Feasible analysis, randomness, and base invariance

Santiago Figueira André Nies

March 26, 2014

Abstract

We show that polynomial time randomness of a real number does not depend on the choice of a base for representing it. Our main tool is an 'almost Lipschitz' condition that we show for the cumulative distribution function associated to martingales with the savings property. Based on a result of Schnorr, we prove that for any base r, $n \cdot \log^2 n$-randomness in base r implies normality in base r, and that n^4-randomness in base r implies absolute normality. Our methods yield a construction of an absolutely normal real number which is computable in polynomial time.

1 Introduction

Algorithmic randomness notions are usually defined not for real numbers, but for their *digit representations* with respect to a fixed base. The corresponding test definitions, such as Martin-Löf tests and computable martingales, are given relative to a fixed finite alphabet, usually the binary alphabet $\{0, 1\}$. Thus definitions of randomness are given for binary sequences.

From a mathematical point of view, the primary objects of interest are real numbers. So it is customary to talk about random *reals* (no matter what the randomness notion is), though we always think of them as binary sequences. All known notions of randomness $\mathcal{R}$ can be adapted to any finite alphabet $\{0, \ldots, r-1\}$ ($r \geq 2$). So it makes sense to ask: what happens if we change the base for representing a real? Is the real always random in the given sense, independently of the base for representing it? More formally, we ask whether $\mathcal{R}$ is *base invariant* in the following sense:

> if X and Y are infinite sequences over different alphabets that denote the same real, then X satisfies $\mathcal{R}$ iff Y satisfies $\mathcal{R}$.

A *base* is any natural number greater than 1. For a base r, let $\Sigma_r = \{0, \ldots, r-1\}$. Randomness notions formalize, in one way or another, the intuitive idea of lack of patterns recognizable in an effective way. For weak notions of randomness, the property of *base invariance* can easily fail. Let us discuss some examples.

For finite strings σ and τ over the alphabet Σ_r, we define $\mathsf{occ}_\sigma(\tau)$ as the number of occurrences of σ in τ, that is

$$\mathsf{occ}_\sigma(\tau) = |\{i \colon 0 \leq i \leq |\tau| - |\sigma|, \sigma = \tau(i)^\frown \ldots {}^\frown\tau(i + |\sigma| - 1)\}|, \tag{1}$$

where $\tau(i)$ denotes the $(i+1)$-th symbol of τ, starting from the left, and $\cdot^\frown\cdot$ denotes the concatenation of strings.

Consider the law of large numbers as a very weak randomness notion. While this concept is too weak to qualify for randomness, it still captures some statistical properties that random sequences must have. An infinite sequence Z over the alphabet Σ_r satisfies the *law of large numbers* if any symbol in Z is equiprobable, that is, for any symbol $b \in \Sigma_r$ we have

$$\lim_n \frac{\mathsf{occ}_b(Z\restriction_n)}{n} = \frac{1}{r},$$

where $Z\restriction_n$ denotes the first n symbols of Z. The sequence $Y = 10101010\ldots$ over the alphabet 2 satisfies the law of large numbers. The real which in binary is represented as $0.Y$ can be represented as $0.2222\ldots$ in base 4. Since the sequence $2222\ldots$ does not satisfy the law of large numbers, the notion of *law of large numbers* is not base invariant.

A stronger notion (but still too weak to qualify as a randomness notion) is Borel normality [7]. An infinite sequence Z over the alphabet Σ_r is *normal in base* r if it satisfies a general form of the law of large numbers: each string of length n occurs in Z with limit relative frequency equal to r^{-n}. Formally, Z is normal in base r if

$$\lim_n \frac{\mathsf{occ}_\sigma(Z\restriction_n)}{n} = \frac{1}{r^{|\sigma|}}$$

for all finite strings σ over the alphabet Σ_r. A well-known example of a normal sequence is Champernowne's [11]. It is obtained by concatenating all natural numbers in base 10, one after the other:

$$X = 01234567891011121314\ldots \tag{2}$$

Analogously, one can define Champernowne's sequences in any base r by concatenating all the natural numbers represented in base r. As expected, one ends up with a sequence which is normal in base r. For the specific case of the sequence X defined in (2), it is unknown if its normality is base invariant. That is, let x be the real which in base 10 is represented as $0.X$, and in base s is represented as $0.Y$ (for some infinite sequence over Σ_s). It is unknown whether Y is always normal in base s, provided s is not a power of 10. The same applies if one considers Champernowne's sequence relative to a base r other than 10. However, it is known that the notion of normality is not base invariant [20].

We discuss a still stronger concept which, in contrast to the examples above, is defined directly for reals. A real x is *absolutely normal* if the following holds for any base r: if the representation in base r of the value $x - \lfloor x \rfloor$ is $0.X$ (for X an infinite sequence over Σ_r), then X is normal in base r. Of course this definition (transferred to sequences instead of reals) is trivially base invariant.

Although it is conjectured that irrationals such as π, e and $\sqrt{2}$ are absolutely normal, their normality has not been proved even for a single base. For now, all examples of absolutely normal numbers are artificial in that they have been specially introduced in order to prove their absolute normality. In [4] and [5] algorithms for constructing absolutely normal numbers are introduced, based on Sierpiński's [23] and Turing's [26] works, respectively. In both cases, the constructions are non-feasible. Recently, Becher, Heiber and Slaman [6] on the one hand, and Lutz and Mayordomo [15] on the other gave polynomial time constructions of absolutely normal numbers.

Let us move on to notions of randomness which are stronger and more robust than the aforementioned concepts. Robustness implies base invariance under base change. However, every notion so far required an ad-hoc proof of this fact.

Martin-Löf [18] viewed the notion of statistical test as a special kind of effective null class. The *law of large numbers* or *normality* can be formalized by such statistical tests. He defined an object to be random if it passes all such tests. Formally a *Martin-Löf test* in base r is a uniformly c.e. sequence $(G_m)_{m\in\mathbb{N}}$ of open sets over the alphabet Σ_r such that for all m, $\lambda_r G_m \leq r^{-m}$, where λ_r is the uniform measure which assigns $r^{-|\sigma|}$ to each basic open cylinder formed by all the infinite extensions of σ over the alphabet Σ_r. An infinite sequence Z over the alphabet Σ_r *passes* the Martin-Löf test $(G_m)_{m\in\mathbb{N}}$ if $Z \notin \bigcap_m G_m$, and X is *Martin-Löf random in base* r if X passes all Martin-Löf tests in base r.

Schnorr [21] gave a characterization of Martin-Löf randomness based on K, the prefix Kolmogorov complexity: X is Martin-Löf random iff all its prefixes are algorithmically incompressible. In formal terms, for an infinite sequence X over the alphabet Σ_r, X is Martin-Löf random in base r iff there is a constant c such that for all n, $K(X\upharpoonright_n) > n - c$. Here K is the prefix Kolmogorov complexity based on Turing machines over the alphabet Σ_r.

Calude and Jürgensen [10] showed that Martin-Löf randomness is base invariant via Martin-Löf tests, and Staiger [25] later gave a straightforward proof based on Schnorr's characterization via K. A completely different approach is the one followed by Hertling and Weihrauch [13]. Here a topological concept of randomness is given directly for reals (instead of representations of them), and then it is shown that this notion coincides with the classical definition of Martin-Löf randomness.

On the other hand, Brattka, Miller and Nies [8] showed results of the form: an infinite sequence Z over the alphabet $\{0,1\}$ is random according to the notion $\mathcal{R}$ iff each function in a given class (depending on $\mathcal{R}$) is differentiable at the real which in base 2 is represented as $0.Z$. One of the $\mathcal{R}$-notions they considered is that of computable randomness. Roughly, a sequence Z over the alphabet Σ_r is *computably random* [22, 21] if no computable betting strategy can succeed on Z. Here 'succeeding' means to gain, following the strategy, unbounded capital along Z by predicting the $(n+1)$-th symbol of Z, having the information of all the preceding n symbols of Z. The notion of a betting strategy is formalized by martingales (see §2 for the formal definition of computable randomness). The class of Martin-Löf random sequences is strictly contained in the class of computably random sequences. Brattka, Miller and Nies showed that an infinite binary sequence Z is computably random iff each computable nondecreasing function is differentiable at the real that is represented by $0.Z$ in base 2. Their methods show base invariance for computable randomness, grounded on a correspondence between martingales and nondecreasing functions (see §5 for more details).

Unlike Martin-Löf randomness, computable randomness can be naturally adapted to the resource (in particular, time) bounded setting. A sequence Z is *$t(n)$-random* if no rational valued martingale computable in time $O(t(n))$ succeeds on Z. (By a result of Schnorr, restricting to rational values is immaterial.) We say that Z is *polynomial time random* if Z is n^c-random for every c, that is, no polynomial time martingale succeeds on Z. Polynomial time random sequences have been studied for instance in [3], where some connections to Lutz's polynomial time bounded measure [16, 17] and polynomial genericity [1, 2] are discussed.

We discuss some examples showing the relevance of polynomial time randomness. Applied fields such as cryptography rely on pseudo-random generators, which produce a sequence of bits, yet the rule is hidden. The quality of such pseudo-random sequences is measured by comparing them to benchmark "truly random" sequences, and actually it suffices to take polynomial time random sequences. More generally, it turns out that for most practical applications, the notion of polynomial time randomness is sufficient, even though it is much weaker than computable randomness.

On the mathematical side, an informal notion of randomness for sequences of bits has been used in an essential way in work of Green and Tao [12] showing that the set of primes has arbitrarily long arithmetic progressions. Inspecting their proofs, one finds that, again, polynomial time randomness suffices.

Our main result is Theorem 14, which states that polynomial time randomness is base invariant (§6). To do this, we first need to state resource bounded versions of some known results about martingales (§2); in particular we study how to construct in an efficient way a betting strategy that does not make the capital grow too quickly. Then we study an efficient method for approximating the problem of base conversion for rationals (§4).

The key idea of the proof is to introduce a feasible version of the methods from effective analysis to prove base invariance for computable randomness [8]. In this way we convert a polynomial time betting strategy in a certain base into a polynomial time betting strategy in another base (§5).

Finally, using a result of Schnorr relating polynomial martingales with normal numbers, we give a polynomial construction of an absolutely normal real (§7).

2 Preliminaries

A *rational in base* r is a rational number with finite representation in base r, i.e. a rational of the form $z \cdot r^{-n}$, for some $z \in \mathbb{Z}$ and $n \in \mathbb{N}$. Let $\mathtt{Rat}_r$ be the set of rationals in base r and let $\mathtt{Rat}_r^{\geq 0}$ be the set of non-negative rationals in base r. $\mathbb{R}$ and $\mathbb{R}^{\geq 0}$ is the set of reals and non-negative reals respectively.

We denote Σ_r^*, Σ_r^n and Σ_r^ω the set of finite strings, strings of length n, and infinite sequences over the alphabet Σ_r, respectively. If $\sigma, \tau \in \Sigma_r^*$ then $\sigma^\frown\tau$ is the concatenation of σ and τ, $|\sigma|$ denotes the length of σ, and for $i \in \{0, \ldots, |\sigma| - 1\}$, the $(i+1)$-th symbol of σ is denoted $\sigma(i)$. We use the same notation in case $\sigma \in \Sigma_r^\infty$. By $\sigma \preceq \tau$ we denote that σ is a prefix of τ, and by $\sigma \prec \tau$ we denote that σ is a strict prefix of τ. We use the same notation in case $\tau \in \Sigma_r^\omega$. We define $[\sigma] = \{X \in \Sigma_r^\omega \colon \sigma \prec X\}$. For $X \in \Sigma_r^\omega$ we denote $X\restriction_n$ the string formed by the first n symbols of X, that is, $X(0), \ldots, X(n-1)$.

