A note on measuring in \( P \)

Olivier Powell

Centre Universitaire d’Informatique, Université de Genève, rue du Général Dufour 24, CH-1211 Genève 4, Switzerland

Received 19 August 2002; received in revised form 19 November 2003; accepted 30 January 2004

Communicated by J. Diaz

Abstract

We revisit the problem of generalising Lutz’s resource-bounded measure (\( \mu_{\text{RBM}} \)) to small complexity classes, and propose a definition of a random-based \( \mu_{\text{RBM}} \) on \( P = \bigcup_{k \in \mathbb{N}} \text{DTIME}(\tilde{c}(n^k)) \), which we argue as being a good generalisation to \( P \) of Lutz’s \( \mu_{\text{RBM}} \). We cannot unconditionally prove the existence of such a measure, but we give sufficient and necessary conditions for its existence. We also revisit \( \mu_{\text{RBM}} \) for \( P \) defined by Strauss [Inform. Comput. 136(1) (1997) 1], and correct an erroneous claim concerning the relations between \( \mu_{\text{RBM}} \) and random sets. A correction to this mistake is then proposed, which is a less powerful but accurate relation between \( \mu_{\text{RBM}} \) and random sets.

In order to obtain these results, we introduce a mathematical structure called a measuring system, which is a general setting that can be used to compare different \( \mu_{\text{RBM}} \)'s on any fixed complexity class through a partial ordering relation.

© 2004 Elsevier B.V. All rights reserved.

Keywords: Resource-bounded measure; Martingale; Computational complexity

1. Introduction

Resource-bounded measure (\( \mu_{\text{RBM}} \)) was introduced by Lutz [11]. Roughly speaking, \( \mu_{\text{RBM}} \) 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 \( \text{EXP} \). The theory of \( \mu_{\text{RBM}} \) is a parametrised tool, which permits one to obtain an \( \mu_{\text{RBM}} \) for many complexity classes: one just adapts the parameters in order to obtain an \( \mu_{\text{RBM}} \) at the desired scale. One of the major limitations of \( \mu_{\text{RBM}} \) 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 \( \text{PSPACE} \), which do not (or are

E-mail address: olivier.powell@cui.unige.ch (O. Powell).
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 RBM to small complexity classes. In [18], an RBM is defined on PSPACE, using a concept of on line Turing machines. This definition yields a notion of RBM in PSPACE, which is interesting but sadly fails to extend to P. Further attempts to construct RBMs for P can be found in the series of papers [1,2,19]. 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 [1] 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 [7], 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 does not hold when translated to P, cf. [1,9,13,15–17] or, for a survey of the previous results, [14]. Nevertheless, these constructions all make compromises with the ideal generalisation of Lutz’s RBM to small complexity classes, which consists of extending Lutz’s RBM to small complexity classes by modifying only the parameters (which, for example, permit one to obtain an RBM on E or EXP). It is interesting to note that such an ideal generalisation of Lutz’s 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 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 RBMs in small complexity classes are unsatisfactory from a theoretical point of view, since the direct approach (plugging into the general theory the adequate parameters) could define consistent notions of RBM for small complexity classes. 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 [3,4–6,8,10,12], could perhaps be adapted to small complexity classes if the ideal generalisation of Lutz’s RBM were indeed a consistent 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 RBM on small complexity classes is to define a concept of random-based RBM, which we argue as being a good generalisation to P of Lutz’s RBM for E, and to give two sufficient conditions for such a measure to exist, one of them, namely the existence of random sets, being also a necessary condition. While trying to give some insight into these questions, we also re-describe μ, the RBM from [19], and point out a mistake in this article which has strong implications if it is not corrected, since it implies the unconditional existence of a random-based measure for P.

2. An axiomatic definition of resource-bounded measure

The goal of this section is to define the concepts of a measuring system (MF) and a RBM. These concepts are used to obtain the results of this article. Although not as
general as RBMs, MSs have the advantage of allowing the definition of a natural generalisation of Lutz’s RBM for P. Intuitively, RBMs and MSs are the following:

An RBM on a fixed class of languages C separates the subsets of C into small sets: those of null measure, and large sets: those of measure one.

An MS is a structure that induces an RBM, whereas the converse is not true. Thus, there are “more” RBMs than MSs. Exact definitions follow.

**Definition 2.1.** Let \( C \subseteq \{0, 1\}^\infty \). A \( \sigma \)-family\(^1\) for \( C \) is a family \( \sigma \) of subsets of \( \{0, 1\}^\infty \) such that:

1. Points of \( C \) are in \( \sigma \): \( \forall L \in C, \{L\} \in \sigma \),
2. The whole class \( C \) is not in \( \sigma \): \( C \not\in \sigma \),
3. A “suitable” union of elements of \( \sigma \) is in \( \sigma \) too,
4. A \( \subseteq B \) and \( B \in \sigma \Rightarrow A \in \sigma \).

Given a \( \sigma \)-family on a class \( C \), we define its two associated RBMs, \( \mu_{\sigma|\emptyset} \) and \( \mu_{\sigma} \), which are the two following partial functions:

\[
\begin{align*}
\mu_{\sigma|\emptyset} : & \quad \mathcal{P}(\{0, 1\}^\infty) \to \{0, 1\}, \\
A & \mapsto 0 \quad \text{if} \quad A \cap C \in \sigma, \\
A & \mapsto 1 \quad \text{if} \quad A \cap C \not\in \sigma.
\end{align*}
\]

\[
\begin{align*}
\mu_{\sigma} : & \quad \mathcal{P}(\{0, 1\}^\infty) \to \{0, 1\}, \\
A & \mapsto 0 \quad \text{if} \quad A \in \sigma, \\
A & \mapsto 1 \quad \text{if} \quad A \in \sigma.
\end{align*}
\]

One could argue that any reasonable definition of an RBM should imply that some intuitively small sets such as sparse languages, or “slices”,\(^3\) are of null measure. However, this is intentionally not included in the general definition of an RBM. The intuition behind this choice is the following: it is noticeable that different attempts to define RBMs 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 RBM captures such intuitively small sets, which could not be done with previous RBMs, but fails to capture such other intuitively small sets, whereas some previous RBMs could[…]”. As an alternative solution to obtain “reasonable” RBMs, we propose, in Definition 2.8, the introduction of a partial ordering relation is better on RBMs. A good RBM will then be one that is better than many other RBMs. Before going any further, let us show that \( \mu_{\sigma|\emptyset} \) and \( \mu_{\sigma} \) are well-defined partial functions.

