A Church-Turing thesis for randomness?*

Johanna N.Y. Franklin[1] [0000−0002−7216−1562]

Hofstra University, Hempstead NY 11590, USA
johanna.n.franklin@hofstra.edu
http://www.johannafranklin.net

Abstract. We discuss the difficulties in stating an analogue of the Church-Turing thesis for algorithmic randomness. We present one possibility and argue that it cannot occupy the same position in the study of algorithmic randomness that the Church-Turing thesis does in computability theory. We begin by observing that some evidence comparable to that for the Church-Turing thesis does exist for this statement: in particular, there are other reasonable formalizations of the intuitive concept of randomness that lead to the same class of random sequences (the Martin-Löf random sequences). However, we consider three properties that we would like a random sequence to satisfy and find that the Martin-Löf random sequences do not necessarily possess these properties to a greater degree that other types of random sequences, and we further argue that there is no more appropriate version of the Church-Turing thesis for algorithmic randomness. This suggests that consensus around a version of the Church-Turing thesis in this context is unlikely.

Keywords: Church-Turing thesis · algorithmic randomness · computability theory.

1 A potential parallel

In 1948, Turing wrote that "[I]t is found in practice that [Turing machines] can do anything that could be described as 'rule of thumb' or 'purely mechanical.' This is sufficiently well established that it is now agreed amongst logicians that 'calculable by means of a [Turing machine]' is the correct accurate rendering of such phrases" ([30], p. 4). We take this as our formulation of the Church-Turing thesis and discuss the prospects for identifying an analogous statement in the context of algorithmic randomness.

Algorithmic randomness is the study of the formalization of the intuitive concept of randomness using concepts from computability theory. We begin by considering elements of the Cantor space (the space of infinite binary sequences, or 2^ω). Therefore, a statement of the following form would be a direct parallel to Church's thesis:

> S: If an infinite binary sequence can be described as random, then it ______.

* Supported in part by Simons Foundation Collaboration Grant #420806.

The question, of course, is which mathematical property should be used to complete this statement. Is there one that occupies the same space in the universe of randomness as calculability by a Turing machine does in the universe of functions? We argue that, while there seems to be such a characterization at first glance, it appears inappropriate on further consideration, as do all other reasonable possibilities.

1.1 An initial characterization of randomness

The first formal definitions of randomness were provided in the mid-1960s and early 1970s. We review these definitions briefly below. First, though, we explain our notation. We will typically denote finite binary strings by lowercase Greek letters and infinite binary sequences by uppercase Roman letters. The length of a finite binary string τ is denoted by $|\tau|$, and the measure of a class C in Cantor space, $\mu(C)$, is given by the Lebesgue measure in which the basic open set $[\sigma]$ consisting of all infinite binary sequences extending the finite string σ has measure $2^{-|\sigma|}$ (in other words, the "coin-flip" measure).

The first approach to be fully defined is due to Martin-Löf and is based on effectivized statistical tests [19]. We recall that a Σ^0_1 class in Cantor space is one that is definable as $\{A \mid (\exists n) R(A \restriction n)\}$ for a computable relation R.

Definition 1. *A* Martin-Löf test *is a sequence $\langle V_i \rangle$ of uniformly Σ^0_1 classes of Cantor space such that $\mu(V_i) \leq 2^{-i}$. An infinite sequence A is said to be* Martin-Löf random *if for any Martin-Löf test $\langle V_i \rangle$, $A \notin \cap V_i$. We say that such a sequence is not captured by any Martin-Löf test and thus* passes *all of them.*

This is the candidate I propose to complete S: "passes all Martin-Löf tests."

The second approach is based on Kolmogorov complexity, initially defined by Kolmogorov in 1965. The prefix-free variant is due to Levin and Chaitin.

Definition 2. *[16,17,4] The* prefix-free Kolmogorov complexity *of a finite binary string σ is defined as $K(\sigma) = \min\{|\tau| \mid U(\tau) = \sigma\}$, where U is a universal prefix-free machine.*

The third approach is probabilistic and is based on Lévy's definition of a martingale [18]:

Definition 3. *A c.e. function $d : 2^{<\omega} \to \mathbb{R}^{\geq 0}$ is a* c.e. martingale *if it obeys the fairness condition*

$$d(\sigma) = \frac{d(\sigma 0) + d(\sigma 1)}{2}$$

for all σ.

Martin-Löf randomness can be defined using all of these approaches.

Theorem 1 ([27,28,4]). *The three following properties are equivalent for an infinite binary sequence A:*

1. *A is Martin-Löf random.*
2. *There is a constant c such that for all $n \in \omega$, $K(A \upharpoonright n) \geq n - c$: the Kolmogorov complexity of each initial segment of A is never much smaller than its length.*
3. *For any c.e. martingale d,* $\limsup_n d(A \upharpoonright n)$ *is finite: it is not possible to win arbitrarily large amounts of capital by betting on A using a c.e. martingale, and thus no such d* succeeds on *A*.

We note that there is not only a universal prefix-free machine but also a universal Martin-Löf test and a universal c.e. martingale.

This suggests that we can justify completing S with "passes a Martin-Löf test" with evidence similar to that given for Church's thesis: these very different approaches to formalizing the intuitive notion of randomness result in the same class of sequences being considered random just as Turing machines, register machines, general recursive functions, and the λ-calculus do for partial computable functions; Porter refers to this as an *equivalence-as-evidence-of-capturing (EEC) claim* [23]. However, we find, as Porter did, that the existence of other "loci of definitional equivalence" greatly weakens the value of this fact.