We represent $q \in \mathtt{Rat}_r$ by the pair $\langle \sigma, \tau \rangle$, where σ and τ are strings in Σ_r^* representing the integer and fractional part of q, respectively. If $p, q \in \mathtt{Rat}_r$ have both length n then $p + q$ can be calculated in time $O(n)$, and $p \cdot q$ can be calculated in time $O(n \cdot \log^2 n)$. Also, if $z \in \mathbb{Z}$ has length m then $p \cdot r^z$ can be calculated in time $O(n + m)$.

If $\sigma \in \Sigma_r^*$ then $\langle 0.\sigma \rangle_r$ represents the rational in $[0, 1]$ whose representation in base r is $0.\sigma$, i.e.

$$\langle 0.\sigma \rangle_r = \sum_{i=0}^{|\sigma|-1} \sigma(i) \cdot r^{-i-1}.$$

If $Z \in \Sigma_r^\omega$, then $\langle 0.Z \rangle_r$ represents the real in $[0, 1]$ whose expansion in base r is Z, i.e.

$$\langle 0.Z \rangle_r = \sum_{i \in \mathbb{N}} Z(i) \cdot r^{-i-1}.$$

The letter t will always denote a time bound such that $t(n) \geq n$.

Definition 1. *For $r \in \mathbb{N}$, $r > 1$, a* supermartingale in base r *is a function $M : \Sigma_r^* \to \mathbb{R}^{\geq 0}$ such that*

$$r \cdot M(\sigma) \geq \sum_{b \in \Sigma_r} M(\sigma^\frown b) \tag{3}$$

for all $\sigma \in \Sigma_r^*$. *A* martingale *is a supermartingale where we turn the inequality of equation (3) into an equality. M is a* $t(n)$-martingale in base r *if M is* $\mathtt{Rat}_r^{\geq 0}$*-valued and M is computable in deterministic time* $O(t(n))$.

We say that M succeeds *on $Z \in \Sigma_r^\omega$ iff* $\limsup_n M(Z\restriction_n) = \infty$. *A sequence $Z \in \Sigma_r^\omega$ is* $t(n)$-random in base r *if no $t(n)$-martingale in base r succeeds on Z. A sequence $Z \in \Sigma_r^\omega$ is* polynomial time random in base r *if for all $c \geq 1$, no n^c-martingale in base r succeeds on Z.*

Since we cannot process real numbers directly, we will approximate them.

Definition 2. *Let $M : \Sigma_r^* \to \mathbb{R}^{\geq 0}$. A computable function $\widehat{M} : \Sigma_r^* \times \mathbb{N} \to \mathtt{Rat}_r^{\geq 0}$ such that $|\widehat{M}(\sigma, i) - M(\sigma)| \leq r^{-i}$ is called a* computable approximation *of M. The complexity of $\widehat{M}$ on argument (σ, i) is measured in $|\sigma| + i$. A $t(n)$-computable approximation is a computable approximation which is computable in deterministic time $O(t(n))$.*

The following result is a generalization of [3, Lemma 2.1] to any base. It states that any real-valued supermartingale M which has a computable approximation $\widehat{M}$ can be transformed into a $\mathtt{Rat}_r$-valued supermartingale which succeeds on all the points M succeeds on, and has the same time complexity as $\widehat{M}$.

Lemma 3. *If M is a supermartingale in base r with a $t(n)$-computable approximation then there is a $t(n)$-supermartingale N in base r such that $N \geq M$.*

Proof. Let $\widehat{M}$ be a $t(n)$-computable approximation of M. Let N be the supermartingale defined as follows: $N(\sigma) = \widehat{M}(\sigma, |\sigma|) + r^2 \cdot r^{-|\sigma|}$. Since $\widehat{M}$ is $\mathtt{Rat}_r$-valued, it is clear that N also is. We have

$$M(\sigma) + (r^2 - 1) \cdot r^{-|\sigma|} \leq N(\sigma) \leq M(\sigma) + (r^2 + 1) \cdot r^{-|\sigma|}. \tag{4}$$

N is a supermartingale in base r because

$$\begin{aligned}
\sum_{b \in \Sigma_r} N(\sigma^\frown b) &\leq r \cdot (r^2 + 1) \cdot r^{-|\sigma|-1} + \sum_{b \in \Sigma_r} M(\sigma^\frown b) && \text{(by (4))} \\
&\leq r \cdot \left(\frac{r^2 + 1}{r} \cdot r^{-|\sigma|} + M(\sigma) \right) && (M \text{ is a supermartingale}) \\
&\leq r \cdot \Big((r^2 - 1) \cdot r^{-|\sigma|} + M(\sigma) \Big) && (\tfrac{r^2+1}{r} \leq r^2 - 1 \text{ for all } r \geq 2) \\
&\leq r \cdot N(\sigma). && \text{(by (4))}
\end{aligned}$$

Working in base r, the calculation of $r^2 \cdot r^{-|\sigma|} = r^{-|\sigma|+2}$ can be done in time $O(|\sigma|)$. Then $N(\sigma)$ is computed in time $O(|\sigma| + t(|\sigma|)) = O(t(|\sigma|))$. □

The following result is a generalization of [19, Proposition 7.1.6], due to Schnorr, to any base, together with an analysis of the time complexity. Roughly speaking, it says that one can dominate a computable $\mathtt{Rat}_r$-valued supermartingale by a computable $\mathtt{Rat}_r$-valued martingale with a linear loss in time complexity.

Lemma 4. *For every $t(n)$-supermartingale M in base r there is an $n \cdot t(n)$-martingale N in base r such that $N \geq M$.*

Proof. For $\sigma \in \Sigma_r^*$, let

$$d(\sigma) = M(\sigma) - r^{-1} \cdot \sum_{b \in \Sigma_r} M(\sigma^\frown b),$$

which is a non-negative rational in base r. Define

$$N(\sigma) = M(\sigma) + \sum_{\tau \prec \sigma} d(\tau),$$

which also is rational in base r. It is clear that $N \geq M$. We verify the martingale condition:

$$\begin{aligned}
\sum_{b \in \Sigma_r} N(\sigma^\frown b) &= r \cdot \sum_{\tau \preceq \sigma} d(\tau) + \sum_{b \in \Sigma_r} M(\sigma^\frown b) && \text{(def. of } N\text{)} \\
&= r \cdot d(\sigma) + r \cdot \sum_{\tau \prec \sigma} d(\tau) + \sum_{b \in \Sigma_r} M(\sigma^\frown b) \\
&= r \cdot \left(M(\sigma) + \sum_{\tau \prec \sigma} d(\tau) \right) && \text{(def. of } d\text{)} \\
&= r \cdot N(\sigma). && \text{(def. of } N\text{)}
\end{aligned}$$

Now $d(\sigma)$ is computable in time $O(t(|\sigma|))$, and so $N(\sigma)$ is computable in time $O(|\sigma| \cdot t(|\sigma|))$. □

3 The time bounded savings property

In general, if M is a supermartingale in base r then $M(\sigma) \leq M(\emptyset) \cdot r^{|\sigma|}$ for any $\sigma \in \Sigma_r^*$. This upper bound can, in fact, be reached for prefixes of a given sequence. For instance

$$M(\sigma) = \begin{cases} r^{|\sigma|} & \text{if all symbols of } \sigma \text{ are } 0 \\ 0 & \text{if } \sigma \text{ contains a symbol} > 0 \end{cases}$$

is a martingale in base r and $M(0^n) = r^n$ for any $n \geq 0$. So in general the capital that the player has following the strategy induced by M can rise (and drop) very fast. We will need to work with supermartingales that keep the player from increasing his capital very quickly.

We say that a supermartingale M in base r has the *savings property* if there is $c > 0$ such that for all $\tau, \sigma \in \Sigma_r^*$, if $\tau \succeq \sigma$ then $M(\sigma) - M(\tau) \leq c$.

While a general supermartingale $M(\sigma)$ can grow exponentially in the length of σ, one with the savings property can only grow linearly.

Proposition 5. *Suppose M is a supermartingale in base r with the savings property via c. Then for all $\sigma \in \Sigma_r^*$ we have $M(\sigma) \leq (r-1) \cdot c \cdot |\sigma| + M(\emptyset)$.*

Proof. We proceed by induction on the length of σ. For $\sigma = \emptyset$ it is straightforward. For the inductive step,

$$\begin{aligned}
M(\sigma^\frown b) &\leq r \cdot M(\sigma) - \sum_{d \in \Sigma_r, d \neq b} M(\sigma^\frown d) && (M \text{ is a supermartingale}) \\
&\leq r \cdot M(\sigma) - (r-1) \cdot (M(\sigma) - c) && (M \text{ has the savings property}) \\
&= (r-1) \cdot c + M(\sigma) \\
&\leq (r-1) \cdot c + (r-1) \cdot c \cdot |\sigma| + M(\emptyset) && \text{(by the inductive hypothesis)} \\
&= (r-1) \cdot c \cdot |\sigma^\frown b| + M(\emptyset).
\end{aligned}$$

This concludes the proof. □

The following result on savings property is folklore for the case of computable martingales (for a published reference, see [8]). Here we give a time bounded version.

Lemma 6 (Time bounded savings property)**.** *For each $t(n)$-[super]martingale L in base r there is an $n \cdot t(n)$-[super]martingale M in base r which has the savings property and succeeds on all the sequences that L succeeds on.*

Proof. Let m be such that $L(\emptyset) \leq r^m$ and define $L'(\sigma) = L(\sigma)/r^m$. It is clear that L' is a $t(n)$-martingale in base r, $L'(\emptyset) \leq 1$ and L' succeeds on the same sequences as L. Then without loss of generality we assume that $L(\emptyset) \leq 1$.

Let $E(\emptyset) = L(\emptyset)$, $G(\emptyset) = 0$. For each $b \in \Sigma_r$ and $\sigma \in \Sigma_r^*$, let

$$\begin{aligned}
\alpha_b(\sigma) &= L(\sigma^\frown b) \cdot E(\sigma)/L(\sigma) \\
E(\sigma^\frown b) &= \begin{cases} \alpha_b(\sigma)/r & \text{if } \alpha_b(\sigma) > r \\ \alpha_b(\sigma) & \text{otherwise} \end{cases} \\
G(\sigma^\frown b) &= \begin{cases} G(\sigma) + \alpha_b(\sigma) \cdot (r-1)/r & \text{if } \alpha_b(\sigma) > r \\ G(\sigma) & \text{otherwise} \end{cases}
\end{aligned}$$

It can be shown by induction on the length of σ that both E and G are $\mathtt{Rat}_r^{\geq 0}$-valued, and that $E(\sigma) \leq r$ (since $L(\sigma^\frown b)/L(\sigma) \leq r$). Define $M : \Sigma_r^* \to \mathtt{Rat}_r^{\geq 0}$ as $M = E + G$. It is straightforward that $M(\sigma^\frown b) = E(\sigma^\frown b) + G(\sigma^\frown b) = \alpha_b(\sigma) + G(\sigma)$. So if L is a martingale [resp. supermartingale] then $\sum_{b \in r} M(\sigma^\frown b) = r \cdot M(\sigma)$ [resp. $\sum_{b \in r} M(\sigma^\frown b) \leq r \cdot M(\sigma)$]. For every $\tau \succeq \sigma$, $G(\tau) \geq G(\sigma)$ and hence $M(\sigma) - M(\tau) \leq E(\sigma) - E(\tau) \leq E(\sigma) \leq r$, so $M : \Sigma_r^* \to \mathtt{Rat}_r^{\geq 0}$ is a [super]martingale in base r with the savings property via r.