**Claim.** \( \mu_{\sigma|\emptyset} \) and \( \mu_{\sigma} \) are well-defined partial functions.

We only substantiate the claim for \( \mu_{\sigma} \). The case of \( \mu_{\sigma|\emptyset} \) is identical. Suppose, that \( \mu_{\sigma} \) were not well defined; i.e., there exists \( A \subseteq C \) such that \( \mu_{\sigma}(A) = 0 \) and \( \mu_{\sigma}(A) = 1 \). By definition, this implies that \( A \in \sigma \) and \( A \not\in \sigma \). M3 then implies that \( A \cup \overline{A} \in \sigma \). M4 (and the fact that \( C \subseteq A \cup \overline{A} \)) then implies that \( C \in \sigma \), which is a contradiction to M2.

---

1 The Greek letter \( \sigma \) is chosen with the word “small” in mind.
2 The meaning of suitable in point 3 is informal, but it should definitely include finite unions.
3 The term “slice” is used informally. For example, the \( k \)th slice of \( P \) could be defined as \( \text{DTIME}(n^k) \).
Remark 2.2. For any non-empty class \( \mathcal{C} \subseteq \{0, 1\}^\infty \), \( \mu_{\sigma}\mid_{\mathcal{C}}(\mathcal{C}) = 1 \). This is so because \( \mu_{\sigma}\mid_{\mathcal{C}}(\emptyset) = 1 \) if \( \emptyset \in \sigma \). Now since \( \mathcal{C} \neq \emptyset \), there exists \( L \in \mathcal{C} \), and by M1, it holds that \( \emptyset \subseteq \{1\} \in \sigma \). This later fact and M4 imply that \( \emptyset \in \sigma \). In general, the set \( \mathcal{C} \) is not a measurable set for \( \mu_{\sigma} \); i.e., M2 implies that \( \mu_{\sigma}(\mathcal{C}) \neq 0 \), but it may be that \( \mu_{\sigma}(\mathcal{C}) \neq 1 \) too.

Remark 2.3. \( \mu_{\sigma}\mid_{\mathcal{C}} \) extends \( \mu_{\sigma} \); i.e., \( \mathcal{D}(\mu_{\sigma}) \subseteq \mathcal{D}(\mu_{\sigma}\mid_{\mathcal{C}}) \) and \( \mu_{\sigma}\mid_{\mathcal{C}} \) restricted to \( \mathcal{D}(\mu_{\sigma}) \) is equal to \( \mu_{\sigma} \).

With this remark, one may ask oneself what interest there is in defining both \( \mu_{\sigma}\mid_{\mathcal{C}} \) and \( \mu_{\sigma} \), since in many situations, it means that \( \mu_{\sigma}\mid_{\mathcal{C}} \) is better than \( \mu_{\sigma} \). Indeed, a typical use of an \( \mathcal{RBM} \) is to separate two classes, say \( A \) and \( B \), by showing that one of them is a big set, (i.e., \( B \) of measure 1), while the other one is a small set, (i.e., \( A \) of measure 0). Remark 2.3 implies that when this scheme works with \( \mu_{\sigma} \), it always works with the \( \mu_{\sigma}\mid_{\mathcal{C}} \) too, so \( \mu_{\sigma}\mid_{\mathcal{C}} \) may as well be used all the time. There are two obvious cases when \( \mu_{\sigma} \) may be preferred to \( \mu_{\sigma}\mid_{\mathcal{C}} \). The first case is similar to the previous one: if we want to separate two classes \( A \) and \( B \), it could be that \( \mu_{\sigma}\mid_{\mathcal{C}} \) is useless, if for example \( \mu_{\sigma}\mid_{\mathcal{C}}(A) = \mu_{\sigma}\mid_{\mathcal{C}}(B) \), but that \( \mu_{\sigma} \) is potentially useful, for example if it holds that \( \mu_{\sigma}(A) = 0 \) and that \( B \) is not in the domain of \( \mu_{\sigma} \), (remember that if \( \mu_{\sigma}(B) = 1 \), we may as well use \( \mu_{\sigma}\mid_{\mathcal{C}} \)). This use of \( \mu_{\sigma} \) is probably often not very realistic, since it implies proving that a set, (the set \( B \) in our case), is not measurable, (i.e., not in the domain of \( \mu_{\sigma} \)), which is usually difficult to prove. Another reason why \( \mu_{\sigma} \) may be preferred to \( \mu_{\sigma}\mid_{\mathcal{C}} \), is when the fact of being a small set can be given some interpretation; e.g., if the fact of being a small set implies some kind of similarity on its elements. In this case, showing that a set \( A \) is such that \( \mu_{\sigma}(A) = 0 \), (which implies that \( \mu_{\sigma}\mid_{\mathcal{C}}(A) = 0 \)), is a stronger result, that potentially implies a stronger similarity on the elements of the set being measured. Although this discussion shows that there is some interest in defining the two measures \( \mu_{\sigma} \) and \( \mu_{\sigma}\mid_{\mathcal{C}} \), it happens that when constructing an abstract \( \mathcal{RBM} \) for the class \( P \), the properties of the two measures \( \mu_{\sigma} \) and \( \mu_{\sigma}\mid_{\mathcal{C}} \) are identical, and proven similarly. Therefore, we restrict our discussion to only one of them: \( \mu_{\sigma}\mid_{\mathcal{C}} \), and make the following simplifying conventions.

Convention 2.4. From now on, the term “\( \mathcal{RBM} \)” is used as a synonym for “\( \mu_{\sigma}\mid_{\mathcal{C}} \).” We do not make any use of \( \mu_{\sigma} \) anymore, and therefore, we simplify notations by redefining \( \mu_{\sigma} \) as \( \mu_{\sigma} := \mu_{\sigma}\mid_{\mathcal{C}} \).

