Pointed computations and Martin-Löf randomness*

George Barmpalias   Andrew Lewis-Pye   Angsheng Li

For Barry, for whom the magnificent incomputability of the world was a deeply held belief.
The only response? An attempt at understanding this chaos at a higher order.

Abstract. Schnorr showed that a real X is Martin-Löf random if and only if $K(X\upharpoonright_n) \geq n - c$ for some constant c and all n, where K denotes the prefix-free complexity function. Fortnow (unpublished) and Nies, Stephan and Terwijn [NST05] observed that the condition $K(X\upharpoonright_n) \geq n - c$ can be replaced with $K(X\upharpoonright_{r_n}) \geq r_n - c$, for any fixed increasing computable sequence (r_n), in this characterization. The purpose of this note is to establish the following generalisation of this fact. We show that X is Martin-Löf random if and only if $\exists c\ \forall n\ K(X\upharpoonright_{r_n}) \geq r_n - c$, where (r_n) is any fixed *pointedly X-computable* sequence, in the sense that r_n is computable from X in a self-delimiting way, so that at most the first r_n bits of X are queried in the computation of r_n. On the other hand, we also show that there are reals X which are very far from being Martin-Löf random, but for which there exists some X-computable sequence (r_n) such that $\forall n\ K(X\upharpoonright_{r_n}) \geq r_n$.

George Barmpalias
State Key Lab of Computer Science, Inst. of Software, Chinese Acad. Sci., Beijing, China.
School of Mathematics and Statistics, Victoria University of Wellington, New Zealand.
E-mail: barmpalias@gmail.com. *Web:* http://barmpalias.net

Andrew Lewis-Pye
Department of Mathematics, Columbia House, London School of Economics, Houghton St., London, WC2A 2AE, United Kingdom.
E-mail: A.Lewis7@lse.ac.uk. *Web:* http://aemlewis.co.uk

Angsheng Li
State Key Lab of Computer Science, Inst. of Software, Chinese Acad. Sci., Beijing, China.
E-mail: angsheng@ios.ac.cn.

**Date:* March 14, 2017. Barmpalias was supported by the 1000 Talents Program for Young Scholars from the Chinese Government, grant no. D1101130. Additional support was received by the Chinese Academy of Sciences (CAS) and the Institute of Software of the CAS. Lewis-Pye was supported by a Royal Society University Research Fellowship. Angsheng Li was partially supported by the National Basic Science Program (973 Program Group) entitled Cyber Information and Computational Theory on Big Data with Grant No. 2014CB340302.

1 Introduction

A well known result of Schnorr (see Chaitin [Cha75]) is that Martin-Löf's notion of algorithmic randomness from [ML66] can be expressed in terms of incompressibility with respect to prefix-free machines. In particular, a real X is Martin-Löf random if and only if $\exists c \forall n\, K(X \upharpoonright_n) > n - c$, where K denotes the prefix-free complexity function. The latter condition says that there exists a constant c such that all the initial segments of X are *c-incompressible* (in a prefix-free sense). As reported in Downey and Hirschfeldt [DH10, Proposition 6.1.4], Fortnow (unpublished) and Nies, Stephan and Terwijn [NST05] showed that Schnorr's characterisation remains valid if we replace the condition $\exists c \forall n\, K(X \upharpoonright_n) > n - c$ with $\exists c \forall n\, K(X \upharpoonright_{r_n}) > r_n - c$, where (r_n) is any computable increasing sequence.

In this note we consider the extent to which this fact can be generalised to incomputable increasing sequences (r_n). It is well known that there are reals which are not Martin-Löf random, yet have infinitely many 0-incompressible initial segments. Hence this characterisation does not hold for arbitrary increasing sequences (r_n). We consider the case when (r_n) is computable from X. Our main result is that if (r_n) is computable from X in a certain restricted way, then X is Martin-Löf random if and only if $\exists c \forall n\, K(X \upharpoonright_{r_n}) > r_n - c$. On the other hand we show how to construct reals X and X-computable sequences (r_n) such that the above equivalence fails, so we have $\forall n\, K(X \upharpoonright_{r_n}) \geq r_n$ but X is very far from being Martin-Löf random.