Both E and G (and hence M) have a recursive definition. To calculate the complexity bound for computing $M(\sigma)$, we first unravel the definitions of $E(\sigma)$ and $G(\sigma)$. To do so, we need to identify the prefixes $\tilde{\sigma}^\frown b$ of σ where $\alpha_b(\tilde{\sigma}) > r$.

Let $\sigma \in \Sigma_r^n$ and let I_σ be the sequence $i_1 < \cdots < i_{k_\sigma}$ such that i_j is the length of the j-th prefix $\tilde{\sigma}^\frown b$ of σ which makes $\alpha_b(\tilde{\sigma})$ go beyond r. More formally, I_σ is the maximal sequence $i_1 < \cdots < i_{k_\sigma}$ such that for all $j = 1, \ldots, k_\sigma$ we have $0 \leq i_j < n$ and $\alpha_{\sigma(i_j)}(\sigma \restriction_{i_j}) > r$.

Fact 7. $E(\sigma) = L(\sigma)/r^{k_\sigma}$ and $G(\sigma) = (r-1) \cdot \sum_{j=1}^{k_\sigma} L(\sigma \restriction_{i_j+1})/r^j$.

Proof. By induction in n. If $n = 0$ then it is clear that $k_\sigma = 0$ and then $E(\emptyset) = L(\emptyset)$ and $G(\emptyset) = 0$. For the induction, suppose $\sigma = \tilde{\sigma}^\frown b \in \Sigma_r^{n+1}$, where $b \in r$.

If $\alpha_b(\tilde{\sigma}) \leq r$ then $I_{\tilde{\sigma}} = I_\sigma$, so $k_{\tilde{\sigma}} = k_\sigma$. On the one hand,

$$\begin{aligned}
E(\sigma) &= L(\sigma) \cdot E(\tilde{\sigma})/L(\tilde{\sigma}) && \text{(def. of } E\text{)} \\
&= L(\sigma)/r^{k_{\tilde{\sigma}}} && \text{(ind. hyp.)} \\
&= L(\sigma)/r^{k_\sigma}. && (k_{\tilde{\sigma}} = k_\sigma)
\end{aligned}$$

On the other hand,

$$\begin{aligned}
G(\sigma) &= G(\tilde{\sigma}) && \text{(def. of } G\text{)} \\
&= (r-1) \cdot \sum_{j=1}^{k_\sigma} L(\sigma \restriction_{i_j+1})/r^j. && \text{(ind. hyp., } k_{\tilde{\sigma}} = k_\sigma \text{ and } \tilde{\sigma} \prec \sigma\text{)}
\end{aligned}$$

If $\alpha_b(\tilde{\sigma}) > r$ then $I_\sigma = i_1 < \cdots < i_{k_{\tilde{\sigma}}} < i_{k_\sigma}$, where $k_\sigma = k_{\tilde{\sigma}} + 1$ and $i_{k_\sigma} = n$. On the one hand,

$$\begin{aligned} E(\sigma) &= \frac{L(\sigma) \cdot E(\tilde{\sigma})}{r \cdot L(\tilde{\sigma})} && \text{(def. of } E\text{)} \\ &= L(\sigma)/r^{k_{\tilde{\sigma}}+1} && \text{(ind. hyp.)} \\ &= L(\sigma)/r^{k_\sigma}. && (k_{\tilde{\sigma}} + 1 = k_\sigma) \end{aligned}$$

On the other hand,

$$\begin{aligned} G(\sigma) &= (r-1) \cdot L(\sigma)/r^{k_{\tilde{\sigma}}+1} + G(\tilde{\sigma}) && \text{(def. of } G\text{)} \\ &= (r-1) \cdot L(\sigma)/r^{k_{\tilde{\sigma}}+1} + (r-1) \cdot \sum_{j=1}^{k_{\tilde{\sigma}}} L(\sigma \restriction_{i_j+1})/r^j && \text{(ind. hyp. and } \tilde{\sigma} \prec \sigma\text{)} \\ &= (r-1) \cdot \sum_{j=1}^{k_\sigma} L(\sigma \restriction_{i_j+1})/r^j. && (k_{\tilde{\sigma}} + 1 = k_\sigma\text{; also } i_{k_\sigma} = n\text{, so } \sigma \restriction_{i_{k_\sigma}+1} = \sigma) \end{aligned}$$

This concludes the proof of Fact 7. □

Since i_j is the least i such that $L(\sigma \restriction_{i+1}) > r^j$, one can compute I_σ in time $O(n \cdot t(n))$. By Fact 7 we can compute $E(\sigma) \in \mathtt{Rat}_r$ and $G(\sigma) \in \mathtt{Rat}_r$ in time $O(n \cdot t(n))$. We conclude that M is an $n \cdot t(n)$-[super]martingale in base r.

Finally, if L succeeds on $Z \in \Sigma_r^\omega$ then $\lim_n k_{Z\restriction_n} = \infty$. Since

$$G(Z \restriction_n) \geq \sum_{j=1}^{k_{Z\restriction_n}} L(Z \restriction_{i_j+1})/r^j$$

and $L(Z \restriction_{i_j+1}) > r^j$ we have $G(Z \restriction_n) > k_{Z\restriction_n}$ and hence $\limsup_n G(Z \restriction_n) = \infty$. Then M succeeds on Z. □

4 Base conversion with small error

Given arbitrarily long prefixes of the fractional expansion of a given real in base s does not allow us to effectively determine a prefix of the fractional expansion of the same real represented in base r. Indeed, there are bases s and r for which there is no functional $\Gamma : \mathbb{N} \to \Sigma_r$ such that for $X \in \Sigma_s^\omega$, $Y \in \Sigma_r^\omega$ Γ^X is total and if $\langle 0.X\rangle_s = \langle 0.Y\rangle_r$ then $\Gamma^X = Y$. For instance, take $s = 3$ and $r = 2$. Observe that $\langle 0.1^\infty\rangle_3 = 1/2$ and for every $k \in \mathbb{N}$, $\langle 0.1^k 0\rangle_3 < 1/2$ and $\langle 0.1^k 2\rangle_3 > 1/2$. If there was such a functional then for some k we would have $\Gamma^{1^k}(0) \downarrow \in \Sigma_2$ and for all $\tau \in \Sigma_3^*$ $\Gamma^{1^k\tau}(0) = \Gamma^{1^k}(0)$. If $\Gamma^{1^k}(0) = 0$ then $\Gamma^{1^k 2}(0) = 0$ but $\langle 0.\Gamma^{1^k 2}\rangle_2 > 1/2$ and this is a contradiction. Analogously, if $\Gamma^{1^k}(0) = 1$ then $\Gamma^{1^k 0}(0) = 1$ but $\langle 0.\Gamma^{1^k 0}\rangle_2 < 1/2$, which is also a contradiction. Hence in this case we are unable to effectively determine the first bit of Y.

However, we can approximate a rational in base s with a rational in base r within a given error. For $\tau \in \Sigma_s^*$ and $i \in \mathbb{N}$, let $\mathsf{bc}_{s,r}^-(\tau, i)$ be the string σ in Σ_r^* of minimal length such that

$$0 \leq \langle 0.\tau\rangle_s - \langle 0.\sigma\rangle_r < r^{-i}, \tag{5}$$

Algorithm 1: Simple approximation of a rational in base s with a rational in base r

input : $\tau \in \Sigma_s^*$ and $i \in \mathbb{N}$
output: $\sigma \in \Sigma_r^*, \sigma = \mathsf{bc}^-_{s,r}(\tau, i)$

$\sigma := \emptyset$
while $\langle 0.\tau\rangle_s - \langle 0.\sigma\rangle_r > r^{-i}$ **do**
  Find the largest $x \in \Sigma_r$ such
    that $\langle 0.\sigma^\frown x\rangle_r \leq \langle 0.\tau\rangle_s$
  $\sigma := \sigma^\frown x$

Algorithm 2: Efficient approximation of a rational in base s with a rational in base r

input : $\tau \in \Sigma_s^*$ and $i \in \mathbb{N}$
output: $\sigma \in \Sigma_r^*, \sigma = \mathsf{bc}^-_{s,r}(\tau, i)$

$a := \sum_{i=0}^{|\tau|-1} s^{|\tau|-i-1} \cdot \tau(i)$ and $b := s^{|\tau|}$
$\sigma := \emptyset$
$c := 0$ and $d := 1$
while $\frac{c}{d} < \frac{a}{b} - r^{-i}$ **do**
  invariant $\frac{a}{b} = \langle 0.\tau\rangle_s$; $\frac{c}{d} = \langle 0.\sigma\rangle_r$
  Find the largest $x \in \Sigma_r$ such that $\frac{c\cdot r + x}{d \cdot r} \leq \frac{a}{b}$
  $\sigma := \sigma^\frown x$
  $c := c \cdot r + x$
  $d := d \cdot r$

and let $\mathsf{bc}^+_{s,r}(\tau, i)$ be the string σ in Σ_r^* of minimal length such that

$$0 \leq \langle 0.\sigma\rangle_r - \langle 0.\tau\rangle_s < r^{-i}.$$

Let $X \in \Sigma_s^\omega$ and $Y \in \Sigma_r^\omega$ be such that $\langle 0.X\rangle_s = \langle 0.Y\rangle_r$. The fact that $\mathsf{bc}^-_{s,r}(X \restriction_n, i) = \sigma$ does not imply that $\sigma \prec Y$. For instance, take $X = 12\ldots$, $s = 3$, $r = 2$ and $i = 2$. One can verify that $\mathsf{bc}^-_{s,r}(X \restriction_1, i) = 01$ though $Y \restriction_1 = 1$ because $\langle 0.Y\rangle_r > 1/2$. Of course, the same happens to $\mathsf{bc}^+_{s,r}$. It is worth mentioning that Staiger [25, Remark on p. 461] provides a different approach to base conversion. He defines a function $h : \Sigma_s^* \to \Sigma_r^* \times \Sigma_r^*$ such that if $h(X \restriction_n) = (\sigma_n^1, \sigma_n^2)$ then either $\sigma_n^1 \prec Y$ or $\sigma_n^2 \prec Y$. Furthermore, the length of each σ_i^n increases with n. This function h can be seen as a non-deterministic (more precisely, two–valued) conversion from reals in base r to reals in base s.

Observe that the length of $\mathsf{bc}^+_{s,r}(\tau, i)$ is at most i, and the same for $\mathsf{bc}^-_{s,r}(\tau, i)$. The time complexity of $\mathsf{bc}^+_{s,r}$ or $\mathsf{bc}^-_{s,r}$ on argument (τ, i) is measured in $n = |\tau| + i$.

Theorem 8. *$\mathsf{bc}^-_{s,r}$ and $\mathsf{bc}^+_{s,r}$ are computable in time $O(n^2)$.*

Proof. We show the result for $\mathsf{bc}^-_{s,r}$; the case for $\mathsf{bc}^+_{s,r}$ is analogous. Observe that by definition, $|\mathsf{bc}^-_{s,r}(\tau, i)| \leq i$. In Algorithm 1 we introduce a simple procedure to determine $\sigma = \mathsf{bc}^-_{s,r}(\tau, i)$.