Definition 2.5. Let \( \mathcal{C} \subseteq \{0, 1\}^\infty \). A measuring system (\( \mathcal{M}\mathcal{S} \)) \( R \) for \( \mathcal{C} \) is \( \{R_i\}_{i \in \mathbb{N}} \), a family of subsets of \( \{0, 1\}^\infty \) such that

A1. \( R_i \supseteq R_j \) for \( j \geq i \),
A2. \( \bigcap_{i \in \mathbb{N}} R_i \cap \mathcal{C} = \emptyset \),
A3. \( \forall i \in \mathbb{N}, R_i \cap \mathcal{C} \neq \emptyset \).

\(^4\)Note that this approach is consistent with the prototype of an \( \mathcal{RBM} \): Lutz’s \( \mathcal{RBM} \), which, for example, at the level of \( E \), has the two forms \( \mu_P \) and \( \mu_{P\mid_{\mathcal{C}}} \).
The σ-family for C associated to R is denoted σ_R and is defined by \( \sigma_R := \{ X \subseteq \{0,1\} \mid \exists i \; X \cap R_i = \emptyset \} \).

In this definition, the implicit claim, which we prove in Lemma 2.7, that the family \( \sigma_R \) is a σ-family in the sense of Definition 2.1, exhibits a first relation between MSs and RBMs: any MS R, also defines a σ-family, called \( \sigma_R \), and thus also defines an RBM, which is \( \mu_{\sigma_R} \).

**Convention 2.6.** If R is an MS and \( \sigma_R \) is its associated C-family, we simply note \( \mu_R \) instead of \( \mu_{\sigma_R} \) for the RBM associated to \( \sigma_R \), and we call \( \mu_R \) the RBM associated with R.

Let us show that the claim that the family \( \sigma_R \) is a σ-family is consistent.

**Lemma 2.7.** The family \( \sigma_R \) of Definition 2.5 is a σ-family for C.

**Proof.** To prove this lemma, we have to show that the four points of Definition 2.1 hold.

- A2 \( \Rightarrow \forall L \in C \exists i \{ L \} \cap R_i = \emptyset \Rightarrow \{ L \} \in \sigma_R \), and thus M1 holds.
- A3 \( \Rightarrow C \notin \sigma_R \), and thus M2 holds.
- Let \( \{ A_i \}_{i \in S} \subseteq \mathbb{N} \) be a family of sets of \( \sigma_R \). To show that M3 holds, we have to show that if \( \bigcup_{i \in S} A_i \) is a “reasonable” union of members of \( \sigma_R \), then \( \bigcup_{i \in S} A_i \in \sigma_R \). Notice that since \( \{ A_i \}_{i \in S} \) is a family of members of \( \sigma_R \), it holds that \( \forall i \in S \exists j A_i \cap R_j = \emptyset \). We will choose that this union is “reasonable” if the condition above holds when we invert the universal and the existential quantifier; \( ^5 \) i.e., when it holds that \( \exists j \forall i \in S A_i \cap R_j = \emptyset \). With this choice made, it is easy to see that any “reasonable” union of members of \( \sigma_R \) is a member of \( \sigma_R \), and that finite unions of members of \( \sigma_R \) are always “reasonable” unions.
- The last point is easy, since \( B \in \sigma_R \Rightarrow B \cap R_i = \emptyset \) for some \( i \in \mathbb{N} \), and it thus trivially holds that if \( A \subseteq B \), then \( \exists i \; A \cap R_i = \emptyset \), and thus \( A \in \sigma_R \). \[ \square \]

The first use of the concept of MS is to permit to define the partial ordering relation is better on RBMs discussed earlier in this section.

**Definition 2.8.** Let R and \( \mu \) be respectively an MS and an RBM on a single fixed class C, then R is said to be an MS for \( \mu \) if \( \mu = \mu_R \). An RBM \( \mu_1 \) is better than an RBM \( \mu_2 \), which is denoted \( \mu_1 \prec \mu_2 \), if they both admit an MS and if \( \mu_1 \) extends \( \mu_2 \).

The idea behind the choice of comparing RBMs that admit an MS only, is that it is considered nice for an RBM to admit an MS, and therefore an RBM which

---

\( ^5 \) This choice is arbitrary, but it is fairly natural in the setting of MSs, since its interpretation is that all the elements of a “suitable” union have to be in a single “slice”, where a slice is the complement of an element of the MS \( R = \{ R_i \}_{i \in \mathbb{N}} \) being considered.

\( ^6 \) A partial function \( f \) extends a partial function \( g \) if \( D(g) \subseteq D(f) \) and \( f|_{D(g)} = g \).
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 $\mathcal{P}$, 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. The definitions of $\mathcal{MS}$s and $\mathcal{RBM}$s make the concept of $\mathcal{MS}$ a stronger one than that of $\mathcal{RBM}$, in 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-$\mathcal{MS}$, which is a structure satisfying some of the conditions required for an $\mathcal{MS}$, but not necessarily all of them, (cf. Definition 2.9). It can also be seen as a sufficient condition for a pre-$\mathcal{MS}$ to be an $\mathcal{MS}$.

Definition 2.9. If a family $R$ satisfies $A1$ only, it is called a pre-measuring system (pre-$\mathcal{MS}$).

Lemma 2.10. Let $\mathcal{C} \subseteq \{0, 1\}^{\infty}$. Let $R = \{R_k\}_{k \in \mathbb{N}}$ be a pre-$\mathcal{MS}$ and $\mu$ an $\mathcal{RBM}$ on $\mathcal{C}$. If $[\mu(A) = 0 \iff \exists k \in \mathbb{N} A \cap R_k \cap \mathcal{C} = \emptyset]$ then $[R$ is an $\mathcal{MS}$ for $\mathcal{C}$ and $\mu = \mu_R]$.\[0pt]

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 $A3$.

$\bullet$ To prove that $A2$ holds, suppose on the contrary that it does not. Then the following holds: $\exists L \in \bigcap_{i \in \mathbb{N}} R_i \cap \mathcal{C}$ $\Rightarrow$ $\exists L \in \mathcal{C} \forall i \in \mathbb{N} \{L\} \cap R_i \neq \emptyset \Rightarrow \exists L \in \mathcal{C} \{i \in \mathbb{N} \{L\} \cap R_i \cap \mathcal{C} = \emptyset$ hypothesis

$\Leftrightarrow$ $\exists L \in \mathcal{C} \mu(\{L\}) \neq 0$, which is a contradiction to M1.