1.1 Pointed computability

Our main result is that if X computes (r_n) in a certain natural fashion, then $\exists c \forall n\, K(X \upharpoonright_{r_n}) > r_n - c$ is a sufficient and necessary condition for the Martin-Löf randomness of X. In this section we formalise the notion of oracle-computability required in order for this equivalence to hold, which we call pointed computability.

A Turing functional Φ can be thought of as a machine which takes as inputs a number n and a program σ, and either halts on these inputs producing a number $\Phi^{\sigma}(n)$ as output, or else diverges. The consistency of Φ requires that if $\rho_0 \subseteq \rho_1$ and $\Phi^{\rho_0}(n) \downarrow$, then the computation $\Phi^{\rho_1}(n)$ is identical to that for $\Phi^{\rho_0}(n)$, yielding the same output. Then $\Phi^X(n)$ can be defined as $\lim_s \Phi^{X \upharpoonright_s}(n)$. Without loss of generality, given a Turing functional Φ, a string ρ and a number n, we may assume that $\Phi^{\rho}(n) \downarrow$ implies $|\rho| \geq n$ and $|\rho| \geq \Phi^{\rho}(n)$. This is a standard convention and it is not hard to see that if $\Psi^X = Z$ for two reals and a Turing functional Ψ which might not obey the convention, then there exists a Turing functional Φ which does obey the stated convention and for which $\Phi^X = Z$.

Given a Turing functional Φ, a number n and strings ρ_0, ρ_1, the consistency property says that if $\Phi^{\rho_0}(n) \neq \Phi^{\rho_1}(n)$ then we must have that $\rho_0 \mid \rho_1$, i.e. the finite oracles differ at a digit which is less than $\min\{|\rho_0|, |\rho_1|\}$. The following definition is based on a more stringent consistency requirement.

Definition 1.1 (Pointed computations)**.** *Given a real X, we say that a sequence (r_n) is pointedly X-computable if (r_n) is (strictly) increasing and there exists a Turing functional Φ such that $\Phi^{X\upharpoonright_{r_n}}(n)\downarrow = r_n$ for each n.*

The latter condition in Definition 1.1 says that some oracle Turing machine computes each r_n from X with oracle-use bounded above by r_n. Note that, without loss of generality, we may assume that the oracle-use in this computation is exactly r_n.

As a typical example of pointed computations (suppressing the monotonicity requirement for now), consider an oracle machine which starts on input n by reading increasingly longer initial segments of the oracle tape, and eventually stops after $s > n$ steps, with output s. If, for a given X, such a machine converges for every n, then it produces a pointed computation in the sense of Definition 1.1. Another example is the settling time of a non-computable c.e. set A: let $r_0 = 0$ and for each n let r_{n+1} be the least number which is larger than r_n and such that $A_s\upharpoonright_n = A\upharpoonright_n$ for all $s \geq r_{n+1}$. Then (r_i) is pointedly A-computable and non-computable.

Later we will note that there are weaker notions of computability which suffice for our characterization of Martin-Löf randomness. One such notion is the condition that $K(r_n \mid \tau) = \mathbf{O}(1)$ for all n and all $\tau \supseteq X\upharpoonright_{r_n}$. Note that the latter is the non-uniform version of the notion of Definition 1.1.

1.2 Our results

Our main result is the following, which we prove in Section 2.

