On Resource-bounded versions of the van Lambalgen theorem*

Diptarka Chakraborty[†‡1], Satyadev Nandakumar[§¶2], and Himanshu Shukla[‖3]

[1]Computer Science Institute of Charles University, Malostranské námesti 25, 118 00 Praha 1, Czech Republic

[2,3]Department of Computer Science and Engineering, Indian Institute of Technology Kanpur, Kanpur, Uttar Pradesh, India.

November 30, 2017

Abstract

The van Lambalgen theorem is a surprising result in algorithmic information theory concerning the symmetry of relative randomness. It establishes that for any pair of infinite sequences A and B, B is Martin-Löf random and A is Martin-Löf random relative to B if and only if the interleaved sequence $A \uplus B$ is Martin-Löf random. This implies that A is random relative to B if and only if B is random relative to A [vL87], [Nie09], [DH06]. This paper studies the validity of this phenomenon for different notions of time-bounded relative randomness.

We prove the classical van Lambalgen theorem using martingales and Kolmogorov compressibility. We establish the failure of relative randomness in these settings, for both time-bounded martingales and time-bounded Kolmogorov complexity. We adapt our classical proofs when applicable to the time-bounded setting, and construct counterexamples when they fail. The mode of failure of the theorem may depend on the notion of time-bounded randomness.

1 Introduction

In this paper, we explore the resource-bounded versions of van Lambalgen's theorem in algorithmic information theory. van Lambalgen's theorem deals with the symmetry of relative randomness. The theorem states that an infinite binary sequence B is Martin-Löf random and a sequence A is Martin-Löf random relative to B if and only if the interleaved sequence $A_0B_0A_1B_1\dots$ is Martin-Löf random [vL87]. It follows that A is Martin-Löf random relative to B if and only if B is Martin-Löf random relative to A.

This result is quite surprising, since it connects the randomness of A with the computational power A possesses [Nie09], [DH06]. This contrasts with relative computability - for instance, every computably enumerable language is computable given the halting problem as an oracle, but the halting problem is not computable given an arbitrary c.e. language. Symmetry of relative randomness is desirable for any robust notion of randomness. However, we now know that it fails in several other settings - both Schnorr randomness and computable randomness exhibit a lack of symmetry of relative randomness [Yu07], [Bau15].

*A preliminary version of this paper [CNS17] was accepted in the 14th Annual Conference on Theory and Applications of Models of Computation (TAMC), 2017, April 20-22, 2017, Bern, Switzerland

†diptarka@iuuk.mff.cuni.cz

‡The author was supported by the European Research Council under the European Union's Seventh Framework Programme (FP/2007-2013)/ERC Grant Agreement no. 616787.

§satyadev@cse.iitk.ac.in

¶The author was supported by SR/FTP/ETA-249/2013 of Department of Science and Technology, Government of India.

‖hshukla.math04@gmail.com

We explore whether this symmetry holds when Martin-Löf randomness is replaced with time-bounded randomness. Considering the failure of the analogies of the van Lambalgen's theorem in many settings, it is natural to guess that such a resource-bounded version of van Lambalgen's theorem is false. Indeed, the existence of *one-way functions* [Gol01] from strings to strings which are easy to compute but hard to invert, can be expected to have some bearing to the validity of the resource-bounded van Lambalgen's theorem. In the context of polynomial-time compressibility, Longpré and Watanabe [LW95] establish the connection between polynomial-time symmetry of information and the existence of one-way functions, and analogously, Lee and Romaschenko [LR05] establish the connection for CD complexity [LV08].

Modern proofs of van Lambalgen's theorem proceed by defining Solovay tests (see [DH06], [Nie09]). The notion of a resource-bounded Solovay test has not been studied, while the notion of resource-bounded martingales [Lut98] and resource-bounded Kolmogorov complexity have been studied extensively (see Allender et. al. [ABK$^+$06]). We approach the classical van Lambalgen's theorem using prefix-free incompressibility and martingales, inspired by the Solovay tests. This part may be of independent interest. We then attempt to adapt these proofs to resource-bounded settings.

Our main results are the following. Let t be a superlinear time bound, and t^X denote t-computable functions with oracle access to the sequence X. Let $A \uplus B$ denotes the interleaving of A and B.

1. Using the notion of t-bounded martingales, we show that there are t-nonrandom $A \uplus B$ where B is t-random and A is t^B-random. This result is unconditional, and analogous to the result of Yu [Yu07].
2. (a) There are t-random sequences A and B where A is t^B-nonrandom, but B is t^A-random. However for this pair, $A \uplus B$ is still t-nonrandom. Thus the randomness of the interleaved sequence and mutual relative randomness of the pair are distinct notions for time-bounded martingales.
   (b) We establish a sufficient condition under which a t-random B and a t^B-nonrandom A could still create t-random $A \uplus B$. This involves a non-invertibility condition reminiscent of one-way functions.
3. There are t-compressible $A \uplus B$ such that B is t-incompressible and A is t-incompressible relative to B. This is an unconditional result analogous to 1.
4. If B is t-compressible or A is t-compressible with respect to B, then $A \uplus B$ is t-compressible. This is in contrast to 2.

Thus van Lambalgen's theorem fails in resource-bounded settings. Surprisingly, the manner of failure may depend on the formalism we choose.

The results in the paper also provide indirect evidence that resource-bounded randomness may vary depending on the formalism. In particular, the set of sequences over which resource-bounded martingales fail may not be the same as the set of resource-bounded incompressible sequences. The results in 2 and 4 provide us a conditional separation between these two formalisms in case of resource-bounded settings.

The manner of failure in 2 has to do with the oracle access mechanism, and the proof hinges on a technical obstacle which may be tangential to time-bounded computation. In the final section of the paper, we propose a modified definition which we call t-bounded "lookahead" martingales with which we are able to show that if B is t-lookahead-nonrandom or A is t-lookahead-nonrandom relative to B, then $A \uplus B$ is t-lookahead nonrandom. Here, the van Lambalgen property for t-lookahead martingales fails in precisely the same manner as t-incompressibility. This may be a reasonable model to study resource-bounded martingales.

2 Preliminaries

We assume familiarity with the basic notions of algorithmic randomness at the level of the initial chapters in Downey and Hirschfeldt [DH06] or Nies [Nie09].

We use the notation $\mathbb{N}$ for the set of natural numbers, $\mathbb{Q}$ for rationals, and $\mathbb{R}$ for reals. We work with the binary alphabet $\Sigma = \{0, 1\}$. We denote the set of finite binary strings as Σ^* and the set of infinite binary sequences as Σ^∞. Finite binary strings will be denoted by lower-case Greek letters like σ, ρ etc. and infinite sequences by upper-case Latin symbols like X, Y etc. The length of a string σ is denoted by $|\sigma|$. The letter λ stands for the empty string. For finite strings σ and ρ and any infinite sequence X, $\sigma \preceq \rho$ and $\sigma \preceq X$ denote that σ is a prefix of ρ and X respectively.

The substring of length n starting from the m^{th} position of a finite string σ or an infinite sequence X is denoted by $\sigma[m \ldots m+n-1]$ and $X[m \ldots m+n-1]$, where $m+n-1 < |\sigma|$. When m is 0, *i.e.* the first position, we abbreviate the notation as $\sigma \upharpoonright n$ and $X \upharpoonright n$ - e.g. $\sigma \upharpoonright n$ is $\sigma[0 \ldots n-1]$.

The concatenation of σ and τ is written usually as $\sigma\tau$. Where we need to indicate a concatenation of three strings or more, or where there may be a confusion otherwise, we indicate concatenation explicitly using the $\circ$ symbol. For example, the concatenation of σ, τ and β is denoted $\sigma \circ \tau \circ \beta$. The notation $A \uplus B$ stands for the sequence we get by interleaving the bits in A with the bits in B, *i.e.* $A_0 B_0 A_1 B_1 \ldots$.[1]

A set of finite strings S is said to be *prefix-free* if no string in S can be a proper prefix of another string in S.