$\bullet$ To show that $A3$ holds, suppose the contrary. Then there exists $i \in \mathbb{N}$ such that $R_i \cap \mathcal{C} = \emptyset$. With the hypothesis in the lemma, this is equivalent to $\mu(\mathcal{C}) = 0$, which is a contradiction to M2.

Since at this point $R$ is shown to be an $\mathcal{MS}$, one can consider its associated $\mathcal{RBM}$ $\mu_R$, and conclude using the following implication, which holds because of the hypothesis in the statement of the lemma and by definition of $\mu_R$: $[\mu(A) = 0 \iff \exists k A \cap R_k \cap \mathcal{C} = \emptyset]$

$\Rightarrow \mu = \mu_R$. \[0pt]

Before using the framework described in this section to define and discuss, in Section 4, the existence of random-based $\mathcal{RBM}$s, we devote the next section to a reminder to the reader of the main result of [19], which is the construction of an $\mathcal{RBM}$ for $\mathcal{P}$. This $\mathcal{RBM}$ will be analysed and compared to the definition of random-based $\mathcal{RBM}$ proposed.

### 3. A previous resource-bounded measure for $\mathcal{P}$

In this section, we summarise the construction of $\mu$, an $\mathcal{RBM}$ for $\mathcal{P}$ that emerged from the series of papers [1,2,19]. The main mathematical concept used is that of a
A betting strategy,\footnote{A betting strategy is a generalisation of a martingale, which is the type of function traditionally used in the context of Lutz’s \( \mathbb{RBM} \). The two concepts coincide at the level of Lutz’s \( \mathbb{RBM} \) in “big” complexity classes.} 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 \( \mu_\epsilon \) was given in [19] by introducing a topology, whereas this was done in [19] 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 and it then becomes easier to compare this \( \mathbb{RBM} \) to its potential related \( \mathbb{M} \)'s. Nevertheless, this definition is equivalent to that of [19].

**Definition 3.1.** A betting strategy is \( \beta : \{0,1\}^* \to \mathbb{R} \) such that the following holds:

1. The initial capital is equal to 1: \( \beta(\lambda) = 1 \), where \( \lambda \) is the empty word.
2. The game is fair: \( \forall \omega \in \{0,1\}^* \quad \beta(\omega 0) = - \beta(\omega 1) \), where \( \omega 0 \) is the concatenation of \( \omega \) and 0.
3. It is impossible to wager more than the total current capital: \( \forall \omega \in \{0,1\}^* \quad \sum_{x \subseteq \omega} \beta(x) \geq 0 \), where \( x \subseteq \omega \) means that \( x \) is a prefix of \( \omega \).

As its name suggests it, a betting strategy can be used to bet money when playing a particular game, called the casino game (cf. for example [5] 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 \( \beta \) be a betting strategy. The success set of \( \beta \), denoted \( S^\infty[\beta] \), is defined to be: \( S^\infty[\beta] := \{ L \in \{0,1\}^* \mid \limsup_{N \to \infty} \sum_{i=0}^{N} \beta(\chi_L[i]) = \infty \} \).

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 \( \mathbb{RBM} \) for \( \mathbb{P} \).

**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 \( V(G_{M,\omega}) \subseteq \{ \omega_0, \ldots, \omega_N \} \) and edges \( E(G_{M,\omega}) \) is called the graph of recursive queries of the algorithm \( M \) on input \( \omega \), 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 \( i \)th 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 \( j \)th bit of its input during its computation on input \( \omega_0 \cdots \omega_i \).

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 \( \omega \), 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 $\omega$ 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 $M$. Then, 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 $L$; cf. [19] for more details.

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

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 $E$; cf. [5] for more details. In order to be able to state the
definition of $\mu_\tau$, the $\mathcal{RBM}$ for $P$ defined in [19], 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
$L/x$, the quotient of $L$ by $x$, is defined to be $L/x := \{ y \in \{0,1\}^* | xy \in L \}$.

The following operation on languages, 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 $R_i$’s. This fact is used in [19] and will also be used in the next
section.

**Definition 3.6.** Let $\{L_i\}_{i \in \mathbb{N}}$ be a family of languages. $\bigotimes L_i$, the direct product of the
$L_i$’s, is defined by $\bigotimes_{i \in \mathbb{N}} L_i := \{ x10^i | x \in L_i \}$.

Notice that direct product and quotient are complementary operations, as suggested
by the following example: $\left( \bigotimes_{i \in \mathbb{N}} L_i \right) /10 = L_i$.

By using the definition of a quotient language, open balls and the associated topology
$\tau$ are defined.

**Definition 3.7.** Let $L \subseteq \{0,1\}^*$. The open ball $B_L$ centered on $L$ is defined to be
$B_L := \{ L/x | x \in \{0,1\}^* \}$. The topology $\tau$ is defined by $\tau := \{ O | L \in O \Rightarrow B_L \subseteq O \}$.
The proof of the fact that \( \mathcal{FS} \) 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 quotient subsequence \(^8\) 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 quotient subsequence of any language in \( A \). Next comes the definition of \( \mu_\tau \), and the theorem from [19], restated in our notations, which says that it is an \( \mathbb{RB.M} \).

**Definition 3.8.** Let \( \mu_\tau : \{0,1\}^\infty \rightarrow \{0,1\} \) be the following partial function: \( \forall A \subseteq \{0,1\}^\infty \), \( \mu_\tau(A) = 0 \) 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\(^9\) \( A \cap \mathcal{P} \subseteq \bigcup_{i \in \mathbb{N}} S^\infty[\beta_i] \), and \( \forall A \in \{0,1\}^\infty \), \( \mu_\tau(A) = 1 \) iff \( \mu_\tau(\overline{A}) = 0 \).

**Theorem 3.9 (Strauss).** \( \mu_\tau \) is well defined. The family \( \{A \subseteq \{0,1\}^\infty | \mu_\tau(A) = 0\} \) is a \( \sigma \)-family, and its associated \( \mathbb{RB.M} \) is \( \mu_\tau \).

In [19], some properties of this measure are demonstrated, such as the fact that some intuitively small sets are of null measure. It is shown that this approach also yields a measure for \( \text{PSPACE} \), and it is then compared to the measure for \( \text{PSPACE} \) of [18]. An alternative definition of \( \mu_\tau \) in terms of random sets was also proposed, but this definition is erroneous, as we prove in the next section.