Theorem 1.2 (Randomness condition)**.** *Suppose that (r_n) is pointedly computable from a real X. Then X is Martin-Löf random if and only if $\exists c\ \forall n\ K(X\upharpoonright_{r_n}) > r_n - c$.*

It is well-known that there are reals which are not Martin-Löf random, yet have infinitely many incompressible initial segments. Hence Theorem 1.2 does not hold if we simply waive the requirement that (r_n) is pointedly computable from X. One may ask, however, if Theorem 1.2 continues to hold if we merely require that (r_n) is computable from X and not that it is pointedly X-computable. It is not surprising that the latter question has a negative answer. One way to exhibit an example witnessing this fact, is to construct a real with infinitely many incompressible initial segments, which computes the halting problem and is not Martin-Löf random. Since the prefix-free complexity function is computable from the halting problem $\emptyset'$, given such an oracle X we can effectively find infinitely many t such that $K(X\upharpoonright_t) \geq t - c$. This gives the following fact.

Proposition 1.3. *Suppose that X computes the halting problem, X is not Martin-Löf random and there exists some constant c and infinitely many n such that $K(X\upharpoonright_n) \geq n - c$. Then X computes an increasing sequence (r_n) such that $K(X\upharpoonright_{r_n}) \geq r_n - c$ for all n.*

In Section 3 we present two ways of constructing oracles X which have the properties mentioned in Proposition 1.3, thus establishing the following.

Theorem 1.4. *There exists a real X and an X-computable increasing sequence (r_n), such that $r_n < K(X \upharpoonright_{r_n})$ for all n, and X is not Martin-Löf random.*

Our first construction of such X involves starting from a Martin-Löf random Y which computes the halting problem, and inserting zeros at certain places, thus causing X to be non-random, while preserving its ability to calculate lengths at which its initial segments have high prefix-free complexity. The second construction of such an oracle X is more flexible, and gives a real which is highly non-random, in the sense that its characteristic sequence has a computable subsequence of zeros.

1.3 Related concepts and results from the literature

A central notion studied in this paper is that of a set X which is able to compute a sequence of positions in its binary expansion where the corresponding initial segments are incompressible. Clearly every Martin-Löf random has this property, but there are also many reals with this property which are not Martin-Löf random. This notion might remind some readers of the *autocomplex reals* (see [KHMS06, KHMS11] or [DH10, Section 8.16]), which are the reals X which compute a non-decreasing unbounded function f such that $K(X \upharpoonright_n) \geq f(n)$ for all n. Moreover, Theorem 1.2 has similarities to a result by Miller and Yu [MY10], which says that if $\sum_i 2^{-g(i)} < \infty$ and g is computable from X with identity oracle-use, then $\exists c\ \forall n\ K(X \upharpoonright_n) \leq n + g(n) + c$. Note that the latter result can be seen as an extension of the following consequence of the Kraft-Chaitin inequality:

if g is computable and $\sum_i 2^{-g(i)} < \infty$ then there exists a constant c such that for all X and all n we have $K(X \upharpoonright_n) \leq n + g(n) + c$. (1.3.1)

It is clear that the result of Miller and Yu [MY10] is related to its special case (1.3.1) in the same way as our Theorem 1.2 is related to results originally obtained by Fortnow (unpublished) and Nies, Stephan and Terwijn [NST05], discussed earlier.

2 Proof of Theorem 1.2

We need to show that if (r_n) is pointedly X-computable, then X is Martin-Löf random if and only if $\exists c\ \forall n\ K(X \upharpoonright_{r_n}) > r_n - c$.

The 'only if' direction in this statement is trivial, so it remains to show the 'if' direction. We prove the contrapositive. Assuming that X is not Martin-Löf random and (r_n) is pointedly X-computable, we show that for each constant c there exists some n such that $K(X \upharpoonright_{r_n}) \leq r_n - c$. Let Φ be a Turing functional such that $\Phi^X(n) = r_n$ for all n, and such that for every n, r, ρ such that $\Phi^\rho(n)\downarrow = r$ we have $\Phi^{\rho\restriction_r}(n)\downarrow$, $|\rho| > n$, $|\rho| \geq r$ and $\Phi^\rho(i)\downarrow$ for all $i < n$. Let U be the underlying optimal universal prefix-free machine.