Theorem 1. *(van Lambalgen, 1987) [vL87] For any two infinite sequences A and B, B is Martin-Löf random and A is Martin-Löf random relative to B if and only if $A \uplus B$ is Martin-Löf random.*

Note that we can define Martin-Löf randomness either using the notion of incompressibility or using martingales. We provide the proof of the above theorem for both the alternatives.

3 A Proof using Incompressibility

We now prove Theorem 1 via incompressibility notions. Throughout the remainder of the paper, we fix a canonical set of prefix-free codes for partial computable functions by $\mathcal{P}$.

Definition 1. *The* self-delimiting Kolmogorov complexity *of $\sigma \in \Sigma^*$ is defined by $K(\sigma) = \min\{|\pi| \mid \pi \in \mathcal{P}$ outputs $\sigma\}$.*

Similarly, the conditional Kolmogorov complexity *of $\sigma \in \Sigma^*$ given $\tau \in \Sigma^*$ is defined by $K(\sigma \mid \tau) = \min\{|\pi| \mid \pi \in \mathcal{P}$ outputs σ on input $\tau\}$.*

Using the notion of incompressibility, it is well-known that we can formulate an equivalent definition of random sequences [Nie09].

Definition 2. *An infinite binary sequence A is said to be* incompressible *if $\exists c \quad \forall n \quad K(A \upharpoonright n) \geq n - c$. The sequence A is* incompressible with respect to *another binary sequence B (or B-incompressible) if $\exists c \quad \forall n \quad \forall m \quad K(A \upharpoonright n \mid B \upharpoonright m) \geq n - c$.*

The set of Martin-Löf random sequences are precisely the set of incompressible sequences. Relativizing the same result, the set of Martin-Löf random sequences relative to a sequence B is precisely the set of sequences incompressible with respect to B.

We now prove van Lambalgen's theorem using incompressibility. When we consider the issue of resource-bounded van Lambalgen's theorems, we try to either adapt these proofs where applicable, or examine the issues which prevent such an adaptation. We prove the two directions of the van Lambalgen's theorem separately so as to emphasize the issues which arise in the resource-bounded setting.

The proof of the first direction relies on a form of Symmetry of Information, a result first established by Levin and Gács [LV08]. To this end, we mention basic results from the theory of self-delimiting (prefix-free) Kolmogorov complexity.

Definition 3 ([Nie09])**.** *A computably enumerable set $L \subseteq \Sigma^* \times \mathbb{N}$ is said to be a* bounded request set *if $\sum_{(\sigma,n) \in L} \frac{1}{2^n} \leq 1$.*

We may view each element (w, n) as a request to encode w using at most n bits. The boundedness condition is a promise that the requested code lengths satisfy the Kraft inequality. The Machine Existence Theorem states that there is some prefix-free code which can satisfy all requests in a bounded request set.

[1] It is also common to use $\oplus$, but we want to avoid confusion with the bitwise xor operation.

Theorem 2. *(Machine Existence Theorem)[Nie09] Let L be a bounded request set. Then there is a prefix-free set of codes $\mathcal{P}$ which, for each $(y, m) \in L$, allocates a prefix-free code $\tau \in \Sigma^m \cap \mathcal{P}$ for y.*

The coding theorem relates the algorithmic probability of a string to its prefix-free Kolmogorov Complexity. We state it here in the form applicable to pairs of strings, but an analogous result holds for strings.

Theorem 3. *(Coding Theorem)[Nie09] Let τ be a finite string. Let $\mathcal{P}$ be a prefix-free encoding of partial-computable functions outputting pairs of strings. Denote $\mathcal{P}_\tau \subseteq \mathcal{P}$ as the set of prefix-free codes which output pairs (σ, τ) for some arbitrary string σ. Then there is a constant c such that*

$$2^{c-K(\sigma,\tau)} > \sum_{\rho \in \mathcal{P} \text{ outputting } (\sigma,\tau)} 2^{-|\rho|}$$

Using these, we now state and prove the variant of "Symmetry of Information" which we use to establish Lemma 3.2.

Lemma 3.1. *Let σ be a finite string with $K(\sigma) > |\sigma| + c$, and τ be a finite string. Then $|\sigma| + K(\tau|\sigma) \leq K(\sigma, \tau) + O(1)$.*

Proof. Let p_i be an arbitrary program in the computable enumeration of $\mathcal{P}$, the set of programs which output string pairs. Consider the program R_{p_i} which can be generated from p_i, defined by the following algorithm.
1. Input σ.
2. Let $U(p_i)$ output the string pair (α, τ).
3. If α is equal to σ, then we output $(\tau, |p_i| - |\sigma| + c)$, where c satisfies the inequality below.

Corresponding to the computable enumeration p_1, p_2, ... of $\mathcal{P}$, we obtain a computable enumeration R_{p_1}, R_{p_2}, ... We now show that this forms a valid enumeration of a *bounded request set* (see Definition 3).

Let N_σ be the set of indices $i \in \mathcal{P}$ where $U(p_i)$ outputs a pair of strings of the form (σ, τ) for some τ. First, we have

$$\sum_{i \in N_\sigma} \frac{1}{2^{|p_i|-|\sigma|+c}} < 2^{|\sigma|-c} \sum_{i \in N_\sigma} \frac{1}{2^{|p_i|}} < 2^{|\sigma|-c+c'} \sum_{\tau \in \Sigma^*} \frac{1}{2^{K(\sigma,\tau)}} = \frac{2^{|\sigma|-c+c'}}{2^{K(\sigma)}} < 1,$$

where the second inequality follows from the Coding Theorem (see, for example, Nies [Nie09], Theorem 2.2.25), and the last inequality follows from the assumption.

Hence R_{p_1}, R_{p_2}, ... is a computable enumeration of a bounded request set. By the Machine existence theorem for prefix-free encoding (see for example, [Nie09] Theorem 2.2.17), it follows that for any request $(\tau, |p_i| - |\sigma| + c)$, there is a prefix-free encoding of τ given σ which has length $|p_i| - |\sigma| + c$. Now, consider a shortest prefix-free code p_i for (σ, τ). We have that $|p_i| = K(\sigma, \tau)$. Hence $K(\tau \mid \sigma) \leq K(\sigma, \tau) - |\sigma| + O(1)$. $\square$

We would like to mention that the above lemma can also be established as a corollary of Theorem 3.9.1 of [LV08].

Lemma 3.2. *If B is incompressible and A is B-incompressible, then $A \uplus B$ is incompressible.*

Proof. Suppose that for every n, $K(B \upharpoonright n) \geq n - c$ and for all m, $K(A \upharpoonright n \mid B \upharpoonright m) \geq n - c'$. This implies that $K(A \upharpoonright n \mid B \upharpoonright (n-1)) \geq n - c'$. By the version of the Symmetry of information in Lemma 3.1, we have

$$(2n-1) - c' \quad \leq \quad (n-1) + K(A \upharpoonright n \mid B \upharpoonright (n-1)) \quad \leq \quad K((A \uplus B) \upharpoonright (2n-1)) + O(1).$$

A similar argument works for $K((A \uplus B) \upharpoonright 2n)$. This completes the proof. $\square$

The above proof relied on symmetry of information of prefix-free Kolmogorov Complexity. Since reasonable complexity-theoretic hypotheses imply that this fails in resource-bounded settings, we can foresee that this direction fails in resource-bounded settings, as we show in section 5.