### 4. A random-based resource-bounded measure for \( \mathbb{P} \)

In this section we revisit the problem of generalising Lutz’s \( \mathbb{RB.M} \) to small complexity classes, and more precisely, to the class of time efficient solvable problems: \( \mathbb{P} \). We give a definition of a random based \( \mathbb{RB.M} \) on \( \mathbb{P} \), which is based on the idea that a random based measure for \( \mathbb{P} \) is one that generalises Lutz’s \( \mathbb{RB.M} \). We also give a necessary and sufficient condition, in terms of random sets, for such a perfect measure to exist. The guideline followed in this section is the revisiting of \( \mu_\tau \), the \( \mathbb{RB.M} \) for \( \mathbb{P} \) from [19] 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

---

\(^8\)In this context, a quotient subsequence of a sequence \( \chi_L \) is a subsequence which is constructed by taking every \( N \)th word of \( \chi_L \), where \( N = 2^n + a \), for some \( n \in \mathbb{N} \) and \( 0 \leq a < 2^n \); as follows from Definitions 3.5 and 3.7.

\(^9\)For a set \( A \), the notation \( \overline{A} \) used hereafter denotes the interior (with respect to the topology \( \tau \)) of the set \( A \); i.e., \( \overline{A} := \bigcup_{O \in \tau \wedge \overline{O} \subseteq A} O \), which is the biggest open subset of \( A \).
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 $\mathbb{RBM}$ at the scale $P$, and define the associated pre-$\mathcal{MS}$ at the same time.

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

**Remark 4.2.** One may wonder why we restrict random sets to only languages of $P$, and do not define $R^P_k$ to be $\{L \in \{0,1\}^* \mid L$ is $n^k$-random$\}$. This alternate definition would have made sense, and is possibly more elegant: there is no obvious reason to restrict random sets to only $P$. The reason we do this is very practical: there is no technical or philosophical difference between the two approaches (all the proofs go through similarly), and the definition we have chosen has the advantage of simplifying notations: we do not have to take care of intersecting classes with $P$ all the time, as required by points A2 and A3 of Definition 2.5.

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 [19], which is the mistake that we correct later in this section.

**Claim (Erroneous).** $\mu(A) = 0$ 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 [19] 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 2.10 to obtain two easy consequences that would follow should the erroneous claim hold

- The first consequence is named $C_1$ and is the following: $R^P$ is an $\mathcal{MS}$ for $P$.
- The second is $C_2: \mu_{R^P} = \mu$. The following result of [6], restated in our notations, permits an interesting interpretation of the two previous statements.

**Lemma 4.3 (Lutz’s $\mathbb{RBM}$ is random based, Ambos-Spies et al. [6]).** Let $R^E_k = \{L \in E \mid$ there exists no $\Gamma(N^k)$ betting strategy covering $L\}$. Let $R^E = \{R^E_k\}_{k \in \mathbb{N}}$. Then $R^E$ is an $\mathcal{MS}$ for $E$ and $\mu_{R^E} = \mu_{p|E}$, where $\mu_{p|E}$ is Lutz’s $\mathbb{RBM}$ for $E$.

The main observation is that the pre-$\mathcal{MS}$ $R^P$ is a $P$ analogous of $R^E$ in $E$. Pushing further the idea behind this observation, and supposing that $C_1$ holds, Lemma 2.7 implies that $\sigma_{R^P}$ is a $\sigma$-family, and that $\mu_{R^P}$ is an $\mathbb{RBM}$ for $P$, which can thus be seen as a $P$ analogous of $\mu_{R^E}$, and thus, with the insight of Lemma 4.3, as an analogous of $\mu_{p|E}$. Adopting the terminology of calling random based a measure that is analogous to (or better then) Lutz’s $\mathbb{RBM}$, we define:
Definition 4.4 (Random-based RBMs). An RBM \( \mu \) for \( P \) is said to be random based if it admits \( R = \{ R_j \}_{j \in \mathbb{N}} \) an \( MS \) such that \( \forall k \in \mathbb{N} \) \( \exists j \in \mathbb{N} \) \( R_j \subseteq R_k^P \).

Notice that it is immediate that if there exists a random-based measure \( \mu \), then \( \mu_{ge} \) is a well-defined measure such that \( \mu \) is better than \( \mu_{ge} \). With this definition of random-based RBMs, it is easy to see that statements C1 and C2 imply that there exists a random-based RBM for \( P \) and \( \mu_t \) is a random-based RBM for \( P \), respectively. The following figure sums up the discussion pursued so far:

Erroneous claim.

\[ \text{lemma 2.10} \begin{cases} \text{C1 holds.} & \Rightarrow \text{There exists a random-based measure for } P. \\ \text{C2 holds.} & \Rightarrow \mu_t \text{ is a random-based measure for } P. \end{cases} \]

This sets the general context in which the following results are obtained. The first result is the fact that \( \mu_t \) admits an \( MS \), 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 \( \mu_t \) is not random-based, 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 \( \mu_t \)

Starting with the first point of the scheme given above, we show that \( \mu_t \) admits an \( MS \), consisting of a parametrised family of an alternative definition of random sets for \( P \).

Definition 4.5. Let \( L \) be a language. \( L \) is \( n^k-\tau \)-random if there is no \( \Gamma(\log(N)^k) \) betting strategy covering \( B_L \). Let \( R_{k,\tau}^P := \{ L \in P \mid L \text{ is an } n^k-\tau \text{-random} \} \). \( R_{\tau}^P \) is the following pre-\( MS \) for \( P \): \( R_{\tau}^P := \{ R_{k,\tau}^P \}_{k \in \mathbb{N}} \).

Lemma 4.6. Let \( A \subseteq \{0,1\}^\infty \), then \( \mu_t(A) = 0 \) iff \( \exists k \in \mathbb{N} \) such that \( A \cap R_{k,\tau}^P = \emptyset \).