It is clear that Algorithm 1, computes $\sigma = \mathsf{bc}^-_{s,r}(\tau, i)$. Since $|\sigma| \leq i$, the main loop is carried out at most i many times. To determine a better time complexity, in Algorithm 2 we refine the procedure. We use representations in base r to store the values of the integer variables a, b, c and d, and to calculate the arithmetic operations. The value of $\langle 0.\sigma\rangle_r$ is represented as a fraction $\frac{a}{b}$, which is constant along the execution. The successive approximations of $\langle 0.\sigma\rangle_r$ are represented as a fraction $\frac{c}{d}$, where d is always a power of r. Each time σ is extended by a new symbol of Σ_r, the values of c and d are adequately updated to maintain the invariant $\langle 0.\sigma\rangle_r = \frac{a}{b}$.

We can initially compute a and b in time $O(n)$. The loop condition involves the value $\frac{a}{b} - r^{-i}$, which is constant and can be computed (just once) in time $O(n)$. As in Algorithm 1, the main loop is carried out at most i times. The sizes of the variables c and d during the computation are $O(i)$. Hence the comparison $\frac{c}{d} < \frac{a}{b} - r^{-i}$, as well as the comparison $\frac{c\cdot r + x}{d \cdot r} \leq \frac{a}{b}$ can be carried out in time $O(n)$. We conclude that the algorithm runs in time $O(n^2)$. □

5 Martingales and base conversion

In this section we follow [8]. In §5.1 we introduce the background needed, and in §5.2 we show how to efficiently compute a key function depending on a given martingale.

5.1 Background

Each martingale M in base r induces a measure μ_M on the algebra of clopen sets defined by

$$\mu_M([\sigma]) = \frac{M(\sigma)}{r^{|\sigma|}},$$

for $\sigma \in \Sigma_r^*$. Via Carathéodory's extension theorem this measure can be extended to a Borel measure on Cantor space, and if μ_M is atomless (i.e. no point has positive measure), we can also think of it as a Borel measure on $[0,1]$. Under this view, μ_M is determined by

$$\mu_M(I_\sigma^r) = \frac{M(\sigma)}{r^{|\sigma|}}, \tag{6}$$

where for any $\sigma \in \Sigma_r^*$ we define

$$I_\sigma^r = \left[\langle 0.\sigma\rangle_r, \langle 0.\sigma\rangle_r + r^{-|\sigma|}\right].$$

We say that a martingale is *atomless* if μ_M is atomless. Observe that if M has the savings property then it is atomless. Indeed, suppose M has the savings property via c. By Proposition 5, for any $\sigma \in \Sigma_r^n$ we have $\mu_M(I_\sigma^r) \leq r^{-n} \cdot ((r-1)\cdot c \cdot n + M(\emptyset))$ and this goes to 0 as n goes to infinity. Hence μ_M is atomless.

In [8] Brattka, Miller and Nies begin by recalling the well-known correspondence between atomless martingales and nondecreasing continuous functions. The cumulative distribution function associated with μ_M, denoted by $\mathsf{cdf}_M(x) : [0,1] \to [0,1]$, is defined as follows:

$$\mathsf{cdf}_M(x) = \mu_M([0,x)). \tag{7}$$

It can be shown that if M is atomless then cdf_M is nondecreasing and continuous. If f is a nondecreasing function with domain containing $[0,1]\cap\mathbb{Q}$ and s is a base then $\mathsf{mart}_f^s : \Sigma_s^* \to \mathbb{R}$ is defined as follows:

$$\mathsf{mart}_f^s(\tau) = \frac{f(\langle 0.\tau\rangle_s + s^{-|\tau|}) - f(\langle 0.\tau\rangle_s)}{s^{-|\tau|}}.$$

It can also be shown that mart_f^s is a martingale in base s.

We will use two results of [8]. One is the relationship between the functions cdf and mart:

Proposition 9 ([8, Fact 3.5])**.** *Let s be a base and let f be a nondecreasing continuous function on $[0,1]$ such that $f(0) = 0$. Then $\mathsf{cdf}_{\mathsf{mart}_f^s} = f$.*

The second result is the following characterization:

Theorem 10 ([8, Theorem 3.6])**.** *Suppose M is a martingale in base r with the savings property, and $z \in [0,1]$ is not a rational in base r. Then M succeeds on the r-ary expansion of z iff*

$$\liminf_{h\to 0} \frac{\mathsf{cdf}_M(z+h) - \mathsf{cdf}_M(z)}{h} = \infty. \tag{8}$$

(Note that the above expression is $\underline{D}\mathsf{cdf}_M(z)$, the lower derivative at z.)

These results yield the following lemma, which, in a slightly different formulation, was used in [8, Theorem 3.7] to prove that computable randomness is base invariant. In §6 we will use it to show that polynomial time random is base invariant.

Lemma 11. *Let r and s be bases and suppose M is a martingale in base r with the savings property. Let $N : \Sigma_s^* \to \mathbb{R}^{\geq 0}$ be the following martingale in base s:*

$$N(\tau) = \mathsf{mart}^s_{\mathsf{cdf}_M}(\tau) = \frac{\mathsf{cdf}_M(\langle 0.\tau\rangle_s + s^{-|\tau|}) - \mathsf{cdf}_M(\langle 0.\tau\rangle_s)}{s^{-|\tau|}}. \tag{9}$$

Suppose $X \in \Sigma_r^\omega$ and $Y \in \Sigma_s^\omega$ are such that $\langle 0.X\rangle_r$ is not a rational in base r, $\langle 0.Y\rangle_s$ is not a rational in base s, and $\langle 0.X\rangle_r = \langle 0.Y\rangle_s$. If M succeeds on X then N succeeds on Y.

Proof. Let $z = \langle 0.X\rangle_r = \langle 0.Y\rangle_s$. Since z is neither a rational in base r nor a rational in base s, $X \in \Sigma_r^\omega$ and $Y \in \Sigma_s^\omega$ are unique. If M succeeds on X, by the left-to-right implication of Theorem 10 applied to M and z, we have that condition (8) is true for M. Observe that $f = \mathsf{cdf}_M$ is nondecreasing, continuous and $f(0) = 0$. By Proposition 9, $\mathsf{cdf}_N = \mathsf{cdf}_M$ and so condition (8) is also true for N instead of M. By the right-to-left implication of Theorem 10 applied to N and z, we conclude that N succeeds on Y. □

5.2 Computing the cumulative distribution function

We analyze the time complexity of computing cdf_M when M is a martingale in base r with the savings property. The value of $\mathsf{cdf}_M(x)$ is defined for reals $x \in [0,1]$, but for our purposes it suffices to compute cdf_M restricted to $\mathtt{Rat}_r$. By the definition of cdf_M we have that $\mathsf{cdf}_M \restriction \mathtt{Rat}_r$ is a function $[0,1] \cap \mathtt{Rat}_r \to \mathtt{Rat}_r$.

We first show that if M has the savings property then cdf_M satisfies an 'almost Lipschitz' condition.

Proposition 12. *Let M be a martingale in base r with the savings property. Then there are constants $k, \epsilon > 0$ such that for every $x, y \in [0,1]$, if $y - x \leq \epsilon$ then*

$$\mathsf{cdf}_M(y) - \mathsf{cdf}_M(x) \leq -k \cdot (y-x) \cdot \log(y-x).$$

Proof. We actually show the following. If M has the savings property via c then for $0 \leq x < y \leq 1$ we have

$$\mathsf{cdf}_M(y) - \mathsf{cdf}_M(x) \leq (r+1) \cdot (y-x) \cdot ((r-1) \cdot c \cdot (1 - \log_r(y-x)) + M(\emptyset)).$$

Let $n \in \mathbb{N}$ be the least such that $r^{-n} < y - x$, and let p be the least rational of the form $p = i \cdot r^{-n}$ such that $x \leq p + r^{-n}$. Let q be the minimum between 1 and $(i + r + 1) \cdot r^{-n}$.

Suppose $q = (i + r + 1) \cdot r^{-n} < y$. Then $y - x > (i + r + 1) \cdot r^{-n} - (i+1)r^{-n} = r^{-(n-1)}$ and this contradicts the choice of n. Then $y \leq q$, and hence $[x, y] \subseteq [p, q]$. Now

$$\begin{aligned}
\mathsf{cdf}_M(y) - \mathsf{cdf}_M(x) &\leq \mathsf{cdf}_M(q) - \mathsf{cdf}_M(p) \\
&= \mu_M[p, q] && \text{(by (7))} \\
&= \sum_{j=0}^{\min(r, r^n - i - 1)} \mu_M([(i+j) \cdot r^{-n}, (i+j+1) \cdot r^{-n}]) \\
&\leq (r+1) \cdot r^{-n} \cdot ((r-1) \cdot c \cdot n + M(\emptyset)).
\end{aligned}$$

The last inequality stems from the fact that each term in the sum is of the form $r^{-n} \cdot M(\sigma)$ for some $\sigma \in \Sigma_r^n$. Since M has the savings property, by Proposition 5, each such term is at most $r^{-n} \cdot ((r-1) \cdot c \cdot n + M(\emptyset))$.

Since $r^{-(n-1)} \geq y - x$, we have $n \leq 1 - \log_r(y-x)$, and since $r^{-n} \leq y - x$, this yields the required inequality. □

Lemma 13. *Let M be a $t(n)$-martingale in base r with the savings property. Then cdf_M restricted to rationals in base r is a rational in base r. Also, if $\langle 0.\sigma\rangle_r$ ($\sigma \in \Sigma_r^n$) is a rational in base r, one can compute the r-ary representation of $\mathsf{cdf}_M(\langle 0.\sigma\rangle_r)$ in time $O(n \cdot t(n))$.*

Proof. If $\sigma \in \Sigma_r^n$ then, according to the condition (6) over μ_M we have

$$\begin{aligned}
\mathsf{cdf}_M(\langle 0.\sigma\rangle_r) &= \mu_M([0, \langle 0.\sigma\rangle_r]) \\
&= \sum_{i=0}^{n-1} \sum_{b=0}^{\sigma(i)-1} \mu_M(I^r_{(\sigma\restriction_i)^\frown b}) \\
&= \sum_{i=0}^{n-1} \sum_{b=0}^{\sigma(i)-1} \frac{M((\sigma\restriction_i)^\frown b)}{r^{i+1}} \\
&= \sum_{i=0}^{n-1} r^{-i-1} \cdot h(i),
\end{aligned}$$

where

$$h(i) = \sum_{b=0}^{\sigma(i)-1} M((\sigma\restriction_i)^\frown b).$$

It is clear that $h(i)$ is computable in time $O(t(i+1))$ using r-ary representation for the output. On the other hand, $\sum_{i=0}^{n-1} r^{n-i-1} \cdot h(i)$ can be computed in time $O(n \cdot t(n))$. We conclude that cdf_M is computable in time $O(n \cdot t(n))$. □

6 Polynomial time randomness is base invariant

In this section we show our main result: polynomial time randomness is base invariant. Through a different argument and without the analysis of the time complexity, a preliminary version of this result can be found in [24].