We define a prefix-free machine M which makes use of the descriptions of U as follows. For each vector (ρ, σ, n, t), such that:

- $\Phi^\rho(i)\downarrow$ for all $i \leq n+1$ and $\Phi^\rho(i) < \Phi^\rho(i+1)$ for all $i < n+1$;
- $t \in (\Phi^\rho(n), \Phi^\rho(n+1)]$ and $U(\sigma) = \rho\restriction_t$;

let τ be the digits of ρ between digit t and digit $\Phi^\rho(n+1)$ and note that

$$U(\sigma) * \tau = \rho\restriction_{\Phi^\rho(n+1)},\ \Phi^{U(\sigma)*\tau}(n+1) = \Phi^\rho(n+1) \text{ and } \Phi^{U(\sigma)*\tau}(n) = \Phi^\rho(n).$$

Let M describe $\rho\restriction_{\Phi^\rho(n+1)}$ with the string $\sigma * \tau$, defining $M(\sigma * \tau) = \rho\restriction_{\Phi^\rho(n+1)}$. This completes the definition of M.

It follows immediately from the definition that M is effectively calculable. Next we show that M does not allocate two different strings the same description. Given two identical M-descriptions $\sigma_0 * \tau_0 = \sigma_1 * \tau_1$, since U is a prefix-free machine we must have $\sigma_0 = \sigma_1$ and $\tau_0 = \tau_1$. By the construction of M, the string described in both cases is then $U(\sigma_0) * \tau_0$. In a similar manner, we may show that M is a prefix-free machine. Suppose that $\sigma_0 * \tau_0 \subseteq \sigma_1 * \tau_1$ are two descriptions issued by M, resulting from the vectors $(\rho_0, \sigma_0, n_0, t_0)$, $(\rho_1, \sigma_1, n_1, t_1)$ respectively. Since U is a prefix-free machine and σ_0, σ_1 are U-descriptions, we have $\sigma_0 = \sigma_1$, $t_0 = t_1$ and $\tau_0 \subseteq \tau_1$. Let σ be σ_0 and let t be t_0. Then $\rho_0 \subseteq \rho_1$ and hence[1]

$$\Phi^{\rho_0}(n_0+1) = \Phi^{U(\sigma)*\tau_0}(n_0+1) = \Phi^{U(\sigma)*\tau_1}(n_0+1) = \Phi^{\rho_1}(n_0+1). \tag{2.0.1}$$

Thus $(\Phi^{\rho_0}(n_0), \Phi^{\rho_0}(n_0+1)] = (\Phi^{\rho_1}(n_0), \Phi^{\rho_1}(n_0+1)]$, and t belongs to both intervals. This means that $n_0 = n_1$, because otherwise t_1 would have to belong to a different interval, not the one determined by n_0 and ρ_1, since the values of Φ are strictly monotone. This would be a contradiction by the choice of $(\rho_1, \sigma_1, n_1, t_1)$ in the definition of M and the fact that $t_0 = t_1$ which was established earlier. So let $n = n_0 = n_1$. Since $U(\sigma) * \tau_0 = \rho_0\restriction_{\Phi^{\rho_0}(n+1)}$ and $U(\sigma) * \tau_1 = \rho_1\restriction_{\Phi^{\rho_1}(n_0+1)}$, by (2.0.1) the strings $U(\sigma) * \tau_0$, $U(\sigma) * \tau_1$ have the same length, so $\tau_0 = \tau_1$, which shows that the two descriptions $\sigma_0 * \tau_0$, $\sigma_1 * \tau_1$ are identical. This completes the proof that M is a prefix-free machine.