Proof. Let us start with the direct implication. If \( A \subseteq \{0,1\}^\infty \) is such that \( \mu_t(A) = 0 \), then there exist \( k_1 \in \mathbb{N} \) and \( \{ \beta_{1i} \}_{i \in \mathbb{N}} \), a family of \( \Gamma(\log(N)^k) \) betting strategies, such that \( A \subseteq \bigcup_{i \in \mathbb{N}} S^\infty[\beta_i] \). Therefore, \( \forall L \in A, \exists \beta \ a \Gamma(\log(N)^k) \) betting strategy such that \( L \in S^\infty[\beta] \). Now if \( L \in S^\infty[\beta] \), since \( S^\infty[\beta] \in \tau \), it holds that \( B_L \subseteq S^\infty[\beta] \), and hence \( L \notin R_{k,\tau}^P \). Since this is true for any language \( L \in A \), it implies that \( A \cap R_{k,\tau}^P = \emptyset \), which proves the first implication.

Let us prove the reverse implication. Suppose that \( A \subseteq \{0,1\}^\ast \) is such that for some fixed integer \( k \), it holds that \( A \cap R_{k,\tau}^P = \emptyset \), then it holds that \( \forall L \in A \exists \beta \ a \Gamma(\log(N)^k) \) betting strategy such that \( B_L \subseteq S^\infty[\beta] \), which implies that \( \forall L \in A \exists \beta \ a \Gamma(\log(N)^k) \)
Corollary 4.7. The two following points hold. C’1: \( R'_P \) is an \( MS \) for \( P \). C’2: \( \mu_{R'_P} = \mu_{R} \).

The last corollary is obtained using Lemmas 2.10 and 4.6 in conjunction. The open problem discussed earlier in this section, which we called statement C1, asking whether \( R_P \) is an \( MS \), which implies\(^{10}\) that there exists a random-based measure for \( P \), is very close to statement C’1. Since we managed to prove that C’1 holds; i.e., that \( R'_P \) is an \( MS \), it is natural to hope enthusiastically to prove, using the same techniques, that \( R_P \) is an \( MS \), and show the existence of a random-based \( RBM \) for \( P \) 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 4.6. Thus proving that C1 holds, adapting the proof that C’1 does, would require an analogue of Lemma 4.6, with the family \( R'_P \) replaced by the family \( R_P \): but this is precisely the erroneous claim, and as we are going to prove in Section 4.3, the erroneous claim does not hold. Therefore the problem of proving or disproving C1; i.e., whether there exists a random-based measure for \( P \), remains open. Now that we have a characterisation of \( \mu_{R} \) in terms of \( RBM \)s, let us turn to the analysis of the plausibility of the existence of random-based measures.

4.2. Conditional existence of random-based measures

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

Lemma 4.8. There exists a random-based \( RBM \) iff the \( pre-MS \) \( R_P \) is also an \( MS \) for \( P \).

Proof. We only prove the direct implication, since the reverse implication is easy, and therefore left to the reader. Since \( R_P \) is a \( pre-MS \), we only need to show that the assumptions imply that \( R_P \) satisfies points A2 and A3 of Definition 2.5. Let us start with A2, which can be proved to hold unconditionally. We need to prove that \( \bigcap_{k \in \mathbb{N}} R^P_k \neq \emptyset \). It is easy to see from the definitions of \( R^P_k \) and \( R_P \) that it holds that \( R^P_k \subseteq R^P_{k+1} \) for any \( k \in \mathbb{N} \). Now since Corollary 4.7 insures that \( R'_P \) is an \( MS \), it holds that \( \bigcap_{i \in \mathbb{N}} R^P_{i+1} = \emptyset \), and thus A2 follows. We now prove A3, that is the fact that \( R^P_{i+1} \neq \emptyset \) for any \( i \in \mathbb{N} \), using the assumption that there exists a random-based \( RBM \). By definition of the existence of a random-based measure, there exists \( R = \{ R_i \}_{i \in \mathbb{N}} \) an \( MS \) such that \( \forall k \in \mathbb{N} \exists i \in \mathbb{N} \) such that \( R_i \subseteq R^P_k \). Since \( R \) is an \( MS \), \( \forall i R_i \neq \emptyset \), and thus \( \forall k R^P_k \neq \emptyset \). \( \square \)

\(^{10}\) In fact, as shown in Lemma 4.8, not only does this condition imply, but it is even equivalent to the existence of a random-based measure.
Corollary 4.9. There exists a random-based $\mathbb{RBM}$ if and only if there are random sets; i.e., if $R_i^p \neq \emptyset$ for all $i$.

Next comes the discussion of another condition, sufficient for the existence of a random-based $\mathbb{RBM}$. One of the main technical difficulties in defining an $\mathbb{RBM}$ for small complexity classes comes from the fact that it cannot be proved that the following assertion (or a variation of it) holds:

Definition 4.10. We call the following assertion the unique betting strategy hypothesis:
\[
\forall k \in \mathbb{N} \quad \forall \{b_i\}_{i \in \mathbb{N}} \quad \exists k' \in \mathbb{N} \quad \exists \beta \quad \text{a } \Gamma(n^k) \text{ betting strategy such that } \bigcup_{i \in \mathbb{N}} S^\infty[b_i] \subseteq S^\infty[\beta'].
\]

The fact that this hypothesis cannot be shown to hold (nor its negation) is the main difference with $\mathbb{RBM}$ at the level of $E$, where the equivalent assertion is true indeed. It is easy to see that if this condition were to hold, the function $\mu_L$ from the next definition, (which is in some sense a natural transposition of Lutz’s $\mathbb{RBM}$ on $E$), would define an $\mathbb{RBM}$ on $P$.

Definition 4.11. If the unique betting strategy holds, we define the following partial function: $\mu_L : \mathcal{P}(P) \rightarrow \{0, 1\}$, where $\mu_L(A) = 0$ if $\exists k' \exists \beta \text{ a } \Gamma(n^k) \text{ betting strategy such that } A \cap P \subseteq S^\infty[\beta]$, and $\mu_L(A) = 1$ if $\mu_L(\overline{A}) = 0$.

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 than 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 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 random-based measure does indeed capture the essence of a good generalisation to $P$ of Lutz’s $\mathbb{RBM}$.

Lemma 4.12. If the unique betting strategy hypothesis holds, then there exist random sets. Furthermore, in this configuration, $\mu_{\mathbb{R}} = \mu_L$.