Theorem 14. *Let $k \geq 1$. If $Y \in \Sigma_s^\omega$ is n^{k+3}-random in base s and $X \in \Sigma_r^\omega$ is such that $\langle 0.X\rangle_r = \langle 0.Y\rangle_s$ then X is n^k-random in base r. In particular, polynomial time randomness is base invariant.*

Proof. We will actually show the following stronger result.

> Suppose t is a time function such that $t(O(n)) = O(t(n))$, that is, for every $c > 0$ there is d such that $t(c \cdot n) \leq d \cdot t(n)$ for every n. If $Y \in \Sigma_s^\omega$ is $t(n) \cdot n^3$-random in base s and $X \in \Sigma_r^\omega$ is such that $\langle 0.X\rangle_r = \langle 0.Y\rangle_s$, then X is $t(n)$-random in base r.

This implies the statement of the theorem by letting $t(n) = n^k$. Observe that any function t with $t(O(n)) = O(t(n))$ is bounded by a polynomial.

If $\langle 0.Y\rangle_r$ is rational then Y is eventually periodic and hence computable in linear time. Define $N : \Sigma_s^* \to \mathtt{Rat}_s^+$ as follows:

$$N(\tau) = \begin{cases} s^{|\tau|} & \text{if } \tau \prec Y \\ 0 & \text{otherwise} \end{cases}$$

It can be shown that N satisfies the martingale condition in base s and that N is computable in linear time, so Y is not $t(n) \cdot n^3$-random. Hence the statement is trivially true when $\langle 0.Y\rangle_r$ is rational. Assume, then, that $\langle 0.Y\rangle_s = \langle 0.X\rangle_r$ is irrational.

For F a martingale in base r and G a martingale in base s, we say that G is an *r to s base conversion* of F in case the following holds: if F succeeds on $X \in \Sigma_r^\omega$, and $Y \in \Sigma_s^\omega$ is such that $\langle 0.X\rangle_r = \langle 0.Y\rangle_s$ is irrational, then G succeeds on Y. The main lemma is the following.

Lemma 15. *Let t be a time function such that $t(O(n)) \in O(t(n))$. For any $t(n)$-martingale M in base r with the savings property there is a (real-valued) martingale N in base s such that N is an r to s base conversion of M, and N has an $n \cdot t(n)$-computable approximation.*

Assuming the lemma, we proceed by contradiction. Suppose that X is not $t(n)$-random in base r. Let M be a $t(n)$-martingale in base r which succeeds on X. Then by Lemma 6 there is an $n \cdot t(n)$-martingale $\widetilde{M}$ in base r with the savings property that succeeds on all the sequences M succeeds on, in particular on X. By Lemma 15 and Lemma 3 there is an $n^2 \cdot t(n)$-supermartingale in base s which is a base conversion of $\widetilde{M}$, so in particular $\widetilde{M}$ succeeds on Y. By Lemma 4. there is an $n^3 \cdot t(n)$-martingale in base s which succeeds on Y, and then Y is not $n^3 \cdot t(n)$-random. This establishes the theorem.

Proof of Lemma 15. Without loss of generality, we assume $M(\emptyset) \leq 1$. Let $X \in \Sigma_r^\omega$ and $Y \in \Sigma_s^\omega$ be such that $z = \langle 0.X\rangle_r = \langle 0.Y\rangle_s$ is irrational. We show that if M succeeds on X then there is a martingale N in base s which succeeds on Y and has an $n \cdot t(n)$-computable approximation.

Define the real martingale $N : \Sigma_s^* \to \mathbb{R}^{\geq 0}$, in base s, as in (9):

$$N(\tau) = s^{|\tau|} \cdot (\mathsf{cdf}_M(q) - \mathsf{cdf}_M(p)),$$

where $p = \langle 0.\tau\rangle_s$ and $q = \langle 0.\tau\rangle_s + s^{-|\tau|}$. Observe that neither $\langle 0.X\rangle_r$ nor $\langle 0.Y\rangle_s$ are rationals in base r or s. By Lemma 11, N succeeds on Y.

The rest of the proof is devoted to showing that N has an $n \cdot t(n)$-computable approximation. To compute the value of $N(\tau)$, we need to calculate $\mathsf{cdf}_M(q)$ and $\mathsf{cdf}_M(p)$. By Lemma 13 we know how to efficiently compute $\mathsf{cdf}_M(x)$, when x is a rational in base r. Since p and q are rationals in base s, we first need to approximate them with rationals $\widetilde{p}$ and $\widetilde{q}$ in base r that are sufficiently close to p and q respectively. To do this, we use the s to r base conversion functions $\mathsf{bc}_{s,r}^-$ and $\mathsf{bc}_{s,r}^+$ introduced in §4. Then we approximate $\mathsf{cdf}_M(p)$ with $\mathsf{cdf}_M(\widetilde{p})$ and $\mathsf{cdf}_M(q)$ with $\mathsf{cdf}_M(\widetilde{q})$. We will use the 'almost Lipschitz' condition of Proposition 12 to show that these are good approximations. Since N has to be approximated by rationals in base s but $\mathsf{cdf}_M(\widetilde{p})$ and $\mathsf{cdf}_M(\widetilde{q})$ are rationals in base r, we finally approximate them with rationals in base s using the r to s base conversion functions $\mathsf{bc}_{r,s}^-$ and $\mathsf{bc}_{r,s}^+$.

Here are the details of the construction. Let $k > 0$ be such that $r \leq s^k$ and for every $x, y \in [0,1]$, if $y - x \leq r^{-k}$ then

$$\mathsf{cdf}_M(y) - \mathsf{cdf}_M(x) \leq -r^k \cdot (y-x) \cdot \log(y-x). \tag{10}$$

The existence of k is guaranteed by Proposition 12. Given $\tau \in \Sigma_s^*$ and $i \in \mathbb{N}$, define

$$v = k \cdot (i + |\tau| + 3) + k.$$

Step 1. *Approximating p with $\widetilde{p}$ and q with $\widetilde{q}$.* Let $\widetilde{\tau}^- \in \Sigma_r^*$ and $\widetilde{p} \in \mathtt{Rat}_r \cap [0,1]$ be defined by $\widetilde{\tau}^- = \mathsf{bc}^-_{s,r}(\tau, 2v+1)$ and $\widetilde{p} = \langle 0.\widetilde{\tau}^- \rangle_r$. If $q < 1$ and $\tau^+ \in \Sigma_s^{|\tau|}$ is such that $q = \langle 0.\tau^+ \rangle_s$, then let $\widetilde{\tau}^+ = \mathsf{bc}^+_{s,r}(\tau^+, 2v+1)$, and let $\widetilde{q} \in \mathtt{Rat}_r \cap [0,1]$ be defined by $\widetilde{q} = \langle 0.\widetilde{\tau}^+ \rangle_r$. If $q = 1$, let $\widetilde{q} = 1$. Note that $\widetilde{p} \leq p < q \leq \widetilde{q}$.

Step 2. *Approximating $\mathsf{cdf}_M(q) - \mathsf{cdf}_M(p)$ with $\mathsf{cdf}_M(\widetilde{q}) - \mathsf{cdf}_M(\widetilde{p})$.*
Fact 16. $0 \leq \mathsf{cdf}_M(p) - \mathsf{cdf}_M(\widetilde{p}) \leq s^{-(i+|\tau|+3)}$ and $0 \leq \mathsf{cdf}_M(\widetilde{q}) - \mathsf{cdf}_M(q) \leq s^{-(i+|\tau|+3)}$.

Proof. Let $\delta = p - \widetilde{p}$ and let $\epsilon = r^{-v}$. Since $\delta < \epsilon^2/r \leq \epsilon^2/2$ then $\frac{\epsilon}{2\delta} > \frac{1}{\epsilon} > -\log \epsilon$. For all z, $\frac{z}{2} > \log z$, and then $\frac{\epsilon}{\delta} - \log \frac{\epsilon}{\delta} > \frac{\epsilon}{2\delta} > -\log \epsilon$, so $\frac{\epsilon}{\delta} > \log \frac{\epsilon}{\delta} - \log \epsilon = -\log \delta$. Therefore $-\delta \cdot \log \delta < \epsilon$ and by the 'almost Lipschitz' condition (10) and the fact that $\delta \leq r^{-k}$ we conclude

$$\begin{aligned}
\mathsf{cdf}_M(p) - \mathsf{cdf}_M(\widetilde{p}) &\leq -r^k \cdot \delta \cdot \log \delta \\
&< r^k \cdot \epsilon \\
&= r^{-k \cdot (i+|\tau|+3)} \\
&\leq s^{-(i+|\tau|+3)}. && (r^k \geq s)
\end{aligned}$$

The argument for q and $\widetilde{q}$ is analogous. □

Let $D = \mathsf{cdf}_M(\widetilde{q}) - \mathsf{cdf}_M(\widetilde{p}) \in \mathtt{Rat}_r \cap [0,1]$. It is clear that $D \geq \mathsf{cdf}_M(q) - \mathsf{cdf}_M(p)$ and from Fact 16 we conclude $D - (\mathsf{cdf}_M(q) - \mathsf{cdf}_M(p)) \leq 2 \cdot s^{-(i+|\tau|+3)} \leq s^{-(i+|\tau|+2)}$. Let $\rho \in \Sigma_r^*$ be such that $D = \langle 0.\rho \rangle_r$. For complexity issues, we next shorten the r-ary representation of D. Let

$$D' = \langle 0.(\rho \restriction_{k \cdot (i+|\tau|+2)}) \rangle_r \in \mathtt{Rat}_r.$$

Since $0 \leq D - D' \leq r^{-k \cdot (i+|\tau|+2)} \leq s^{-(i+|\tau|+2)}$, then we have

$$|D' - (\mathsf{cdf}_M(q) - \mathsf{cdf}_M(p))| \leq s^{-(i+|\tau|+1)}. \tag{11}$$

Figure 1 illustrates Steps 1 and 2.

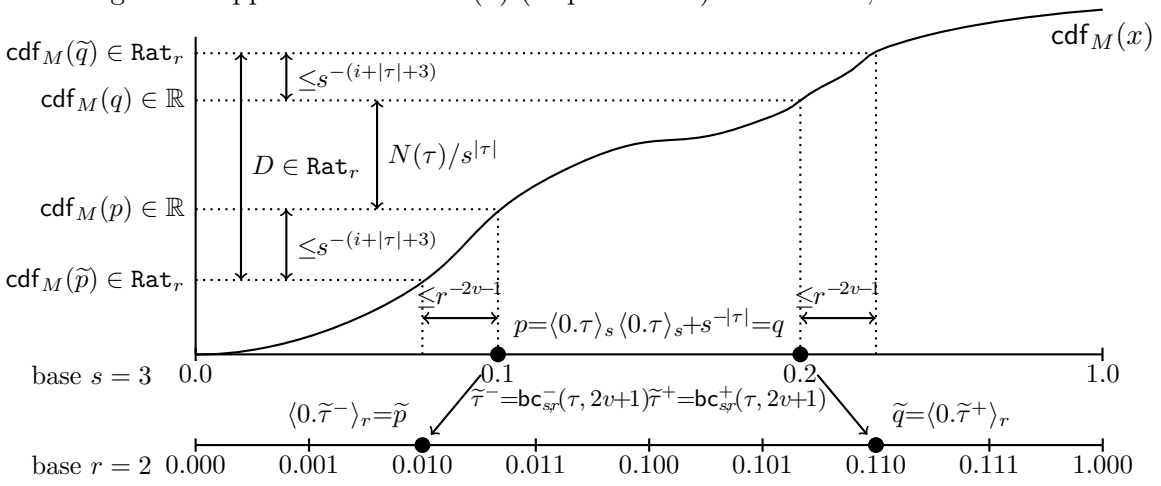
Step 3. *Approximating $D = \mathsf{cdf}_M(\widetilde{q}) - \mathsf{cdf}_M(\widetilde{p})$ with rationals in base s.*

We now approximate $D' = \langle 0.\rho' \rangle_r \in \mathtt{Rat}_r$ with a rational in base s. Define $\beta = \mathsf{bc}^-_{r,s}(\rho', i + |\tau| + 1) \in \Sigma_s^*$. Since $0 \leq \langle 0.\beta \rangle_s - D' < s^{-(i+|\tau|+1)}$, from (11) we conclude

$$|\langle 0.\beta \rangle_s - (\mathsf{cdf}_M(q) - \mathsf{cdf}_M(p))| \leq s^{-(i+|\tau|)}. \tag{12}$$

Finally define $\widehat{N}(\tau, i) = s^{|\tau|} \cdot \langle 0.\beta \rangle_s \in \mathtt{Rat}_s$. Since $N(\tau) = s^{|\tau|} \cdot (\mathsf{cdf}_M(q) - \mathsf{cdf}_M(p))$, from (12) we obtain $|\widehat{N}(\tau, i) - N(\tau)| \leq s^{-i}$.