Since the first direction was a consequence of Symmetry of Information, it is reasonable to expect the converse direction to follow from the subadditivity of K: $K((A \uplus B) \upharpoonright 2n) \quad \leq \quad K(B \upharpoonright n) + K(A \upharpoonright n \mid B \upharpoonright$

$n) + O(1)$. However, this runs into the following obstacle. If the prefix of B is compressible with complexity, say $n - \log(K(n))$, and the prefix of A is B-incompressible with conditional complexity $n + K(n)$, then we cannot conclude from subadditivity that $K((A \uplus B) \upharpoonright 2n)$ is less than $2n$. Thus concatenating the shortest prefix-codes for $B \upharpoonright n$ and $A \upharpoonright n$ given $B \upharpoonright n$ to obtain a prefix-free code for $(A \uplus B) \upharpoonright 2n$ may be insufficient for our purpose. We now show the converse direction through more succinct prefix-free codes.

Lemma 3.3. *If B is compressible or A is B-compressible, then $A \uplus B$ is compressible.*

Proof. First we show that if B is compressible then so is $A \uplus B$ and then we show the other part of the theorem. Although the proof of the second part of the theorem subsumes the first part, for the sake of clarity we start with the first one. Proofs for both the parts involve similar argument.

For any fixed c let n satisfies $K(B \upharpoonright n) < n - c$, and let σ be a shortest program from the c.e. set of codes $\mathcal{P}$ which outputs $B \upharpoonright n$. More specifically, suppose R be an universal machine such that $R(\sigma)$ outputs $B \upharpoonright n$. Consider the prefix-free set defined by

$$\mathcal{Q}_n = \{\tau\rho \mid \tau \in \mathcal{P}, |\rho| = n\}. \tag{1}$$

This is a prefix-free c.e. set of codes. Then $\sigma \circ (A \upharpoonright n)$ - *i.e.* σ concatenated with the first n bits of A - is a code for $A \uplus B$ for some machine M which first runs $R(\sigma)$ to output $B \upharpoonright n$, then interleaves $A \upharpoonright n$ with $B \upharpoonright n$ to produce $(A \uplus B) \upharpoonright 2n$. The length of this code is at most $K(B \upharpoonright n) + n + O(1)$, showing that $A \uplus B$ is compressible at length $2n$.

Now, assume that A is B-compressible, and for any fixed c let n and m satisfy

$$K(A \upharpoonright n \mid B \upharpoonright m) < n - c.$$

Since we can make redundant queries, without loss of generality, we assume that $m \geq n$. Let $\mathcal{P}$ be the set of prefix-free encodings of one-argument partial computable functions. We construct a prefix-free code to show that $(A \uplus B)$ is compressible at length $2m$. Consider $\mathcal{Q}_{m,n}$ defined by

$$\mathcal{Q}_{m,n} = \{\tau\rho \quad | \quad \tau \in \mathcal{P},\ |\rho| = 2m - n\}. \tag{2}$$

Since $\mathcal{P}$ is a prefix-free set and we append strings of a fixed length to the prefix-free codes, $\mathcal{Q}_{m,n}$ is also a prefix-free set. If $\mathcal{P}$ is computably enumerable, then so is $\mathcal{Q}_{m,n}$. Let σ be a shortest program in the set $\mathcal{P}$ that given $B \upharpoonright m$ as an input, outputs $A \upharpoonright n$. Then it is easy to see that the string $\alpha = \sigma \circ (B \upharpoonright m) \circ (A[n \dots m-1])$ - *i.e.* σ concatenated with the first m bits of B and the substring $A[n \dots m-1]$ - is an encoding of $A_0 B_0 \dots A_{m-1} B_{m-1}$. Moreover $\alpha \in \mathcal{Q}_{m,n}$. Since $K(A \upharpoonright n \mid B \upharpoonright m) < n - c$, $|\sigma| < n - c$. Hence $|\alpha| < n - c + m + m - n = 2m - c$.

Since the above argument is true for all c, we get that for all $c > 0$ there exists an m such that $K(A \uplus B \upharpoonright 2m) < 2m - c$, which in turn implies that the string $A \uplus B$ is compressible. □

We may expect this proof to be easily adapted to resource-bounded settings. Inherent in the above proof is the concept of universality – since there is a universal self-delimiting Turing machine which incurs at most additive loss over any other prefix-free encoding, it suffices to show that there is some prefix-free succinct encoding. We appropriately modify this in resource-bounded settings which lack such universal machines in general.

4 Martingales and van Lambalgen's Theorem

We now approach van Lambalgen's theorem using martingales, adapting the Solovay tests in the literature [Nie09], [DH06].

Definition 4. *A function $d : \Sigma^* \to [0, \infty)$ is said to be a* martingale *if $d(\lambda) = 1$ and for every string w, $d(w) = (d(w0) + d(w1))/2$, and a* supermartingale *if for every string w, $d(w) \geq (d(w0) + d(w1))/2$.*

A martingale *or a* supermartingale *is said to be* computably enumerable *(c.e.) if there is a Turing Machine $M : \Sigma^* \times \mathbb{N} \to \mathbb{Q}$ such that for every string w, the sequence $M(w, n)$ monotonically converges to $d(w)$ from below.*

The rate of convergence in the above definition need not be computable.

We follow the customary notation on computable enumerations (see, for example, Downey and Hirschfeldt [DH06] Chapter 2), we denote the contents of the output tape of a Turing machine M at computation step s as $M[s]$. We say that the computation converges if there is a finite s_0 such that the machine M halts at step s_0, and say that the output of the computation M is $M[s]$. Further, we adopt the convention that $M[s] = M[s_0]$ for all $s > s_0$.

Definition 5. *We say that a martingale d* succeeds *on $X \in \Sigma^\infty$ if* $\limsup_{n\to\infty} d(X \upharpoonright n) = \infty$*, written $X \in S^\infty[d]$, and that d* strongly succeeds *on X, written $X \in S^\infty_{str}[d]$, if* $\liminf_n d(X \upharpoonright n) = \infty$.

If no computably enumerable martingale or supermartingale succeeds on X, then we say that X is Martin-Löf random. We say that X is non-Martin-Löf random *relative to Y if there is a computably enumerable oracle martingale d such that* $\limsup_{n\to\infty} d^Y(X \upharpoonright n) = \infty$.

We introduce the notion of bivariate martingales, following the approach of Bauwens [Bau15].

Definition 6. *A function $m : \Sigma^* \times \Sigma^* \to [0, \infty)$ is called a* bivariate martingale *if for each string x, $m(x, \cdot)$ and $m(\cdot, x)$ are both martingales.*

We say that a bivariate martingale *succeeds* on a pair of infinite binary sequences (X, Y) if the set

$$\{m(X \upharpoonright n, Y \upharpoonright m) \mid n, m \in \mathbb{N}\}$$

has no finite upper bound. We say that a pair (A, B) of infinite sequences is Martin-Löf random if there is no computably enumerable bivariate martingale which succeeds on it.

We adapt the following lemma from [Bau15] to the setting of computably enumerable martingales.

Lemma 4.1 (Folklore). *(A, B) is Martin-Löf random if and only if $A_0B_0A_1B_1\dots$ is Martin-Löf random.*

The proof is identical to that of Bauwens except to note that the martingales are computably enumerable. We reproduce this for completeness.

Proof. (Bauwens [Bau15]) Suppose $f : \Sigma^* \to [0, \infty)$ is a univariate martingale. Construct a bivariate martingale $m : \Sigma^* \times \Sigma^* \to [0, \infty)$ as follows. For strings σ and τ of length n, defined $m(\sigma, \tau)$ to be $f(\sigma_0\tau_0 \dots \sigma_{n-1}\tau_{n-1}$. If $|\sigma| < |\tau|$, then define $m(\sigma, \tau)$ to be the average over all extensions $\sigma^\frown\nu$ of length $|\tau|$ of $g((\sigma^\frown\nu) \uplus \tau)$. m is computably enumerable if f is, and succeeds on a pair of infinite sequences (A, B) if f succeeds on $(A \uplus B)$.