It remains to show that if X is not Martin-Löf random, then for each c there exists some n with $K(X\restriction_{r_n}) \leq r_n - c$. Let d be a constant such that $K(\eta) \leq K_M(\eta) + d$ for all strings η. Given any constant c, since X is not Martin-Löf random, there exists some $t > 0$ such that $K(X\restriction_t) \leq t - c - d$. Let n be such that $t \in (r_n, r_{n+1}]$. Then M will describe $X\restriction_{r_{n+1}}$ with $\sigma * \tau$

[1] An intuitive description of the argument that follows for showing that $\tau_0 = \tau_1$ is this: each of ρ_0, ρ_1 determine a sequence $\Phi^{\rho_0}(i), i \leq n_0+1$, although ρ_1 may be able to define $\Phi^{\rho_1}(i)$ for $i > n_0+1$. However $t \in (\Phi^{\rho_0}(n_0), \Phi^{\rho_0}(n_0+1)]$ so by the construction of M we have that both τ_0, τ_1 equal the digits of ρ_0 (or equivalently ρ_1) between digit t and digit $\Phi^{\rho_0}(n_0+1)$.

where σ is the shortest description of $X \upharpoonright_t$ and the length of τ is $r_{n+1} - t$. The length of σ is $K(X \upharpoonright_t)$, which is at most $t - c - d$. We have:

$$K_M(X \upharpoonright_{r_{n+1}}) \leq (t - c - d) + (r_{n+1} - t) = r_{n+1} - c - d.$$

So $K(X \upharpoonright_{r_{n+1}}) \leq r_{n+1} - c$, as required.

3 Proof of Theorem 1.4

As discussed in the introduction, we present two different constructions of a real X which computes an increasing sequence (r_n) such that $K(X \upharpoonright_{r_n}) > r_n$ for all n and X is not Martin-Löf random.

3.1 An ad hoc construction

One way to construct a real X with the property of Proposition 1.3 is to start from a a Martin-Löf random real Y which computes the halting problem, and insert zeros into Y in a way that does not change the fact that $\emptyset'$ is computable from the resulting oracle, but does ensure non-randomness. Recall that a Martin-Löf random real Y which computes the halting problem exists by the Kučera-Gács theorem [Kuč85, Gác86]. In this construction we use the result of Chaitin [Cha75], which asserts that:

$$\text{if } Z \text{ is Martin-Löf random then } \lim_s \left(K(Z \upharpoonright_s) - s\right) = \infty. \tag{3.1.1}$$

We also use the fact that for each real Z which is Martin-Löf random and each string σ, the real $\sigma * Z$ is Martin-Löf random, and the fact from [Cha87] that:

> if Z is Martin-Löf random and f is a partial computable function on strings, then if $f(Z \upharpoonright_n)\downarrow$ for infinitely many n, there are infinitely many t such that $f(Z \upharpoonright_t)\downarrow \neq Z(t)$. (3.1.2)

The reader may observe that a partial computable prediction rule f as above which is always successful on Z would give rise to a computable martingale which succeeds on Z, which we know is not possible for Martin-Löf random reals (e.g. see [DH10, Section 6.3]).

Let Φ be a functional via which Y computes the complexity function K, i.e. such that $\Phi^Y(\sigma) = K(\sigma)$ for all σ. We form X from Y by inserting 0s at various positions, in a stage by stage process. The real X is defined as the limit of a sequence X_s and we form each X_{s+1} from X_s by inserting a 0 at position t_{s+1}, which means that we define $X_{s+1}(n) = X_s(n)$ for $n < t_{s+1}$, $X_{s+1}(n) = 0$ for $n = t_{s+1}$ and $X_{s+1}(n+1) = X_s(n)$ for $n \geq t_{s+1}$. At stage 0 we define $X_0 = Y$, and (for convenience) define $t_0 = -1$. Now inductively suppose that we have performed stages $0, \dots, k$, and that we have recorded $t_0, \dots, t_k$. For any string $\tau \subset X_k$, let τ^* be the string which results from removing all of the 0s that we have inserted during the stages $\leq k$. At step $k+1$ we search for $\sigma \subset X_k$ of length $> t_k + 2$ and $\tau \subset X_k$ with $\sigma \subset \tau$ such that Φ^{τ^*} computes $K(\sigma)$ and $K(\sigma) > |\sigma|$. By (3.1.1), it follows that such σ and τ exist. Then we define $t_{k+1} = |\tau|$ and insert a 0 at position t_{k+1}.