Figure 1: Approximation of $N(\tau)$ (steps 1 and 2) when $\tau = 1$, $s = 3$ and $r = 2$



For the complexity analysis, let $n = |\tau| + i$. The value of v can be obtained in time $O(n)$. By Theorem 8 the values of $\widetilde{\tau}^-$ and $\widetilde{\tau}^+$ can be computed in time $O(m^2)$, where $m = |\tau| + 2v + 1 \in O(n)$, so $\widetilde{\tau}^-$ and $\widetilde{\tau}^+$ can be computed in time $O(n^2)$. Since the length of $\widetilde{\tau}^-$ and $\widetilde{\tau}^+$ are at most $2v+1 \in O(n)$, then, by Lemma 13 and the fact that $t(O(n)) \in O(t(n))$, the r-ary representation of $\mathsf{cdf}_M(\langle 0.\widetilde{\tau}^+\rangle_r)$ and $\mathsf{cdf}_M(\langle 0.\widetilde{\tau}^-\rangle_r)$ are computed in time $O(n \cdot t(n))$, the same as their difference $D = \langle 0.\gamma\rangle_s$. The computation of $D' = \langle 0.\gamma'\rangle_s$ can be done in time $O(n)$, and since $|\gamma'|$ is $O(n)$, the computation of β takes $O(n^2)$ steps. In summary, step 1 can be done in time $O(n)$, step 2 in time $O(n \cdot t(n))$ and step 3 in $O(n^2)$. Since $t(n) \geq n$, in total, the procedure takes time $O(n \cdot t(n))$. □

This concludes the proof of Lemma 15 and Theorem 14. □

7 Polynomial time martingales and normality

In [22] Schnorr showed that if $Z \in \Sigma_2^\omega$ is n^2-random in base 2 then Z satisfies the law of large numbers. He concluded that n^2-randomness implies normality in base 2. We adapt in two ways Wang's version [27] of Schnorr's proof that all n^2-random sequences in base 2 satisfy the law of large numbers. Firstly, we consider any base; secondly, we generalize it to the notion of normality.

Theorem 17. *If Z is $n \cdot \log^2 n$-random in base r then Z is normal in base r.*

Proof. We suppose that Z is not normal in base r and we define an $n \cdot \log^2 n$-martingale L which succeeds on Z. In fact, we show that there is $\beta > 1$ such that $L(Z\upharpoonright_n) > \beta^n$ for infinitely many n.

Recall the definition of $\mathsf{occ}_\sigma(\tau)$ in (1). Let $c \in \Sigma_r$ and $\alpha \in \Sigma_r^*$ such that $\alpha^\frown c$ is a string of minimal length for which it is not the case that $\lim_{n\to\infty} \mathsf{occ}_{\alpha^\frown c}(Z\upharpoonright_n)/n = r^{-|\alpha|-1}$. Define

$$\mathsf{occ}_{\alpha^\frown \bar{c}}(\sigma) = \sum_{d \in \Sigma_r \setminus \{c\}} \mathsf{occ}_{\alpha^\frown d}(\sigma).$$

By the choice of α, there is $\epsilon > 0$ such that one of the following is true:

$$(\exists^\infty n) \qquad \frac{\mathsf{occ}_{\alpha^\frown c}(Z\restriction_n)}{n} > r^{-|\alpha|-1} + \epsilon \tag{13}$$

$$(\exists^\infty n) \qquad \frac{\mathsf{occ}_{\alpha^\frown c}(Z\restriction_n)}{n} < r^{-|\alpha|-1} - r\epsilon. \tag{14}$$

Since $\mathsf{occ}_\alpha(\sigma) \leq 1 + \sum_{b\in\Sigma_r} \mathsf{occ}_{\alpha^\frown b}(\sigma) = 1 + \mathsf{occ}_{\alpha^\frown c}(\sigma) + \mathsf{occ}_{\alpha^\frown \bar{c}}(\sigma)$, in case (14) we have that there are infinitely many n such that

$$\begin{aligned}\frac{\mathsf{occ}_{\alpha^\frown \bar{c}}(Z\restriction_n)}{n} &> \frac{\mathsf{occ}_\alpha(Z\restriction_n) - 1}{n} - r^{-|\alpha|-1} + r\epsilon \\ &= \frac{\mathsf{occ}_\alpha(Z\restriction_n) - 1}{n} - r^{-|\alpha|} + (r-1)r^{-|\alpha|-1} + r\epsilon.\end{aligned}$$

By construction, $\alpha^\frown c$ is of minimal length. Thus for almost all n we have

$$\frac{\mathsf{occ}_\alpha(Z\restriction_n) - 1}{n} - r^{-|\alpha|} > -\epsilon,$$

and so there are infinitely many n such that $\mathsf{occ}_{\alpha^\frown \bar{c}}(Z\restriction_n)/n > (r-1)\cdot(r^{-|\alpha|-1} + \epsilon)$. Suppose n is such that $\mathsf{occ}_{\alpha^\frown \bar{c}}(Z\restriction_n) > n\cdot(r-1)\cdot(r^{-|\alpha|-1}+\epsilon)$. Since $\mathsf{occ}_{\alpha^\frown \bar{c}}(Z\restriction_n)$ is a sum of $r-1$ terms, one of them must be greater than $n\cdot(r^{-|\alpha|-1}+\epsilon)$. Thus there exists $d \in \Sigma_r \setminus \{c\}$ such that for infinitely many n we have $\mathsf{occ}_{\alpha^\frown d}(Z\restriction_n)/n > r^{-|\alpha|-1} + \epsilon$. Hence without loss of generality we may assume that (13) holds.

Let δ be so that $\delta/(r-1) \in \mathtt{Rat}_r^{\geq 0}$ and

$$\limsup_n \frac{\mathsf{occ}_{\alpha^\frown c}(Z\restriction_n)}{n} > \frac{1+\delta}{r^{|\alpha|+1}}. \tag{15}$$

Let $p = 1+\delta$ and $q = 1 - \frac{\delta}{r-1}$. Note that $p, q \in \mathtt{Rat}_r^{\geq 0}$. Define $L : \Sigma_r^* \to \mathtt{Rat}_r^{\geq 0}$ as follows:

$$\begin{aligned} L(\lambda) &= 1 \\ L(\sigma^\frown b) &= \begin{cases} L(\sigma) & \text{if } \alpha \text{ is not a suffix of } \sigma \\ p\cdot L(\sigma) & \text{if } \alpha \text{ is a suffix of } \sigma, \text{ and } b = c \\ q\cdot L(\sigma) & \text{if } \alpha \text{ is a suffix of } \sigma, \text{ and } b \neq c \end{cases}\end{aligned}$$

It is clear that for all $\sigma \in \Sigma_r^*$, we have

$$L(\sigma) = p^{\mathsf{occ}_{\alpha^\frown c}(\sigma)} \cdot q^{\mathsf{occ}_{\alpha^\frown \bar{c}}(\sigma)}. \tag{16}$$

Fact 18. L is a $\mathtt{Rat}_r^{\geq 0}$-valued martingale in base r.

Proof. By the choice of δ it is clear that L is $\mathtt{Rat}_r^{\geq 0}$-valued. Clearly, if α is not a suffix of σ, then $\sum_{i\in\Sigma_r} L(\sigma i) = \sum_{i\in\Sigma_r} L(\sigma) = r\cdot L(\sigma)$. Suppose that α is a suffix of σ, then

$$\begin{aligned}\sum_{i\in\Sigma_r} L(\sigma^\frown i) &= (1+\delta)\cdot L(\sigma) + \sum_{j\in\Sigma_r\setminus\{c\}} (1 - \frac{\delta}{r-1})\cdot L(\sigma) \\ &= (1+\delta)\cdot L(\sigma) + (r-1-\delta)\cdot L(\sigma) \\ &= r\cdot L(\sigma).\end{aligned}$$

This shows that L is a martingale in base r. □

Fact 19. L is computable in time $O(n \cdot \log^2 n)$.

Proof. In (16), both p and q are fixed rationals in base r and α is a fixed string in Σ_r^*. Given $\sigma \in \Sigma_r^n$, it is clear that $L(\sigma)$ can be represented with $O(n)$ many symbols of Σ_r. Given σ, one can calculate the unary representation of $\mathsf{occ}_{\alpha^\frown c}(\sigma)$ and $\mathsf{occ}_{\alpha\bar{c}}(\sigma)$ in linear time. For a fixed rational x, the method of exponentiation by repeated squaring computes x^m with a loop that is carried out $O(\log m)$ times, as follows:

$$x^m = \begin{cases} (x^2)^{\frac{m}{2}} & \text{if } m \text{ is even} \\ x \cdot (x^2)^{\frac{m-1}{2}} & \text{if } m \text{ is odd} \end{cases}$$

In the i-th iteration, the algorithm performs a fixed number of multiplications and additions of rationals of size $O(m/2^i)$. Hence the cost of the i-th operation is $O(m/2^i \cdot \log^2(m/2^i)) \leq O(m/2^i \cdot \log^2 m)$. In total, the time needed to compute x^m is

$$\sum_{i \leq O(\log m)} O(m/2^i \cdot \log^2 m) \leq O(m \cdot \log^2 m).$$

Finally, the multiplication of $p^{\mathsf{occ}_{\alpha^\frown c}(\sigma)}$ with $q^{\mathsf{occ}_{\alpha^\frown \bar{c}}(\sigma)}$ takes time $O(n \cdot \log^2 n)$. In total we compute $L(\sigma)$ in time $O(n \cdot \log^2 n)$. □

Fact 20. L succeeds on Z.