Conversely, suppose $m : \Sigma^* \times \Sigma^* \to [0, \infty)$ is a bivariate martingale. We construct a univariate martingale $f : \Sigma^* \to [0, \infty)$ as follows.

$$f(\sigma) = \begin{cases} m(\sigma_0\sigma_2 \dots \sigma_{|\sigma|-2}, \sigma_1\sigma_3 \dots \sigma_{|\sigma|-1}) & \text{if } |\sigma| \text{ is even,} \\ m(\sigma_0\sigma_2 \dots \sigma_{|\sigma|-1}, \sigma_1\sigma_3 \dots \sigma_{|\sigma|-2}) & \text{otherwise.} \end{cases}$$

The martingale f is computably enumerable if m is. By the savings account trick, it suffices to consider martingales g such that for every pair of strings (σ, τ), and all extensions $(\sigma\mu, \tau\nu)$, we have $m(\sigma\mu, \tau\nu) \geq m(\sigma, \nu)/2$. If m strongly succeeds on (A, B), then it follows that f succeeds on $(A \uplus B)$. $\square$

Lemma 4.2. *If B is not Martin-Löf random or A is not Martin-Löf random relative to B, then $A \uplus B$ is not Martin-Löf random.*

Proof. Let d_B be a martingale that succeeds on B. Then the martingale d_{AB} defined by setting $d_{AB}(\lambda)$ to 1 and

$$\begin{aligned} d_{AB}(\sigma_0\tau_0 \dots \tau_{n-2}\sigma_{n-1}) &= d_{AB}(\sigma_0\tau_0 \dots \tau_{n-2}). \\ d_{AB}(\sigma_0\tau_0 \dots \sigma_{n-1}\tau_{n-1}) &= d_B(\tau_0 \dots \tau_{n-1}). \end{aligned} \tag{3}$$

The above definition is a martingale since for any $n \geq 2$,

$$d_{AB}(\alpha_0\beta_0 \ldots \beta_{n-2}\alpha_{n-1}) = d_B(\beta_0 \ldots \beta_{n-2}).$$

Clearly, $\limsup_{n\to\infty} d_{AB}(A \uplus B) = \limsup_{n\to\infty} d_B(B)$ and hence d_{AB} succeeds on $A \uplus B$.

Now, suppose d succeeds strongly on A given oracle access to B. Consider the bivariate martingale m defined by setting $m(\lambda, \lambda) = 1$ and setting

$$m(\sigma, \tau)[s] = \frac{\sum_{\nu \in \Sigma^s} d^{\tau\nu}(\sigma)[s]}{2^s}.$$

It follows that

$$m(\sigma, \tau) = \lim_{s\to\infty} \frac{\sum_{\nu \in \Sigma^s} d^{\tau\nu}(\sigma)[s]}{2^s}.$$

The above limit exists because for every τ and extension $\nu \in \Sigma^s$,

$$\lim_{s\to\infty} d^{\tau\nu}(\sigma)[s] = d^{\tau\nu}(\sigma),$$

uniformly in τ, since the use of σ is finite and since d is a total martingale. Observe that, if n is the use of σ, then we can write the above limit as

$$m(\sigma, \tau) = \lim_{s\to\infty} \frac{\sum_{\nu \in \Sigma^n} d^{\tau\nu}(\sigma)[s]}{2^n}.$$

We show that m is a martingale in each of its arguments separately. For each $s \in \mathbb{N}$,

$$\begin{aligned}
m(\sigma 0, \tau) + m(\sigma 1, \tau) &= \lim_{s\to\infty} \frac{m(\sigma 0, \tau)[s] + m(\sigma 1, \tau)[s]}{2} \\
&= \lim_{s\to\infty} \frac{\sum_{\nu \in \Sigma^n} d^{\tau\nu}(\sigma 0)[s] + d^{\tau\nu}(\sigma 1)[s]}{2 \times 2^n} \\
&= \lim_{s\to\infty} \frac{\sum_{\nu \in \Sigma^n} d^{\tau\nu}(\sigma)}{2^n} \\
&= m(\sigma, \tau).
\end{aligned}$$

Hence we can see that m is a martingale in its first argument. Now, assume that n is a length longer than the use of σ.

$$\begin{aligned}
\frac{m(\sigma, \tau 0) + m(\sigma, \tau 1)}{2} &= \lim_{s\to\infty} \frac{\sum_{\nu \in \Sigma^s} \left(d^{\tau 0\nu}(\sigma)[s] + d^{\tau 1\nu}(\sigma)[s]\right)}{2 \times 2^s} \\
&= \lim_{s\to\infty} \frac{\sum_{\nu \in \Sigma^n} \left(d^{\tau 0\nu}(\sigma)[s] + d^{\tau 1\nu}(\sigma)[s]\right)}{2 \times 2^n} \\
&= \frac{\sum_{\mu \in \Sigma^{n+1}} d^{\tau\mu}(\sigma)}{2^{n+1}} \\
&= \lim_{s\to\infty} \frac{\sum_{\nu \in \Sigma^s} d^{\tau\nu}(\sigma)}{2^s} \\
&= m(\sigma, \tau).
\end{aligned}$$

The limit above stabilises since the use on σ is finite. Hence beyond a point, $d^{\tau\nu'}(\sigma)$ and $d^{\tau\nu}(\sigma)$ tend to the same limit.

Since d is a c.e. oracle martingale, it follows that m is a c.e. martingale. For every pair of infinite sequences V and W and for every l, there is a number n computable from $V \upharpoonright l$ and W such that for all large enough stages s, $d^{W\upharpoonright s}(V \upharpoonright l) = d^W(V \upharpoonright l)$. Thus for each l, the value of $m((V \upharpoonright l) \uplus (W \upharpoonright l))[s]$ is the same as $m((V \upharpoonright l) \uplus (W \upharpoonright l))[s_1]$ for all $s_1 > s$, for some large enough s. It follows that m is c.e. martingale.

We know that d strongly succeeds on every sequence that it succeeds on. Let N_0 and M_0 be such that $d^{B\upharpoonright M}(A \upharpoonright N) > K$ for all $M \geq M_0$ and $N \geq N_0$. Then, we can verify that $m(A \upharpoonright N_1, B \upharpoonright M_1) > K$. Thus m succeeds on the pair (A, B). $\square$

The converse also holds. However, in the latter part of this paper we show that the analogous results may not hold in time-bounded versions.

Lemma 4.3. *If $A \uplus B$ is not Martin-Löf random, then either B is not Martin-Löf random or A is not Martin-Löf random relative to B.*

For the proof of this lemma, it is convenient to use a notion which is related to martingales.

Definition 7. *A function $f : \Sigma^\infty \to [0, \infty]$ is called* lower semicomputable *if the set*

$$\{(\sigma, q) \mid \sigma \prec X, X \in \Sigma^\infty \text{ and } q \leq f(X)\}$$

is computably enumerable – i.e. *the rational points in the lower graph of f is computably enumerable.*

Definition 8. *A lower semicomputable function f is said to be a* measure of impossibility[2] *with respect to a probability measure P if $\int f dP < \infty$.*

We focus our attention on the uniform probability measure on $[0, 1]$. We have the following theorem characterizing Martin-Löf randomness in terms of measures of impossibility.

Theorem 4. *A sequence $X \in \Sigma^\infty$ is Martin-Löf random if and only if for every measure of impossibility $f : \Sigma^\infty \to [0, \infty]$, $f(X) < \infty$.*

Relativizing the proof of the above theorem, we have the following.