This completes the construction of X given Y. From the construction it follows that X computes both Y and the sequence (t_k). This follows because X is able to retrace the construction. Inductively suppose that X has been able to retrace the construction up until the end of stage k, and so knows the values $t_0, \dots, t_k$. Then, using the oracle for X we can perform the same search that was carried out at stage $k+1$, but using X rather than X_k: we search for $\sigma \subset X$ of length $> t_k + 2$ and $\tau \subset X$ with $\sigma \subset \tau$ such that Φ^{τ^*} computes $K(\sigma)$ and $K(\sigma) > |\sigma|$. Since the next zero is inserted after τ, the result of the search is the same as when X_k was used during the construction at stage $k+1$. Then $t_{k+1} = |\tau|$, completing the induction step. Therefore X computes the halting set $\emptyset'$. Moreover there is a partial computable function f such that for each $\sigma \subset X$ we have $f(\sigma)\downarrow$ if and only if $\sigma = X \upharpoonright_{t_k}$ for some k (f uses σ as an oracle to try and retrace the construction and converges on σ if it is of length t_k for some k in the retraced construction). For each k, the next digit t_k of X is a 0, so f is a partial computable prediction rule that succeeds on X, which means that X is not Martin-Löf random. This completes the construction of a set X with the properties of Proposition 1.3.

3.2 A refined construction

Here we construct the required X by finite extensions. This construction can be combined with other requirements. For example, X can be highly non-random, in the sense that it has a computable sequence of 0s. We need some facts from the theory of prefix-free Kolmogorov complexity. For each string σ, let σ^* denote the shortest prefix-free description of σ (if there are many shortest descriptions, we consider the one which describes σ first). Also let $K(\tau \mid \rho)$ denote the prefix-free complexity of τ relative to string ρ. The following is a relativized version of Chaitin's counting theorem from [Cha75].

Lemma 3.1 (Relativized counting theorem)**.** *There exists a constant c such that for all σ, r and all $n > \sigma$:*

$$\left|\left\{\tau \;\middle|\; \sigma \subseteq \tau \wedge \tau \in 2^n \wedge K(\tau \mid \sigma^*) \leq |\tau| - r - K(\sigma)\right\}\right| \leq 2^{n-K(\sigma)+c-r-K(n \mid \sigma^*)}.$$

Proof. Given σ we define $F(n \mid \sigma^*)$ for $n > |\sigma|$ to be the $-\log$ of the weight of the prefix-free descriptions relative to σ^* which describe extensions of σ of length n. Then since the relative prefix-free complexity K is a minimal information measure, there exists a constant c such that for all n, σ,

$$2^{-F(n \mid \sigma^*)} < 2^{-K(n \mid \sigma^*)+c}. \tag{3.2.1}$$

We claim that the constant c has the property of the statement of the lemma. For a contradiction, suppose that this is not the case. Then for some n there are more than $2^{n-K(\sigma)+c-r-K(n \mid \sigma^*)}$ many

τ such that $K(\tau \mid \sigma^*) \leq |\tau| - r - K(\sigma)$. In that case we have

$$2^{-F(n \mid \sigma)} > 2^{n-K(\sigma)+c-r-K(n \mid \sigma^*)} \cdot 2^{-n+r+K(\sigma)} = 2^{c-K(n \mid \sigma^*)},$$

which contradicts (3.2.1). This contradiction concludes the proof of the lemma. $\square$

Recall the symmetry of information fact from [Gác74, Cha75]:

$$K(\tau) + K(\sigma \mid \tau^*) = K(\sigma) + K(\tau \mid \sigma^*) + \Omega(1)$$

where $f = g + \Omega(1)$ for two functions f, g means that $|f(n) - g(n)|$ is bounded above. Since $K(\tau) = K(\sigma, \tau) + \mathbf{O}(1)$ for all strings σ, τ, by the symmetry of information, Lemma 3.1 has the following corollary.