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 $L \in P$ such that $L \notin \bigcup_{\beta \in \Gamma(n^k) \text{ betting strategies}} S^\infty[\beta]$. By hypothesis, there exists $k'$ and $\gamma$ a $\Gamma(n^{k'})$ betting strategy such that $\bigcup_{\beta \in \Gamma(n^k) \text{ betting strategies}} S^\infty[\beta] \subseteq S^\infty[\gamma]$. Since the definition of $\Gamma$ betting strategies was given in order to enable the construction of a language $L \in P$...
that diagonalises against a single betting strategy, it is easy to construct a language of $P$ which is not in $S^\infty_\gamma$, and thus not in $\bigcup_{\beta \in \{\Gamma(n^k)\} \text{ betting strategies}} S^\infty[\beta]$ 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, $\mu_L = \mu^{R^e}$, it only needs to be shown that for any $A \subseteq P$, $\mu_L(A) = 0$ iff $\mu^{R^e}(A) = 0$. Suppose that $\mu_L(A) = 0$, then there exists $k \in \mathbb{N}$ and $\gamma$ a $\Gamma(n^k)$ betting strategy, such that $A \subseteq S^\infty[\gamma]$. Thus $A \cap \{n^k\text{-random}\} = \emptyset$, and by definition $\mu^{R^e}(A) = 0$. On the other hand, suppose that $A \subseteq P$ is such that $\mu^{R^e}(A) = 0$. Therefore there exists $k$ such that $A \cap \{n^k\text{-random}\} = \emptyset$. Thus $A \subseteq \bigcup_{\beta \in \{\Gamma(n^k)\} \text{ betting strategies}} S^\infty[\beta]$. By hypothesis, there exists $k'$ and $\gamma$ a $\Gamma(n^{k'})$ betting strategy such that $A \subseteq S^\infty[\gamma]$, and thus $\mu_L(A) = 0$. 

In [19], as well as in this article, it is ensured that no “good” betting strategy covers the whole space $P$, thanks to the second condition 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 $\text{DTIME}(n^{(2k+1)})$; cf., [19] for more details. This restriction imposed on 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 $\beta$, there has to exist a language $L$ in $\text{DTIME}(n^{f(k)})$ such that $L \notin S^\infty[\beta]$, where $f$ is some arbitrary computable function. It would enable the definition of measures $\mu_\gamma$ “à la Strauss”, generalising $\mu$, 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 [19]. 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 implicit claim to have defined a somehow general downwards translation to $P$ of Lutz’s $\mathbb{RB.M}$. This unpleasant problem can be solved by the following remark.

**Remark 4.13.** If one replaces the second condition of Definition 3.4 by the following: a $\Gamma(n^k)$ betting strategy $\beta$ must not cover the whole of $P$, then all the proofs of this subsection go unchanged.

The definition of a random-based measure thus obtained has the advantage of being free of any arbitrary choice. The most pleasant case would be if, as in the case of Lutz’s $\mathbb{RB.M}$, the condition a $\Gamma(n^k)$ betting strategy $\beta$ must not cover the whole of $P$ is in fact void.

**Remark 4.14.** In [1], a generalisation for $P$ of Lutz’s $\mathbb{RB.M}$ was defined. The approach was somehow different to that taken in this paper and in the following [2,19], in the sense that it was defined by somehow forcing the unique betting strategy to hold, by defining small sets to be only those that are covered by a single betting strategy. The difficulty is then to ensure that easy unions of null sets are null sets too, and this is strongly dependent on the exact condition imposed to ensure that a single betting
strategy does not cover the whole space. This approach is equivalent to that we take in this article, if the unique betting strategy holds. Otherwise, it yields a weaker measure, since less sets are measurable. The interested reader is referred to [1] for more details on this approach to generalising Lutz’s R.R. to P.

4.3. Previous relations between $\mu_i$ and randomness

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

Lemma 4.15. $\exists \mathcal{A} \subseteq P \; \exists k \in \mathbb{N}$ such that $\mathcal{A} \cap R^0_k = \emptyset$ but $\mu_i(\mathcal{A}) \neq 0$.

Proof. Suppose on the contrary that the lemma is false, then the following implication holds: $\forall \mathcal{A} \subseteq P \; \forall k \in \mathbb{N} \; [\mathcal{A} \cap R^0_k = \emptyset \Rightarrow \mu_i(\mathcal{A}) = 0]$. We use this absurd hypothesis twice: at the end of the proof to obtain a contradiction, and just below, to deduce from it the existence of a particular family $\{L_i\}_{i \in \mathbb{N}}$ of random languages.

- If $\exists K \in \mathbb{N}$ such that $\forall k \geq K \; R^0_k = \emptyset$, then the absurd hypothesis implies that $\mu_i(P) = 0$.
  This is a contradiction to Theorem 3.9, which states that $\mu_i$ satisfies M2, and thus $\mu_i(P) \neq 0$.
- Thus, using the absurd hypothesis above, we can suppose (wlog) that $\forall k \in \mathbb{N}, \; R^0_k \neq \emptyset$.
  Using this latter fact, we let $\{L_i\}_{i \in \mathbb{N}}$ be a family of languages such that $L_i \in R^0_k$, and define $\mathcal{A} := \bigcup_{i \in \mathbb{N}} L_i$, where $L_i := \{x0 \mid x \in L_i\}$. Now we need the following claim, for which we also give a short idea of the demonstration.

Claim. The following holds:
1. $\mathcal{A} \subseteq P$.
2. $\exists k \in \mathbb{N}$ such that $\mathcal{A} \cap R^0_k = \emptyset$.
3. $\mu_i(\mathcal{A}) \neq 0$.