Corollary 4.1. *A sequence $X \in \Sigma^\infty$ is Martin-Löf random relative to $Y \in \Sigma^\infty$ if and only if for every measure of impossibility $f^Y : \Sigma^\infty \to [0, \infty]$, $f^Y(X) < \infty$.*

Proof of Lemma 4.3. Suppose d_{AB} is a martingale which succeeds on $A \uplus B$. Define the martingale d_B by setting $d_B(\lambda) = 1$ and

$$d_B(\sigma) = 2^{-|\sigma|} \sum_{\{\tau \,:\, |\tau| = |\sigma|\}} d_{AB}(\tau \uplus \sigma) \tag{4}$$

for finite nonempty strings σ. It is easy to establish that d_B is c.e. if d_{AB} is.

Suppose that for any positive N, there are infinitely many n such that

$$\sum_{\sigma \in \Sigma^n} d_{AB}(\sigma_0 B_0 \dots \sigma_{n-1} B_{n-1}) \geq N 2^n. \tag{5}$$

In this case, $d_B(B \upharpoonright n)$ is at least N. Hence d_B succeeds on B, and the lemma holds.

Otherwise, there is some positive N and an n_0 such that for all $n \geq n_0$, we have the inequality in (5) reversed.

By using the "savings account" trick, we can define another martingale which succeeds strongly on $A \uplus B$. We consider the paired functions $(f, s) : \Sigma^* \to [0, \infty)$ defined as follows. Initially, $f(\lambda) = 1$ and $s(\lambda) = 1$. On any $\sigma \in \Sigma^*$, $f(\sigma b)$ bets the same ratio of its capital as d_{AB}, and if the resulting capital is greater than 2, then we set $f(\sigma b)$ to 1 and transfer the remaining capital to $s(\sigma b)$.

$$f(\lambda) = 1$$
$$f(\sigma b) = \begin{cases} \frac{d_{AB}(\sigma b)}{d_{AB}(\sigma)} f(\sigma) & \text{if } \frac{d_{AB}(\sigma b)}{d_{AB}(\sigma)} f(\sigma) < 2 \\ 1 & \text{otherwise,} \end{cases}$$

[2] also called an *integral test*

and

$$s(\lambda) = 0$$
$$s(\sigma b) = \begin{cases} s(\sigma) & \text{if } \frac{d_{AB}(\sigma b)}{d_{AB}(\sigma)} f(\sigma) < 2 \\ s(\sigma) + \left(\frac{d_{AB}(\sigma b)}{d_{AB}(\sigma)} f(\sigma) - 1 \right) & \text{otherwise.} \end{cases}$$

We can verify that s is monotone increasing in its prefix length and if $X \in S^{\infty}[d_{AB}]$, then $X \in S^{\infty}_{\text{str}}[s]$. Moreover, it is possible to compute $s(\sigma b)$ incrementally in a monotone increasing manner from $s(\sigma)$ by computing $d(\sigma b)$, and transferring the excess amount to s. (For the savings account trick, see Proposition 6.3.8 in Downey and Hirschfeldt [DH06]).

Now consider the function $g^Y : \Sigma^{\infty} \to [0, \infty]$ defined by

$$g^Y(X) = \lim_{n \to \infty} s(X_0 Y_0 \ldots X_{n-1} Y_{n-1}).$$

For every sufficiently large n, we have $\int_{C_\sigma} g^Y d\mu \leq N 2^n$, by assumption, where $C_\sigma \subseteq \Sigma^{\infty}$ consists of all infinite sequences with σ as a prefix, and μ is the Lebesgue measure on Cantor Space. As in [Nan09], we can verify that g is a measure of impossibility, using Fatou's lemma.

Hence g^Y is a measure of impossibility. Now by Theorem 4.1, if d_{AB} succeeds on $A \uplus B$, then $g^B(A) = \infty$. Also, if d_{AB} is computably enumerable, then g^B is lower semicomputable. Hence A is not Martin-Löf random relative to B. □

5 Resource-bounded relative randomness and incompressibility

We consider time-bounded self-delimiting Kolmogorov complexity in this section. While there are several variants of this notion (see e.g. [LW95], [ABK+06]), we deal with the simplest one here.

The time-bound is a function of the lengths of its output[3] as in [LW95]. Throughout this paper we assume t to be any time-constructible function. We first fix a prefix-free set $\mathcal{P}$ encoding the set of partial-computable functions. We do not insist that $\mathcal{P}$ consist solely of functions which run in t steps, since the results are identical with or without this assumption.

Definition 9. *The* t-time-bounded complexity *of σ is defined by*

$$K_T(\sigma; t) = \min\{|\pi| \mid \pi \in \mathcal{P} \text{ outputs } \sigma \text{ in at most } t \text{ steps}\}, \tag{6}$$

and the conditional t-time-bounded complexity *of σ given τ be defined by*

$$K_T(\sigma \mid \tau; t) = \min\{|\pi| \mid \pi \in \mathcal{P}, \pi(\tau) \text{ outputs } \sigma \text{ in at most } t \text{ steps}\}. \tag{7}$$

For any fixed time bound function $t : \mathbb{N} \to \mathbb{N}$, we do not have universal machines within the class of t-bounded machines. However, there are invariance theorems (see e.g. [LV08] Chapter 7). Hence we can use the definition of time-bounded complexity to define the notion of incompressible infinite sequences.

Definition 10. *An infinite binary sequence X is said to be* t-incompressible *if* $\exists c \quad \forall n \quad K_T(X \upharpoonright n; t(n)) \geq n - c$ *and* t^Y-incompressible *if* $\exists c \quad \forall n \quad \forall m \quad K_T(X \upharpoonright n \mid Y \upharpoonright m; t(n)) \geq n - c$.

If for $t' > t$, a sequence X is t'-incompressible, then it is t-incompressible as well. Moreover, for every X and n, $K_T(X \upharpoonright n) \geq K(X \upharpoonright n)$. Since the set of K-incompressible sequences has measure 1, we know that the set of t-incompressible sequences has measure 1 as well. When the time bound is understood from the context, we write $K_T(\sigma)$ and $K_T(\sigma \mid \tau)$. Throughout this paper we consider the time bound function

[3]Considering time bound that is dependent on output length is customary for decompressors. To make it input-length dependent it is customary to append 1^l as an additional input where l is the output length

to be $t(n) > \ell n$ for some constant $\ell > 1$. Without the assumption of such a super-linear time bound the decompressor algorithm may not be able to even output the whole string.

We now show that for time-bounded Kolmogorov complexity, only one direction of van Lambalgen's theorem holds. We first show that if we can compress B, or A relative to B within the time bound, then it is possible to compress $A \uplus B$ within the time bounds, adapting the proof of Lemma 3.3.

Lemma 5.1. *If B is t-compressible or A is t^B-compressible, then $A \uplus B$ is t-compressible.*

Proof. Assume that B is t-compressible. Then for every constant c there is an n such that there is a short program in $\beta \in \mathcal{P}$ with $|\beta| < n - c$ which outputs $B \upharpoonright n$ within $t(n)$ steps.

For any such n, consider the prefix-code defined by

$$\mathcal{Q}_n = \{\sigma\alpha \mid \sigma \in \mathcal{P}, |\alpha| = n\}. \tag{8}$$

This forms a prefix encoding, containing a code $\beta \circ (A \upharpoonright n)$ - β concatenated with the first n bits of A - for $(A \uplus B) \upharpoonright 2n$. Moreover, it is possible to decode $(A \uplus B) \upharpoonright 2n$ from its code within $t(2n)$ steps.