Corollary 3.2 (Relativized counting, again)**.** *There exists a constant c such that*

$$\left|\left\{\tau \;\middle|\; \sigma \subseteq \tau \wedge \tau \in 2^n \wedge K(\tau) \leq |\tau| - r\right\}\right| \leq 2^{n-K(\sigma)+c-r-K(\sigma \mid \tau^*)-K(n \mid \sigma^*)}$$

for all σ, r and all $n > \sigma$.

Corollary 3.2 is the tool we are going to use for our finite extension construction. The problem we face is, given a string σ to find an extension τ such that $K(\tau) > |\tau|$. Since there are $2^{n-|\sigma|}$ many extensions of σ of length n, by Corollary 3.2 it suffices to consider n such that $2^{n-K(\sigma)+c-K(n \mid \sigma^*)} < 2^{n-|\sigma|}$, which means that $|\sigma| + c < K(\sigma) + K(n \mid \sigma^*)$ so

$$K(n \mid \sigma^*) > |\sigma| - K(\sigma) + c.$$

Such a number n clearly exists in the interval $[|\sigma|, |\sigma| + 2^{c+|\sigma|-K(\sigma)}]$. The quantity $|\sigma| - K(\sigma)$ is sometimes called the *randomness deficiency* of σ. We have shown that:

> There exists a constant c such that each σ can be extended by less than $2^{c+|\sigma|}-1$ many bits to a string τ with $K(\tau) > |\tau|$. (3.2.2)

We are ready to construct the required real X by finite extensions

$$\rho_0 \subset \tau_1 \subset \rho_1 \subset \tau_2 \subset \cdots \tag{3.2.3}$$

In this construction the lengths $\ell_i := |\tau_i|$ will be computable while the strings ρ_i will be chosen so that $K(\rho_i) > |\rho_i|$ for all i. For each i the string τ_{i+1} will be the concatenation of ρ_i with a string $10\ldots0$ such that $|\tau_i| = \ell_i$. So for each i the string ρ_i will be uniformly computable from τ_i: simply find the first 1 starting from position $|\tau_i|$ in τ_i and moving to the left, and if this 1 is at position t then $\rho_i = \tau_i \restriction_t$. Let c be the constant in (3.2.2).

Let ρ_0 be the empty string λ, so that $K(\rho_0) > |\rho_0|$. Let τ_1 be the string $\rho_0 * 10$ and let $\ell_1 = |\rho_0| + 2 = 2$. Note that the last digit of τ_1 is a 0. By (3.2.2) there exists an extension ρ_1 of τ_1 such that $|\rho_1| - |\tau_1| < 2^{c+\ell_1} - 1$ and $K(\rho_1) > |\rho_1|$. Then let τ_2 be the concatenation of ρ_1

with a string $10\dots0$ such that the length $\ell_2 := |\tau_2|$ is $\ell_1 + 2^{c+\ell_1}$. Note that τ_2 is longer than ρ_1 by at least 2 bits, so the last digit of τ_2 is a 0. Similarly, we can choose an extension ρ_2 of τ_2 of less than $2^{c+\ell_2} - 1$ many additional bits such that $K(\rho_2) > |\rho_2|$. As before we let τ_3 be the concatenation of ρ_2 with a string $10\dots0$ such that the length of τ_3 is $\ell_3 := \ell_2 + 2^{c+\ell_2}$. Note that τ_3 is longer than ρ_2 by at least 2 bits, so the last digit of τ_3 is a 0.