Proof. Since $\mathsf{occ}_{\alpha^\frown \bar{c}}(\sigma) \leq \mathsf{occ}_\alpha(\sigma) - \mathsf{occ}_{\alpha^\frown c}(\sigma)$ and $\log\ q$ is negative, from (16) we have

$$\begin{aligned} \log\ L(Z\upharpoonright_n) &\geq \mathsf{occ}_{\alpha^\frown c}(Z\upharpoonright_n) \cdot \log\ p + \left[\mathsf{occ}_\alpha(Z\upharpoonright_n) - \mathsf{occ}_{\alpha^\frown c}(Z\upharpoonright_n)\right] \cdot \log\ q \\ &= \mathsf{occ}_\alpha(Z\upharpoonright_n) \cdot \log\ q + \mathsf{occ}_{\alpha^\frown c}(Z\upharpoonright_n) \cdot (\log\ p - \log\ q). \end{aligned}$$

By taking the lim sup we obtain

$$\begin{aligned} \limsup_n \frac{\log\ L(Z\upharpoonright_n)}{n} &\geq \limsup_n \frac{\mathsf{occ}_\alpha(Z\upharpoonright_n)}{n} \cdot \log\ q + \frac{\mathsf{occ}_{\alpha^\frown c}(Z\upharpoonright_n)}{n} \cdot (\log\ p - \log\ q) \\ &= \frac{\log\ q}{r^{|\alpha|}} + (\log\ p - \log\ q) \cdot \limsup_n \frac{\mathsf{occ}_{\alpha^\frown c}(Z\upharpoonright_n)}{n} \\ &> \frac{\log\ q}{r^{|\alpha|}} + (\log\ p - \log\ q) \cdot \frac{1+\delta}{r^{|\alpha|+1}} \qquad \text{(by the choice of } \delta \text{ (15))} \\ &= \frac{1}{r^{|\alpha|+1}} \cdot ((1+\delta) \cdot \log(1+\delta) + (r-\delta-1) \cdot \log(1 - \frac{\delta}{r-1})) \\ &= \ell, \end{aligned}$$

where the first equality (second line) comes from the minimality of $\alpha^\frown c$.

It can be shown that for any $\epsilon \in (0,1)$ and any $x \geq 1$ we have

$$(1+\epsilon) \cdot \log(1+\epsilon) + (x-\epsilon) \cdot \log(1 - \epsilon/x) > 0.$$

Taking $\epsilon = \delta$ and $x = r - 1$ we conclude $\ell > 0$, and this means that there exist infinitely many n such that $\log\ L(Z\upharpoonright_n)/n > \ell$, that is $L(Z\upharpoonright_n) > 2^{\ell \cdot n}$. □

This completes the proof of Theorem 17. □

By combining Theorem 17 with Lemma 6 we conclude that if $Z \in \Sigma_r^\omega$ is not normal in base r then there is an $n^2 \cdot \log^2 n$-martingale with the savings property which succeeds on Z. We can actually show:

Proposition 21. *If $Z \in \Sigma_r^\omega$ is not normal in base r then there is an n^2-martingale in base r with the savings property that succeeds on Z.*

Proof. We combine the ideas from the proof of Theorem 17 with the proof of Lemma 6. Suppose $Z \in \Sigma_r^\omega$ is not normal in base r and define L, α, p, q and c as in the proof of Theorem 17. The function $\widetilde{L} : \Sigma_r^+ \to \mathtt{Rat}_r^{\geq 0}$ defined by

$$\widetilde{L}(\sigma^\frown b) = \begin{cases} 1 & \text{if } \alpha \text{ is not a suffix of } \sigma \\ p & \text{if } \alpha \text{ is a suffix of } \sigma, \text{ and } b = c \\ q & \text{if } \alpha \text{ is a suffix of } \sigma, \text{ and } b \neq c \end{cases}$$

is computable in linear time because $\alpha \in \Sigma_r^*$ is fixed. Note that $\widetilde{L}(\sigma^\frown b) = L(\sigma^\frown b)/L(\sigma)$.

Let E, G and M be as in the proof of Lemma 6. Using $\widetilde{L}$ we can rewrite its definitions:

$$E(\emptyset) = L(\emptyset) = 1 \quad E(\sigma^\frown b) = \begin{cases} \frac{\widetilde{L}(\sigma^\frown b)}{r} \cdot E(\sigma) & \text{if } E(\sigma) > \frac{r}{\widetilde{L}(\sigma^\frown b)} \\ \widetilde{L}(\sigma^\frown b) \cdot E(\sigma) & \text{otherwise} \end{cases}$$

$$G(\emptyset) = 0 \qquad G(\sigma^\frown b) = \begin{cases} G(\sigma) + \frac{(r-1)\cdot\widetilde{L}(\sigma^\frown b)}{r} \cdot E(\sigma) & \text{if } E(\sigma) > \frac{r}{\widetilde{L}(\sigma^\frown b)} \\ G(\sigma) & \text{otherwise} \end{cases}$$

Since r is constant, by the definition of $\widetilde{L}$, we have that $\widetilde{L}(\sigma^\frown b)/r$, $r/\widetilde{L}(\sigma^\frown b)$ and $(r-1)\cdot \widetilde{L}(\sigma^\frown b)/r$ are constant values (i.e. they do not depend on σ). Then the comparison $E(\sigma) > r/\widetilde{L}(\sigma^\frown b)$ can be done in linear time. Thus, one can compute E and G, and so M, in quadratic time. By Lemma 6, M succeeds on all the sequences that L does, and then M succeeds on Z. □

It follows from Hitchcock and Mayordomo [14, Corollary 3.3] that any polynomial time random is absolutely normal. We show that n^4-randomness suffices:

Corollary 22. *Suppose $Z \in \Sigma_r^\omega$ is such that no n^3-supermartingale in base r succeeds on Z. Then $z = \langle 0.Z \rangle_r$ is absolutely normal. In particular, if Z is n^4-random in base r then z is absolutely normal.*

Work in preparation of Lutz and Mayordomo [15] shows that in fact the result can be improved to n^2-randomness.

Proof. By contradiction, suppose that the real $z = \langle 0.Z \rangle_r$ is not absolutely normal. Then there is a base s and $Y \in \Sigma_s^\omega$ such that $z = \langle 0.Y \rangle_s$ and Y is not normal in base s. By Proposition 21 there is an n^2-martingale M in base s with the savings property that succeeds on Y. By Lemma 15, there is a martingale in base r with an n^3-computable approximation which succeeds on Z. By Lemma 3 there is an n^3-supermartingale in base r which also succeeds on Z. This establishes the first statement of the theorem. The second one follows from Lemma 4. □

8 An absolutely normal number in polynomial time

In the following result we improve the time bound of [3, Theorem 2.3].

Proposition 23. *There is $Z \in \Sigma_r^\omega$ computable in time $O(n^{k+2} \cdot \log^3 n)$ such that no n^k-supermartingale in base r succeeds on Z. In particular Z is n^k-random.*

Proof. Fix a time constructible nondecreasing and unbounded function h, suppose t is time constructible, and let $p(x) = x \cdot \log x$. We actually construct a sequence $Z \in \Sigma_r^\omega$ which is computable in time $O(n^2 \cdot \log n \cdot p(h(|\lceil \log n \rceil|) \cdot t(n)))$, and such that no $t(n)$-supermartingale succeeds on Z. The statement of the proposition follows by taking $t(n) = n^k$ and $h(n) = n$.

We first give an effective enumeration $(G_i)_{i\in\mathbb{N}}$ of all $t(n)$-supermartingales in base r with initial capital 1 and bound the time complexity of this enumeration. Take an enumeration of all Turing machines defined over the alphabet Σ_r, and define Φ_i as the function partially computable by the i-th Turing machine of such enumeration. We may view Φ_i as a partial function $\Sigma_r^* \to \mathtt{Rat}_r^{\geq 0}$.

Let

$$\widetilde{\Phi}_i(\sigma) = \begin{cases} \Phi_i(\sigma)[h(|i|) \cdot t(|\sigma|)] & \text{if } \Phi_i(\sigma)[h(|i|) \cdot t(|\sigma|)] \downarrow \\ 0 & \text{otherwise} \end{cases}$$

Define $G : \mathbb{N} \times \Sigma_r^* \to \mathtt{Rat}_r^{\geq 0}$ as follows:

$$G(i,\sigma) = \begin{cases} 1 & \text{if } \sigma = \emptyset \\ \widetilde{\Phi}_i(\sigma) & \text{if } \sigma = \tau^\frown b \text{ for } b \in \Sigma_r, \text{ and } \sum_{j\in\Sigma_r} \widetilde{\Phi}_i(\tau^\frown j) \leq r \cdot G(i,\tau) \\ 0 & \text{otherwise} \end{cases}$$

Let $G_i(\sigma) = G(i,\sigma)$. It can be shown that for all i, G_i is a $\mathtt{Rat}_r^{\geq}$-valued supermartingale in base r with $G_i(\emptyset) = 1$.

Fact 24. $G(i,\sigma)$ is computed in time $O(|\sigma| \cdot p(h(|i|) \cdot t(|\sigma|)))$.

Proof. Let $|\sigma| = n$ and $|i| = m$. Since h and t are time constructible, one can compute $h(m)$ in time $O(h(m))$ and $t(n)$ in time $O(t(n))$. Then the multiplication $h(m) \cdot t(n)$ can be done in time $O(|h(m)| \cdot |t(n)|)$. The simulation of $\widetilde{\Phi}_i(\sigma)$ takes time $O(p(h(m) \cdot t(n)))$ and then $G(i,\sigma)$ is computed in time $O(n \cdot p(h(m) \cdot t(n)))$. □

Fact 25. Suppose F is a $t(n)$-supermartingale such that $F(\emptyset) = 1$. Then there is e such that $F = G_e$.

Proof. Suppose $d > 0$ such that for all $\sigma \in \Sigma_r$, the computation of $F(\sigma)$ halts in at most $d \cdot t(|\sigma|)$ many steps. We can choose e with $F(\sigma) = \Phi_e(\sigma)$ for all σ with time bound $d \cdot t(|\sigma|)$, and $d < h(|e|)$. Then $\Phi_e = \widetilde{\Phi}_e = G_e$. □

Let $(n_i)_{i\in\mathbb{N}}$ be a strictly increasing computable sequence of natural numbers such that $n_i > i$. Define $\widehat{G}_i : \Sigma_r^* \to \mathbb{R}^{\geq 0}$ by

$$\widehat{G}_i(\sigma) = \begin{cases} r^{-i} - r^{-(i+1)} & \text{if } |\sigma| \leq n_i \\ r^{-2\cdot n_i} \cdot G_i(\sigma) & \text{otherwise} \end{cases}$$

Fact 26. $\widehat{G}_i$ is a supermartingale in base r.

Algorithm 3: Leftmost non-ascending path given by H

input : $n \in \mathbb{N}$
output: $\zeta_n \in \Sigma_r^n$

$\zeta_n := \emptyset$
for $i = 1$ *to* n **do**
  Find least $b \in \Sigma_r$ such that $H(\zeta_n) \geq H(\zeta_n{}^\frown b)$
  $\zeta_n := \zeta_n{}^\frown b$

Proof. We verify that $\sum_{b\in\Sigma_r} \widehat{G}_i(\sigma^\frown b) \leq r \cdot \widehat{G}_i(\sigma)$. The only non-trivial case is when $|\sigma| = n_i$:

$$\begin{aligned}
\sum_{b\in\Sigma_r} \widehat{G}_i(\sigma^\frown b) &= \sum_{b\in\Sigma_r} r^{-2\cdot n_i} \cdot G_i(\sigma^\frown b) && \text{(def. of } \widehat{G}) \\
&\leq r^{-2\cdot n_i+1} \cdot G_i(\sigma) && (G_i \text{ is a supermartingale}) \\
&\leq r \cdot r^{-n_i} && (G_i(\emptyset) = 1 \text{ and } |\sigma| = n_i) \\
&\leq r \cdot r^{-i}/2 && (i < n_i) \\
&\leq r \cdot (r^{-i} - r^{-(i+1)}) \\
&= r \cdot \widehat{G}_i(\sigma). && \text{(def. of } \widehat{G})
\end{aligned}$$

□

For any $\sigma \in \Sigma_r^*$, let

$$H(\sigma) = \sum_i \widehat{G}_i(\sigma).$$

Note that if $|\sigma| \leq n_0$ then $H(\sigma) = 1$, and if $n_j < |\sigma| \leq n_{j+1}$ then

$$H(\sigma) = r^{-(j+1)} + \sum_{i\leq j} r^{-2\cdot n_i} \cdot G_i(\sigma). \tag{17}$$

It is clear that H is a supermartingale, and by (17), it is $\mathtt{Rat}_r^{\geq 0}$-valued. From now on, let us fix $n_i = r^i$.