Suppose A is t^B-compressible. Assume that for a fixed c there exist n and m such that $K_T((A \upharpoonright n) \mid (B \upharpoonright m); t(n)) < n - c$, witnessed by a code α. Without loss of generality, we may assume $n \leq m$. Then consider $\mathcal{Q}_{m,n}$ as defined in (2). We see that $\mathcal{Q}_{m,n}$ is a computably enumerable prefix set. The code $\alpha \circ (B \upharpoonright m) \circ A[n \dots m-1] \in \mathcal{Q}_{m,n}$ of $(A \uplus B) \upharpoonright 2m$ can be decoded in time $t(2m)$, and is shorter than $2m + c$.

Hence $K_T((A \uplus B) \upharpoonright 2m; t(2m)) < 2m - c$. Since the above argument is true for all constants c, the lemma follows. ☐

The converse of the above lemma is false. We do not appeal to the failure of polynomial-time (in general, resource-bounded) symmetry of information (see for example, [LW95]), but directly construct a counterexample pair.

Lemma 5.2. *There are sequences A and B where $A \uplus B$ is t-compressible, but B is t-incompressible and A is t-incompressible relative to B.*

Proof. We build such a pair in stages. In the stage $s = 0$, we set $A_s = B_s = \lambda$. Then in $s \geq 1$, assume that we have inductively defined prefixes A_{s-1} of A and B_{s-1} of B, where $|A_{s-1}| = t(s-1)$ and $|B_{s-1}| = 2^{t(s-1)^2}$. We select strings α_s and β_s satisfying specific incompressibility properties and then define

$$A_s = A_{s-1}\alpha_s \quad \text{and} \quad B_s = B_{s-1}\beta_s\alpha_s.$$

We choose α_s and β_s which satisfy following incompressibility requirements.

1. Length requirements: $|\alpha_s| = t(s) - t(s-1)$ and $|\beta_s| = 2^{t(s)^2} - 2^{t(s-1)^2} - t(s) + t(s-1)$. These lengths ensure that $|A_s| = t(s)$ and $|B_s| = 2^{t(s)^2}$.

2. Incompressibility requirements for B: there is a constant c such that

$$K(B_{s-1}\delta) \geq |B_{s-1}\delta| - c$$

   for every $\delta \preceq \beta_s\alpha_s$.

3. Incompressibility requirements for A relative to B:

$$K(A_{s-1}\tau \mid B_{s-1}\beta_s) \geq |A_{s-1}\tau| - c'$$

   for some constant c' and every $\tau \preceq \alpha_s$.

It suffices to show we can find such strings α_s and β_s. We can select the strings in the following order. First, select a string β_s such that $K(\delta \mid B_{s-1}) > |\delta| - c$ for every prefix δ of β_s, and some constant c. Such a string exists, since the set of Martin-Löf random strings has measure 1. Then select the string α_s to satisfy $K(\tau \mid A_{s-1}, B_{s-1}\beta_s) \geq |\tau| - c'$ for every prefix τ of α_s, and a constant c'. Each of these selections is possible because the set of incompressible strings conditioned on any other strings is non-empty (for example, see the Ample Excess Lemma [MY08]).

By the above construction it is clear that B is t-incompressible and $A \uplus B$ is t-compressible for any function $t(n) > n$ due to the shared component α_s for all s between A and B as long as $t(.)$ is time-constructible which is indeed the case by our assumption in the beginning of the current section.

We now show that A is t^B-incompressible. Inductively, assume that A_{s-1} is t-incompressible given access to $B \restriction (2^{t(s-1)^2})$. By construction, for every τ such that $A_{s-1} \prec \tau \preceq A_s$ is t-incompressible given access to $B \restriction (2^{t(|\tau|)})$, since we ensure that every prefix of A_s is incompressible given $B_{s-1}\beta_s$, i.e. $B \restriction (2^{t(s)^2} - t(s) + t(s-1))$, which is longer than $B \restriction (2^{t(s)})$, the prefix of B that A_s can query within the time-bound t. □

6 Resource-bounded relative randomness and martingales

In this section, we show that the symmetry of relative randomness does not hold for resource-bounded martingales. Let $t : \mathbb{N} \to \mathbb{N}$ be a superlinear time-constructible function. For any input $\sigma \in \Sigma^*$, we henceforth restrict ourselves to martingales computed in time $t(|\sigma|)$ and we define t-randomness accordingly.

Definition 11. *A* t-bounded martingale *is a martingale* $d : \Sigma^* \to [0, \infty)$ *such that for all* $w \in \Sigma^*$, $d(w)$ *can be computed in at most* $t(|w|)$ *steps.*

Unlike computably enumerable martingales, these martingales have to terminate with the ultimate value of the bet in a finite number of steps. The notion of success of a t-bounded martingale is the same as that in the case of computably enumerable martingales.

Definition 12. *We say that* $X \in \Sigma^\infty$ *is* t-random *if there is no* t*-bounded martingale which succeeds on* X*, and* t-random with respect to $Y \in \Sigma^\infty$ *if no* t*-bounded oracle martingale* $d^Z : \Sigma^* \to [0, \infty)$ *exists such that* $X \in S^\infty[d^Y]$.

Lemma 6.1. *There is a* t*-random sequence* B *and a sequence* A *which is* t^B*-random, such that* $A \uplus B$ *is* t*-nonrandom.*

The idea of the construction is that at some positions, substrings in A are copied exactly from regions of B. These regions of B sufficiently far so that it is not possible to consult the relevant region in time t. Of course, $A \uplus B$ is non-random since a significant suffix of B can be computed directly from the relevant region of A.

Elsewhere, if B is random, and A random relative to B, then we can make B t-random, and A to be t^B-random.

In short, the construction ensures that B has sufficient time to look into the prefix of A, but A does not have time to look into the extension of B.

Proof. We construct two sequences A and B in stages, where at stage $s = 0$, we have $A_s = B_s = \lambda$. At stage $s \geq 1$, let us assume that we have inductively defined prefixes A_{s-1} of A and B_{s-1} of B and additionally $|A_{s-1}| = t(s-1)$ and $|B_{s-1}| = 2^{t(s-1)^2}$. We select strings α_s and β_s satisfying specific randomness properties and then define

$$A_s = A_{s-1}\alpha_s \quad \text{and} \quad B_s = B_{s-1}\beta_s\alpha_s$$

We choose strings α_s and β_s which satisfy all the following randomness requirements.

1. Length requirements: $|\alpha_s| = t(s) - t(s-1)$ and $|\beta_s| = 2^{t(s)^2} - 2^{t(s-1)^2} - t(s) + t(s-1)$. These lengths ensure that $|A_s| = t(s)$ and $|B_s| = 2^{t(s)^2}$.
2. Randomness requirements for B: for some universal martingale $d^{B_{s-1}}$, for every $\delta \preceq \beta_s$, $d(B_{s-1}\delta) \leq d(B_{s-1})$.
3. Randomness requirements for A relative to B: for some universal oracle martingale $d^{B_{s-1}\beta_s}$, for every $\tau \preceq \alpha_s$, $d^{B_{s-1}\beta_s}(A_{s-1}\tau) \leq d^{B_{s-1}}(A_{s-1})$.

It suffices to show we can find such strings α_s and β_s. We can select the strings in the following order. First, select a string β_s which satisfies the fact that for a universal martingale d, and for every $\sigma \preceq \beta_s$, $d(B_{s-1}\sigma) \leq d(B_{s-1})$. Such a string β_s exists because the martingale property together with the Markov inequality allows us to show that for any string κ and any n, the set $\{\rho \in \Sigma^n \mid \forall \sigma \preceq \rho,\ d(\kappa\sigma) \leq d(\kappa)\}$ has positive probability. By a similar argument we can then select the string α_s such that for a universal martingale $d^{B_{s-1}\beta_s}$, and for every $\tau \preceq \alpha_s$, $d^{B_{s-1}\beta_s}(A_{s-1}\tau) \leq d^{B_{s-1}}(A_{s-1})$.