The construction continues similarly, thus defining the computable sequence of lengths $\ell_{n+1} = \ell_n + 2^{c+\ell_n}$ for each $n > 0$, where $\ell_1 = 2$, and the sequences (3.2.3) such that for all $i > 0$ we have $K(\rho_i) > |\rho_i|$, $|\tau_i| = \ell_i$ and the last digit of τ_i is 0. If we let X be the infinite extensions of the strings (3.2.3) then we have $X(\ell_i - 1) = 0$ for all i, so X is not Martin-Löf random. On the other hand $X \upharpoonright_{\ell_i} = \tau_i$ for all i, and since τ_i uniformly computes ρ_i, we have that the sequence $(|\rho_i|)$ is X-computable. Finally $K(X \upharpoonright_{|\rho_i|}) = K(\rho_i|) > |\rho_i|$ for all i, which concludes the verification of the required properties of X.

4 Conclusion and discussion

We have generalized the criterion for Martin-Löf randomness by Fortnow (unpublished) and Nies, Stephan and Terwijn [NST05], which says that if X has incompressible segments of a computable sequence of lengths (r_n), then it is Martin-Löf random. We proved that the condition that (r_n) is computable can be replaced by the weaker condition that (r_n) is pointedly X-computable, in the sense that r_n is uniformly computable from any extension of $X \upharpoonright_{r_n}$. It is a simple exercise to extend our proof of this fact in order to replace the condition of pointed computation with a non-uniform version of it, namely that $K(r_n \mid \tau) = \mathbf{O}(1)$ for all n and all $\tau \supseteq X \upharpoonright_{r_n}$. On the other hand, we showed that this condition is no longer sufficient for Martin-Löf randomness, if we merely require that r_n be computable from X. It would be interesting to refine this analysis and find exactly what kind of computations are allowed of a sequence (r_n) from an oracle X such that the Martin-Löf randomness of X is equivalent to the segments $X \upharpoonright_{r_n}$ being incompressible.

References

[Cha75] Gregory J. Chaitin. A theory of program size formally identical to information theory. *J. Assoc. Comput. Mach.*, 22:329–340, 1975.

[Cha87] Gregory J. Chaitin. Incompleteness theorems for random reals. *Advances in Applied Mathematics*, 8:119–146, 1987.

[DH10] Rod G. Downey and Denis Hirshfeldt. *Algorithmic Randomness and Complexity*. Springer, 2010.

[Gác74] Peter Gács. The symmetry of algorithmic information. *Dokl. Akad. Nauk SSSR*, 218:1265–1267, 1974.

[Gác86] Péter Gács. Every sequence is reducible to a random one. *Inform. and Control*, 70(2-3):186–192, 1986.

[KHMS06] Bjørn Kjos-Hanssen, Wolfgang Merkle, and Frank Stephan. Kolmogorov complexity and the recursion theorem. In *STACS*, pages 149–161, 2006.

[KHMS11] Bjørn Kjos-Hanssen, Wolfgang Merkle, and Frank Stephan. Kolmogorov complexity and the recursion theorem. *Trans. Amer. Math. Soc.*, 363, 2011.

[Kuč85] Antonín Kučera. Measure, Π^0_1-classes and complete extensions of PA. In *Recursion theory week (Oberwolfach, 1984)*, volume 1141 of *Lecture Notes in Math.*, pages 245–259. Springer, Berlin, 1985.

[ML66] Per Martin-Löf. The definition of random sequences. *Information and Control*, 9:602–619, 1966.

[MY10] Joseph S. Miller and Liang Yu. Oscillation in the initial segment complexity of random reals. *Adv. Math.*, 2010. Volume 226, Issue 6, 2011, Pages 4816–4840

[NST05] André Nies, Frank Stephan, and Sebastiaan A. Terwijn. Randomness, relativization and Turing degrees. *J. Symbolic Logic*, 70(2):515–535, 2005.