of Complexity.* Addison-Wesley, 1994.

[BDG94a] J.L Balcázar, J. Díaz, and J. Gabaró. *Structural Complexity I.* Springer-Verlag, 1994.

[BDG94b] J.L Balcázar, J. Díaz, and J. Gabaró. *Structural Complexity II.* Springer-Verlag 1990, 1994.

[CSS97] J.-Y. Cai, D. Sivakumar, and M. Strauss. Constant depth circuits and the lutz hypothesis. *IEEE Symposium on Foundations of Computer Science*, 1997.

[JL95a] D.W. Juedes and J.H. Lutz. The complexity and distribution of hard problems. *SIAM Journal on Computing*, 24(2):279–295, 1995.

[JL95b] D.W. Juedes and J.H. Lutz. Weak completeness in e and e_2. *Theoretical Computer Science*, 143:149–158, 1995.

[Jue95] D.W. Juedes. Weakly complete problems are not rare. *Computational Complexity*, 5:267–283, 1995.

[LM94] J.H. Lutz and E. Mayordomo. Measure, stochasticity, and the density of hard languages. *SIAM Journal on Computing*, 23:762–779, 1994.

[LM96] J.H. Lutz and E. Mayordomo. Cook versus Karp-Levin: Separating completeness notions if NP is not small. *Theoretical Computer Science*, 164(1–2):141–163, 1996.

[Lut92] J.H. Lutz. Almost everywhere high non-uniform complexity. *Journal of Computer and System Science*, 44:220–258, 1992.

[Lut95] J.H. Lutz. Weakly hard problems. *SIAM Journal on Computing*, 24:1170–1189, 1995.

[Lut96] J. H. Lutz. Observations on measure and lowness for Δ_2^{P}. In *Proceedings of the 13th Symposium on Theoretical Aspects of Computer Science*, volume 1046 of *Lecture Notes in Computer Science*, pages 87–97, Berlin, 1996. Springer Verlag.

[Lut97a] J. H. Lutz. The quantitative structure of exponential time. In L. A. Hemaspaandra and A. L. Selman, editors, *Complexity Retrospective II*, chapter 12, pages 250–254. Springer, 1997.

[Lut97b] J. H. Lutz. The quantitative structure of exponential time. In L. A. Hemaspaandra and A. L. Selman, editors, *Complexity Retrospective II*, pages 225–260. Springer, 1997.

[May94a] E. Mayordomo. Almost every set in exponential time is P-bi-immune. *Theoretical Computer Science*, 136:487–156, 1994.

[May94b] E. Mayordomo. *Contribution to the Study of Resource Bounded Measure.* PhD thesis, Universitat Politécnica de Catalunya, Barcelona, 1994.

[Mer95] W. Merkle. Personal communication, 1995.

[MV93] M.L. and P. Vitànyi. *An Introduction to Kolmogorov Complexity and its Applications.* Springer-Verlag New York, 1993.

[Pap94] C.H. Papadimitriou. *Computational Complexity.* Addison-Wesley, 1994.

[RS98] K.W. Regan and D. Sivakumar. Probabilistic martingales and BPTIME classes. *IEEE*, pages 186–200, 1998.

[Str97] M. Strauss. Measure on P: Strength of the notion. *Information and Computation*, 136(1):1–23, 1997.

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'