Let us prove each point separately.
1. It is sufficient to show that $\forall i \in \mathbb{N} \; L_i \in P$. But this is an easy consequence of the fact that $\forall i \in \mathbb{N} \; L_i \in P$ since by hypothesis $L_i \in R^0_k \subseteq P$.
2. This point holds because it is easy to construct a $\Gamma(\log(N))$ betting strategy that covers $\mathcal{A}$, taking advantage of the fact that the elements of $\mathcal{A}$ are very predictable, in the sense that every language $L \in \mathcal{A}$ has the property that every word $x$ whose rightmost bit is a 1 does not belong to $L$.
3. To show that this point holds, suppose on the contrary that $\mu_i(\mathcal{A}) = 0$. 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 $\mathcal{A} \subseteq \bigcup_{i \in \mathbb{N}} S^\infty_0[\beta_i]$. This implies that $\forall j \in \mathbb{N} \; \exists i \in \mathbb{N}$ such that $\tilde{L}_j \in S^\infty_0[\beta_i]$. Now observe $\tilde{L}_j \in S^\infty_0[\beta_i] \Rightarrow B_{\tilde{L}_j} \subseteq S^\infty_0[\beta_i] \Rightarrow \forall i \; L_j \in S^\infty_0[\beta_i] \Rightarrow L_j \not\subseteq R^0_k$, where the last implication holds since, for all $i \in \mathbb{N}$, $\beta_i$ is, by assumption a $\Gamma(\log(N))^k$ betting strategy. We have thus obtained a contradiction, since $\{L_j\}_{j \in \mathbb{N}}$ is a family of languages such that $L_j \in R^0_k \subseteq R^0_k$ if $j \geq k$, and $R^0_k \subseteq R^0_k$ trivially.
The three claims above give rise to the following contradiction: the first two claims show that the set $A$ (constructed using the absurd hypothesis that the lemma does not hold) satisfies $A \subseteq \mathbb{P} \cap \{0, 1\}^\infty$, which implies, using the absurd hypothesis at the beginning of the proof, that $\mu_r(A) = 0$, which is a contradiction to the third claim.

This technical lemma enables one to compare $\mu_r$ and $\mu_{\text{ref}}$ in terms of the partial ordering relation “is better than” defined in Section 2.

**Lemma 4.16.** If $R^p$ is an $\mathcal{M}$, then $\mu_{\text{ref}}$ is strictly better than $\mu_r$.

**Proof.** Suppose that $R^p$ is an $\mathcal{M}$. Thus the function $\mu_{\text{ref}}$ is defined, and is an $\mathcal{RBM}$. Now we need to prove the two following facts: $\mu_{\text{ref}} \prec \mu_r$ and $\mu_r \not\prec \mu_{\text{ref}}$. 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 $\mathcal{M}$ and that $\mu_{\text{ref}}$ extends $\mu_r$. The fact that $\mu_{\text{ref}}$ admits an $\mathcal{M}$ is trivial, and $\mu_r$ admits an $\mathcal{M}$ too, as follows from Corollary 4.7. The assertion that $\mu_{\text{ref}}$ extends $\mu_r$ is substantiated by showing that for any $A \subseteq \mathbb{P}$, if $A$ is $\mu_r$-measurable, then $A$ is $\mu_{\text{ref}}$-measurable, and $\mu_r(A) = \mu_{\text{ref}}(A)$: first suppose that $\mu_r$ is defined on $A$ and that $\mu_r(A) = 0$. Together with Lemma 4.6, it implies that $\exists k \in \mathbb{N}$ such that $A \cap R^p_k = \emptyset$. Now since by definition of $R^p$ and $R^r_k$, it holds that $\forall k \in \mathbb{N}$ $R^p_k \subseteq R^r_k$, we also have that $\exists k \in \mathbb{N}$ such that $A \cap R^r_k = \emptyset$. Now using the hypothesis that $R^p$ is an $\mathcal{M}$ and Definition 2.5, the last equation implies in turn that $A$ is $\mu_{\text{ref}}$ measurable and that $\mu_{\text{ref}}(A) = 0$. A similar proof holds if one starts with the case where $A$ is $\mu_r$-measurable with $\mu_r(A) = 1$, and thus $\mu_{\text{ref}}$ extends $\mu_r$. This also finishes the proof that $\mu_{\text{ref}} \prec \mu_r$.

We now turn to proving that $\mu_r \not\prec \mu_{\text{ref}}$. Suppose on the contrary that $\mu_r \prec \mu_{\text{ref}}$. If this were so, then we would have the following implications: $\mu_r \prec \mu_{\text{ref}} \Rightarrow [\mu_{\text{ref}}(A) = 0 \Rightarrow \exists k \in \mathbb{N} \ A \cap R^p_k = \emptyset \Rightarrow \mu_r(A) = 0]$. But the last implication is a contradiction to Lemma 4.15, thus the absurd hypothesis that $\mu_r \prec \mu_{\text{ref}}$ is false.

The next corollary follows from the easy claim that if a measure $\mu$ is random-based, then necessarily $\mu \prec \mu_{\text{ref}}$. Together with Corollary 4.6, it makes a correction to the erroneous claim.

**Corollary 4.17.** $\mu_r$ is not a random-based measure, $C2$ does not hold and the erroneous claim does not hold.

## 5. Conclusion

The quest for a generalisation of Lutz’s $\mathcal{RBM}$ to small complexity classes is a difficult one. Success in it would probably enable many results obtained via Lutz’s $\mathcal{RBM}$ to be translated downwards to small complexity classes. The main contribution of this paper is to have proposed a definition of a random based $\mathcal{RBM}$ in small complexity classes, which reproduces, at the level of $\mathbb{P}$, some important properties of Lutz’s $\mathcal{RBM}$ for $E$:
• Both measures have a similar relation to random sets.
• In Lemma 4.12, we show that the unique betting strategy hypothesis, which holds in the context of Lutz’s RBM, is stronger than the hypothesis of the existence of random sets, but that, surprisingly, it yields the same notion of measure.

The question of whether a random-based RBM exists, which is central to this line of research, is unanswered, but we clearly identify the following open problem on the family \( \{R_i\}_{i \in \mathbb{N}} \) from Definition 4.1, which is a necessary and sufficient condition for the existence of a random-based RBM: Is it true that \( \forall i \in \mathbb{N}, R_i \neq \emptyset \)?

Another open question, that follows from Lemma 4.12, is whether the unique betting strategy hypothesis, which implies the existence of random sets, is in fact equivalent to it: Does the existence of random sets imply that the unique betting strategy holds?

We consider Lemma 4.12 as evidence that random based measures are a good generalisation to P of Lutz’s RBM, which could exist even if the unique betting strategy hypothesis were not to hold; thus, answering the last open question above would be interesting, whether answered positively or not.

The final contribution of this paper is to have revisited \( \mu_c \), the measure for P that was developed in [19], and to have corrected a mistake concerning the relation of this measure to random sets, which, in light of Lemma 4.8, has implications about the existence of a random based RBM, and to propose, in Lemma 4.6, an alternative description of \( \mu_c \) in terms of a special kind of random sets.

References