Fact 27. If $\sigma \in \Sigma_r^n$ then $H(\sigma)$ is computable in time $O(n \cdot \log n \cdot p(h(|\lceil \log n \rceil|) \cdot t(n)))$.

Proof. Suppose $n_j < |\sigma| \leq n_{j+1}$. Observe that $j \leq \log n$. By Fact 24, for each $i \leq j$, the value $v = G_i(\sigma)$ can be obtained in time $O(n \cdot p(h(|j|) \cdot t(n)))$ Computing the value of n_i in unary (which takes time $O(n \cdot \log n)$) allows us to compute the value of $r^{-2\cdot n_i} \cdot v$ with $O(n)$ many shift operations on v. The sum in (17) has $j + 1 \leq 1 + \log n$ many terms, so in total we need $O(n \cdot \log n \cdot p(h(|\lceil \log n \rceil|) \cdot t(n)))$. □

By (17), and Fact 25, if F is a $t(n)$-supermartingale in base r then there are $c, d > 0$ such that $c + d \cdot F \leq H$. So if $Z \in \Sigma_r^\omega$ is such that $\limsup_n H(Z\upharpoonright_n) < \infty$ then no $t(n)$-supermartingale in base r succeeds on Z. In particular, Z is $t(n)$-random. One can define Z as the leftmost non-ascending path given by H, i.e., given n define let ζ_n be the output Algorithm 3 with input n, and define $Z = \bigcap_n [\zeta_n]$. The complexity of Algorithm 3 on input n is measured in n. By Fact 27 the time needed to compute $Z\upharpoonright_n$ is $O(n^2 \cdot \log n \cdot p(h(|\lceil \log n \rceil|) \cdot t(n)))$. □

Corollary 28. *There is $Z \in \Sigma_r^\omega$ which is computable in time $O(n^5 \cdot \log^3 n)$ such that $\langle 0.Z \rangle_r$ is absolutely normal.*

Proof. By Proposition 23, there is $Z \in \Sigma_r^\omega$ which is computable in time $O(n^5 \cdot \log^3 n)$ for which no n^3-supermartingale in base r succeeds on. By Corollary 22, $\langle 0.Z \rangle_r$ is absolutely normal. □

9 Open questions

For many of our results it may be possible to improve time bounds. For instance, in Theorem 8 we showed a method for approximating rationals in a given base with rationals in another.

Question 29. *Is it possible to compute $\mathsf{bc}^-_{s,r}(\sigma)$ in less than quadratic time?*

In Theorem 14 we proved that polynomial time randomness is base invariant. In fact, we showed that n^{k+3}-randomness in a given base implies n^k-randomness in another base.

Question 30. *Is it possible to lower the '+3', or even show that n^k-randomness is base invariant (for large enough k)?*

Any improvement in this direction would be transferred to the complexity of the construction of an n^k-random sequence, and, in particular, to the complexity of computing an absolutely normal number.

In Theorem 17 we showed that $n \cdot \log^2 n$-randomness in base r implies normality in base r. As we explained in the proof of this result, one can 'count' the number of occurrences of a block of symbols in a given string in linear time.

Question 31. *Does linear-randomness in base r imply the law of large numbers in base r, or even normality in base r?*

A sequence $(y_i)_{i \in \mathbb{N}}$ of reals in $[0,1]$ is *uniformly distributed* if for each interval $[u,v] \subseteq [0,1]$, the proportion of $i < N$ with $y_i \in [u,v]$ tends to $v-u$ as $N \to \infty$. More formally,

$$\lim_{N \to \infty} \frac{|\{i < N \mid y_i \in [u,v]\}|}{N} = v - u.$$

For a real x let $\mathsf{frac}(x)$ denote the fractional part $x - \lfloor x \rfloor$.

Definition 32. *Let r be any rational number greater than one. We say that $x \in [0,1]$ is* normal in base r *if the sequence $(\mathsf{frac}(x \cdot r^n))_{n \in \mathbb{N}}$ is uniformly distributed in $[0,1]$.*

For every r the set of reals which are normal in base r has measure 1. Observe that this definition applies to *reals* in $[0,1]$, while the definition of normality given on page 2 (the one used along this work) applies to *sequences* of symbols in Σ_r. It is not hard to see that for any integer $r > 1$, and any $X \in \Sigma_r^\omega$, $\langle 0.X \rangle_r$ is normal in base r iff X is normal in base r. Hence a real x is absolutely normal if it is normal in all integer bases > 1. Let us say x is *rationally normal* if it is normal in all rational bases > 1.

In the following we discuss the fact that rational normality is stronger than absolute normality, even though it still has measure 1. This is a special case of a result by Brown, Moran and Pearce [9, Theorem 2]. Sets $A, B \subseteq (1, \infty)$ are called *multiplicatively independent* (m.i.) if there are no $a \in A, b \in B, r, s \in \mathbb{N}$ such that $a^r = b^s$. For instance, $A = \mathbb{N} \setminus \{0, 1\}$ and $B = \{3/2\}$ are m.i. The result of Brown et al. says that given m.i. sets of algebraic numbers, every real is the sum of four numbers that are normal for all bases in A, but none in B. In particular, there are uncountably many reals that are absolutely normal, but not normal for the base 3/2.

By our result that polynomial time randomness is base invariant (Theorem 14), it makes sense to talk about polynomial time *reals* in $[0, 1]$: a real $x \in [0, 1]$ is polynomial time random if whenever $x = \langle 0.X \rangle_r$ for some integer $r > 1$, we have that X is polynomial time random in base r.

In Corollary 22 we showed that every polynomial time random real is absolutely normal. An affirmative answer to the following would extend this result.

Question 33. *Is every polynomial time random real rationally normal?*

Acknowledgements. We thank Verónica Becher, Pablo Heiber, Jack Lutz, Elvira Mayordomo and Theodore A. Slaman. We also thank the referee for careful reading and mindful suggestions. This research was partially carried out while the authors participated in the Buenos Aires Semester in Computability, Complexity and Randomness, 2013. Nies was supported by the Marsden fund of New Zealand. Figueira was supported by UBA (UBACyT 20020110100025) and ANPCyT (PICT-2011-0365).

References

[1] Klaus Ambos-Spies, Hans Fleischhack, and Hagen Huwig. Diagonalizations over polynomial time computable sets. *Theor. Comput. Sci.*, 51:177–204, 1987.

[2] Klaus Ambos-Spies, Hans Fleischhack, and Hagen Huwig. Diagonalizing over deterministic polynomial time. In *CSL*, volume 329 of *Lecture Notes in Computer Science*, pages 1–16, 1987.

[3] Klaus Ambos-Spies, Sebastiaan Terwijn, and Xizhong Zheng. Resource bounded randomness and weakly complete problems. *Theoretical Computer Science*, 172:195–207, 1997.

[4] Verónica Becher and Santiago Figueira. An example of a computable absolutely normal number. *Theoretical Computer Science*, 270:947–958, 2002.

[5] Verónica Becher, Santiago Figueira, and Rafael Picchi. Turing's unpublished algorithm for normal numbers. *Theoretical Computer Science*, 377(1-3):126–138, 2007.

[6] Verónica Becher, Pablo Heiber, and Theodore A. Slaman. A polynomial-time algorithm for computing absolutely normal numbers. Manuscript, 2013.

[7] Émile Borel. Les probabilités dénombrables et leurs applications arithmétiques. *Rendiconti del Circolo Matematico di Palermo*, 27:247–271, 1909.

[8] Vasco Brattka, Joseph S. Miller, and André Nies. Randomness and differentiability. To appear, 2011.

[9] Gavin Brown, William Moran, and Charles E. M. Pearce. A decomposition theorem for numbers in which the summands have prescribed normality properties. *J. Number Theory*, 24(3):259–271, 1986.

[10] Cristian S. Calude and Helmut Jürgensen. Randomness as an invariant for number representations. In J. Karhumäki H. Maurer and G. Rozenberg, editors, *Results and Trends in Theoretical Computer Science*, pages 44–66. Springer-Verlag, 1994.

[11] David G. Champernowne. The construction of decimals in the scale of ten. *Journal of the London Mathematical Society*, 8:254–260, 1933.

[12] Ben Green and Terence Tao. The primes contain arbitrarily long arithmetic progressions. *Annals of Mathematics*, 167(2):481–547, 2008.

[13] Peter Hertling and Klaus Weihrauch. Randomness space. In *Automata, Languages and Programming*, pages 796–807. Springer-Verlag, 1998.

[14] John Hitchcock and Elvira Mayordomo. Base invariance of feasible dimension. Manuscript, 2012.

[15] Jack Lutz and Elvira Mayordomo. Construction of an absolutely normal real number in polynomial time. Manuscript, 2012.

[16] Jack H. Lutz. Category and measure in complexity classes. *SIAM J. Comput.*, 19(6):1100–1131, 1990.

[17] Jack H. Lutz. Almost everywhere high nonuniform complexity. *J. Comput. Syst. Sci.*, 44(2):220–258, 1992.

[18] Per Martin-Löf. The definition of random sequences. *Information and Control*, 9:602–619, 1966.

[19] André Nies. *Computability and Randomness*. Clarendon Press, Oxford, 2009.

[20] Wolfgang M. Schmidt. On normal numbers. *Pacific Journal of Mathematics*, 10:661–672, 1960.

[21] Claus-Peter Schnorr. A unified approach to the definition of a random sequence. *Mathematical Systems Theory*, 5:246–258, 1971.

[22] Claus-Peter Schnorr. Zufälligkeit und Wahrscheinlichkeit. *Lecture Notes in Mathematics*, 218, 1971.

[23] Waclaw Sierpinski. Démonstration élémentaire du théorème de M. Borel sur les nombres absolument normaux et détermination effective d'un tel nombre. *Bulletin de la Société Mathématique de France*, 45:127–132, 1917.

[24] Javier Silveira. *Invariancia por cambio de base de la aleatoriedad computable y la aleatoriedad con recursos acotados*. PhD thesis, University of Buenos Aires, 2011. Advisor: Santiago Figueira. Unpublished.

[25] Ludwig Staiger. The Kolmogorov complexity of real numbers. In *Proceedings of the 12th International Symposium on Fundamentals of Computation Theory*, FCT '99, pages 536–546, London, UK, 1999. Springer-Verlag.

[26] Alan M. Turing. A note on normal numbers. In J.L. Britton, editor, *Collected Works of A.M. Turing: Pure Mathematics*, pages 117–119. North Holland, Amsterdam, 1992.

[27] Yongge Wang. *Randomness and Complexity.* PhD thesis, University of Heidelberg, 1996.