By construction it is clear that B is Martin-Löf random and $A \uplus B$ is not t-random for any superlinear t due to the shared component α_s for all s between A and B as long as the function $t(.)$ is time-constructible which is indeed the case by our assumption. However we can show that A is t^B-random. By the construction it can be noted that any martingale d^B, can gain capital on the stretch α_s only if it can query the corresponding portion of the sequence B. To calculate the value of $d^B(A \upharpoonright n)$ it needs to query the index bigger than $2^{\omega(t(n))}$ of the sequence B, which is impossible in the given time-bound. □

Now, we consider the converse.

Lemma 6.2. *Let B be an arbitrary t-random sequence. Then there is a t-random sequence A which is t^B-nonrandom, such that B is t^A-random.*

Proof. (Sketch) The construction is similar to that of Lemma 6.1. Let B be a Martin-Löf random sequence, and A be a Martin-Löf random sequence, except for a short string at $A_{2^{t(n)^2}}$ identical to a string at B_n, $n \in \mathbb{N}$. We see that A is t^B-nonrandom. However, B does not have sufficient time to consult the relevant position in A, and is t^A-random. □

However, in the above example, $A \uplus B$ is t-nonrandom, since the substring at $(A \uplus B)_{2\times 2^{t(n)^2}}$ is computable from the prefix of $(A \uplus B) \upharpoonright 2n$. Thus the identification of relative randomness of A and B with the randomness of $A \uplus B$ breaks down in time-bounded settings.

Corollary 6.1. *There are sequences A and B such that A is t^B nonrandom, $A \uplus B$ is t-nonrandom, and B is t^A random.*

Now let us first make an observation.

Lemma 6.3. *If B is t-nonrandom then for any sequence A, $A \uplus B$ is t-nonrandom.*

Proof. If d_B be a t-martingale witnesses the fact that B is t-nonrandom, then the martingale d_{AB} defined in (1) is a t-martingale that succeeds on $A \uplus B$.

□

We wish to investigate the question of t-randomness of $A \uplus B$ given that A is t^B-nonrandom. We have weak converses which we now describe. The above corollary suggests that we stipulate "honest" reductions - that a bit at position n in A cannot depend on bits at positions $o(t^{-1}(n))$ in B. With this stipulation, we have the following weak converse to Lemma 6.1. First, we consider a restricted class of reductions from A to B.

Definition 13. *We say that an infinite sequence A is* infinitely often reducible *to B in time t via f, written $A \leq^t_{i.o} B$, if $\{n \in \mathbb{N} \mid f(B[n - t(n) \dots n + t(n) - 1]) = A_n\}$ is computable in time $t(n)$, i.e., t-computable.*

Note that we have incorporated an honesty requirement into the definition.

Definition 14. *We say that a function $f : \Sigma^* \to \Sigma$ is* strongly influenced by the last index *if for every $\sigma \in \Sigma^n$, $f(\sigma) \neq f((\sigma \restriction n-1)\overline{\sigma_n})$, where $\overline{\sigma_n}$ denotes the complement of the bit σ_n.*

The function that projects the last bit of its input, and the function computing the parity of all input bits are two examples of such functions.

Lemma 6.4. *Let A be t^B-nonrandom and $A \leq^t_{i.o} B$ via a function that is strongly influenced by the last index. Then $A \uplus B$ is also t-nonrandom.*

Proof. Consider the t-computable set of positions $S = \{n \mid f(B[n - t(n) \dots n + t(n) - 1]) = A_n\}$ where A queries B. We define a martingale d with initial capital 1 and which bets evenly on all positions except those in the set T defined by

$$T = \{2(i + t(i)) + 1 \mid i \in S\}.$$

For positions $2(i + t(i)) + 1 \in T$, sets $d(A_0 B_0 \dots A_{i+t(i)} b)$ to $2d(A_0 \dots A_{i+t(i)})$ if $f((B \restriction i + t(i) - 1)b) = A_i$, and to 0 otherwise. Then $A \uplus B \in S^\infty[d]$. □

A second weak converse can be obtained by assuming that the t-martingale succeeds on the interleaved sequence in a specific manner.

Definition 15. *We say that a pair of sequences (A, B) is t-resilient if*

1. *For every oracle martingale h runs in time $t(n)$, $\limsup_{n\to\infty} h^{B\restriction n-1}(A \restriction n) < \infty$.*
2. *For every oracle martingale g runs in time $t(n)$, $\limsup_{n\to\infty} g^{A\restriction n}(B \restriction n) < \infty$.*

We say that a martingale d wins at position i on a sequence X if $d(X \restriction i) > d(X \restriction i - 1)$.

Lemma 6.5. *If $A \uplus B$ is t-random then (A, B) is a t-resilient pair. On the converse, if (A, B) is a t-resilient pair then $A \uplus B$ is $\sqrt{t(n)/n}$-random.*

Note that the above equivalence will be exact if we consider all the polynomial time martingales.

Proof. If (A, B) is not a t-resilient pair then either there is a oracle martingale h runs in time $t(n)$ such that $\limsup_{n\to\infty} h^{B\restriction n-1}(A \restriction n) = \infty$, or a oracle martingale g runs in time $t(n)$ such that $\limsup_{n\to\infty} g^{A\restriction n}(B \restriction n) = \infty$. If the first condition holds, then

$$\begin{aligned} d(A \uplus B \restriction 2n - 1) &= h^{B\restriction n-1}(A \restriction n), \\ d(A \uplus B \restriction 2n) &= d(A \uplus B \restriction 2n - 1) \end{aligned}$$

is a t-martingale witnessing that $A \uplus B$ is t-nonrandom. If the second condition holds then we can define a similar martingale d based on g, witnessing t-nonrandomness of $A \uplus B$.

Conversely, suppose that there exists a martingale d which runs in time $t(n)$ and witnesses the fact that $A \uplus B$ is t-nonrandom. Now construct the oracle martingales h and g as follows:

$$\begin{aligned} h^Y(\sigma) = g(\sigma) &= d(\lambda) \text{ if } \sigma = \lambda \text{ or } \sigma \in \Sigma \\ h^Y(X \restriction n) &= \frac{d(X \uplus Y \restriction 2n - 1)}{d(X \uplus Y \restriction 2n - 2)} \cdot h^Y(X \restriction n - 1) \\ g^X(Y \restriction n) &= \frac{d(X \uplus Y \restriction 2n)}{d(X \uplus Y \restriction 2n - 1)} \cdot g^X(Y \restriction n - 1) \end{aligned}$$

Clearly h is dependent on $B \restriction n - 1$ and g is dependent on $A \restriction n$. Since $\limsup_{n\to\infty} d(A \uplus B \restriction n) \uparrow \infty$, we claim that one of h and g succeeds over A and B given $B \restriction n - 1$ and $A \restriction n$ respectively. We have

$$\begin{aligned} \limsup_{n\to\infty} h^{B\restriction n-1}(A \restriction n) \cdot g^{A\restriction n}(B \restriction n) &= \limsup_{n\to\infty} \frac{d(A \uplus B \restriction 2n)}{c} \\ &\leq \limsup_{n\to\infty} h^{B\restriction n-1}(A \restriction n) \cdot \limsup_{n\to\infty} g^{A\restriction n}(B \restriction n) \end{aligned}$$

for some fixed constant c (independent of n). Note that LHS is ∞ because $d(A \uplus B \upharpoonright n)$ is a sequence which satisfies the property

$$2d(A \uplus B \upharpoonright n-1) \geq d(A \uplus B \upharpoonright n) \geq 0$$

and $\limsup_{n\to\infty} d(A \uplus B \upharpoonright n) = \infty$. So one of the term involving h or g has to go to ∞. Observe that by the construction, h and g are oracle functions computable in time $n(t(n))^2$. Now we show that h and g are oracle martingales.

$$\sum_{b\in\Sigma} h((A \upharpoonright n)b) = \frac{h(A \upharpoonright n)}{d(A \uplus B \upharpoonright 2n)} \sum_{b\in\Sigma} d((A \uplus B \upharpoonright 2n)b) = 2 \cdot h(A \upharpoonright n)$$

and thus h is a oracle martingale. By a similar argument g is also a oracle martingale. Since either $\limsup_{n\to\infty} h^{B\upharpoonright n-1}(A \upharpoonright n) = \infty$ or $\limsup_{n\to\infty} g^{A\upharpoonright n}(B \upharpoonright n) = \infty$, it follows that (A, B) is a not a t'-resilient pair where $t'(n) = n(t(n))^2$.

□

7 A Modified Definition of Resource-bounded Martingales

In this section, we propose an alternate definition of a time-bounded martingale whose behavior with respect to van Lambalgen's theorem is identical to the definition using time-bounded prefix-complexity. In the light of van Lambalgen's theorem, we may view this as a reasonable variant definition.

Definition 16. *We say that a martingale $d : \Sigma^* \to [0, \infty)$ is a t-*bounded lookahead *martingale if there is for each string σ, there is a set $L_{d,\sigma} \subseteq \mathbb{N}$ such that the following conditions are satisfied.*

1. *$d(\lambda) = 1$ and $L_{d,0} = \emptyset$.*
2. *For any string σ, $d(\sigma 0) + d(\sigma 1) = 2d(\sigma)$.*
3. *For any string $\sigma \in \Sigma^{n-1}$, if $n \notin L_{d,\sigma}$ then to compute $d(\sigma b)$, $b \in \Sigma$, the martingale can query a set of positions $S \subseteq \{0, \dots, n-2, n, \dots, t(n)\}$. Subsequently, $L_{d,\sigma b}$ is set to $L_{d,\sigma} \cup S$. If $n-1 \in L_{d,\sigma}$, then we forbid betting, and set $d(\sigma b)$ to $d(\sigma)$, and $L_{d,\sigma b}$ to $L_{d,\sigma}$.*

Definition 17. *We say that an infinite sequence is t-*lookahead-non-random *if there is a t-bounded lookahead martingale which succeeds on it.*

To compute $d(X \upharpoonright n)$, the martingale is allowed to wait until an appropriate extension length is available, and base its decision on a few bits ahead. However, we have to be careful not to reveal X_{n-1} itself, and to ensure that positions once revealed can never later be bet on. These restrictions ensure that the betting game is not trivial, and that there are unpredictable or random sequences.

Lemma 7.1. *There is a t-lookahead random sequence B and a t^B-lookahead random sequence A such that $A \uplus B$ is t-lookahead nonrandom.*

The proof is essentially the same as that of Lemma 6.1. With the modified definition, we can now prove result similar to Lemma 5.1.

Lemma 7.2. *If B is t-lookahead nonrandom or A is t^B-lookahead nonrandom. Then $A \uplus B$ is t-lookahead nonrandom.*

Proof. Suppose h is a t-lookahead-martingale that succeeds on B. Then define the t-lookahead martingale d by setting $d(\lambda) = 1$ and $L_{d,\lambda} = \emptyset$, and

$$d((X \uplus Y) \upharpoonright 2n+1) = d((X \uplus Y) \upharpoonright 2n), \quad L_{d,(X\uplus Y)\upharpoonright 2n+1} = L_{d,(X\uplus Y)\upharpoonright 2n}$$
$$d((X \uplus Y) \upharpoonright 2n+2) = h(Y \upharpoonright n), \quad L_{d,(X\uplus Y)\upharpoonright 2n+2} = \{2i+1 | i \in L_{h,Y\upharpoonright n}\}.$$

Then clearly $A \uplus B \in S^\infty[d]$ as $B \in S^\infty[h]$.

Now, assume that $A \in S^\infty[g^B]$ for a t-lookahead martingale g. Then we define the t-lookahead martingale d by $d(\lambda) = 1$ with $L_{d,\lambda} = \emptyset$ and

$$d((X \uplus Y) \upharpoonright 2n+2) = d((X \uplus Y) \upharpoonright 2n+1), \quad L_{d,(X \uplus Y)\upharpoonright 2n+2} = L_{d,(X \uplus Y)\upharpoonright 2n+1}$$
$$d((X \uplus Y) \upharpoonright 2n+1) = g^{Y \upharpoonright t(n)}(X \upharpoonright n),$$
$$L_{d,(X \uplus Y)\upharpoonright 2n+1} = L_{d,(X \uplus Y)\upharpoonright 2n} \cup \{2i | i \in L_{g,X\upharpoonright n}\} \cup \{2i+1 | i \in Q_{g,X,Y,n}\},$$

where $Q(g, X, Y, n)$ are the bits in the oracle queried by $g^Y(X \upharpoonright n)$. We know that $A \in S^\infty[g^B]$. Hence $A \uplus B \in S^\infty[d]$. $\square$

Acknowledgments

The authors thank the anonymous reviewers for their insightful comments, and Jack Lutz, Manjul Gupta and Michal Koucký for helpful discussions.

References

[ABK+06] Eric Allender, Harry Buhrman, Michal Koucký, Dieter van Melkebeek, and Detlef Ronneburger. Power from random strings. *SIAM Journal on Computing*, 35(4):1467–1493, 2006.

[Bau15] Bruno Bauwens. Uniform van lambalgen's theorem fails for computable randomness. *ARXIV*, abs/1510.00554, 2015.

[CNS17] Diptarka Chakraborty, Satyadev Nandakumar, and Himanshu Shukla. On resource-bounded versions of the van lambalgen theorem. In *Theory and Applications of Models of Computation - 14th Annual Conference, TAMC 2017, Bern, Switzerland, April 20-22, 2017, Proceedings*, pages 129–143, 2017.

[DH06] R. Downey and D. Hirschfeldt. *Algorithmic randomness and complexity.* Book Draft, 2006.

[Gol01] Oded Goldreich. *The Foundations of Cryptography - Volume 1, Basic Techniques.* Cambridge University Press, 2001.

[LR05] Troy Lee and Andrei Romaschenko. Resource-bounded symmetry of information revisited. *Theoretical Computer Science*, 345:386–405, 2005.

[Lut98] J. H. Lutz. Resource-bounded measure. In *Proceedings of the 13th IEEE Conference on Computational Complexity*, pages 236–248, New York, 1998. IEEE Computer Society Press.

[LV08] M. Li and P. M. B. Vitányi. *An Introduction to Kolmogorov Complexity and its Applications.* Springer-Verlag, Berlin, 2008. Third Edition.

[LW95] Luc Longpré and Osamu Watanabe. On symmetry of information and polynomial-time invertibility. *Information and Computation*, 121:14–22, 1995.

[MY08] Joseph S. Miller and Liang Yu. On initial segment complexity and degrees of randomness. *Trans. Am. Math. Soc.*, 360(6):3193–3210, 2008.

[Nan09] S. Nandakumar. A characterization of constructive dimension. *Mathematical Logic Quarterly*, 55(3):271–286, 2009.

[Nie09] André Nies. *Computability and Randomness.* Oxford Science Publications, 2009.

[vL87] M. van Lambalgen. *Random Sequences.* Academish Proefschri't, Amsterdam, 1987.

[Yu07] Liang Yu. When van Lambalgen's theorem fails. *Proc. Am. Math. Soc.*, 135(3):861–864, 2007.