2 Other randomness notions

It was recognized in the early 1970s that the three characterizations of Martin-Löf randomness given above could be modified slightly to obtain other classes of sequences that could also reasonably be called random. For instance, we can define Schnorr randomness in each of these three ways by making each component of the definition computable rather than merely approximable from below:

– Rather than consider all Martin-Löf tests, we consider only *Schnorr tests*: those whose components have measure exactly 2^{-i} for the appropriate i rather than no larger than 2^{-i} [28].
– Rather than consider all prefix-free machines, we consider only prefix-free machines whose domains have computable measure [5].
– Rather than consider all c.e. martingales, we consider only computable martingales, and our success condition changes slightly: a martingale *d h-succeeds on A* if $\limsup_n \frac{d(A \upharpoonright n)}{h(n)} = \infty$. Here, h is taken to be an order function: a computable, nondecreasing, unbounded function on ω [27,28].

The resulting characterizations of randomness are, at worst, only slightly more complicated than the characterizations of Martin-Löf randomness we have already seen. Any increased complexity of the definitions results from the following facts: (1) there is no universal prefix-free computable measure machine, Schnorr test, or computable martingale, and (2) we have modified the definition of a martingale's success to reflect the idea that it may be possible for a martingale's values to increase unboundedly but so slowly that we cannot recognize this increase computably.

Schnorr randomness is certainly no stronger than Martin-Löf randomness: if we consider the test definitions, we can see that a sequence has to pass fewer tests in order to be Schnorr random than to be Martin-Löf random. In fact, it is a strictly weaker notion [28].

There is also a well-studied randomness notion strictly between Martin-Löf and Schnorr randomness: computable randomness, first described by Schnorr in [27,28]. Its characterizations in terms of Kolmogorov complexity and tests are far more complicated than those of either Martin-Löf or Schnorr randomness (see sections 7.1.4 and 7.1.5 of [6]), but its martingale characterization is as simple as that of Martin-Löf randomness: one simply substitutes "computable martingale" for "c.e. martingale."

The existence of these other notions of randomness would not necessarily preclude the analogy to Church's thesis given above. After all, computability theorists routinely investigate weak truth table reducibility and truth table reducibility in addition to Turing reducibility and don't consider this to contraindicate Church's thesis. We may ask whether the same sort of relationship holds between Turing, weak truth table, and truth table functionals as between Martin-Löf, computable, and Schnorr randomness.

At first, this analogy seems reasonable. Turing reducibility places no requirements on the convergence of the functional; weak truth table reducibility requires convergence within a computable bound, if such exists; and truth table reducibility requires convergence for all inputs. We can see that the characterizations of Martin-Löf randomness involve c.e. martingales and tests with components and prefix-free machines with domains that need only have lower semicomputable measures. This degree of approximability is precisely that which can be obtained from a Turing functional. The characterizations of computable randomness and Schnorr randomness, on the other hand, require computable martingales, and the components of Schnorr tests have computable measures, which better corresponds to weak truth table or truth table functionals.

While this suggests that Martin-Löf randomness is analogous to Turing reducibility and thus that "passing a Martin-Löf test" seems analogous to "being calculable by a Turing machine," we should investigate further and determine how far this analogy extends. While there are rich structural results for the Turing, weak truth table, and truth table degrees, it is the Turing degrees that have found the widest applicability to branches of computability beyond degree theory. The author knows of no results concerning truth table degrees and computable structure theory or weak truth table degrees and computable analysis, for instance. This could be a further sort of evidence for Church's thesis: that the degree structure generated by Turing functionals is the most generally applicable to other aspects of computability theory. This leads us to ask whether a similar statement can be made about Martin-Löf randomness.

3 Three desiderata

In this section, we will consider the question of applicability discussed above as well as the question of whether Martin-Löf randomness most aptly captures our intuitions about random sequences. It has certainly been argued that Martin-

Löf randomness does not capture these intuitions, most notably (and earliest) by Schnorr in [28]. We discuss some of these considerations here.

3.1 Decompositions and combinations of random sequences

We begin by considering what happens if we computably decompose a random sequence: must this result in random sequences? Or, if we interleave two random sequences, under what circumstances will the resulting sequence be random? These questions were answered for Martin-Löf randomness by van Lambalgen [15] and are closely related to the role of relativization in computability.

Theorem 2 (van Lambalgen's Theorem). *The following are equivalent for any two Martin-Löf random sequences A and B:*

1. *$A \oplus B$ is Martin-Löf random.*
2. *A is Martin-Löf random relative to B and B is Martin-Löf random relative to A.*

In short, a sequence is Martin-Löf random if, when you decompose it into its "even" and "odd" bits, each half is not only Martin-Löf random but Martin-Löf random relative to the other. This result is frequently mentioned as a desideratum for a randomness notion (see, for instance, Section 7.1.2 in [6]) and is thus a reasonable place for us to begin. We should now ask if computable and Schnorr randomness have this property as well.

The answer is complicated. It is straightforward to see that the forward direction of the theorem does not hold for computable or Schnorr randomness (see, for instance, Kjos-Hanssen's argument in [22]). However, it becomes more complicated when we consider the backward direction. This direction was long claimed to hold for both computable and Schnorr randomness with "essentially the same proof" as for Martin-Löf randomness ([6], p. 276). However, no proof was provided until Franklin and Stephan gave one for Schnorr randomness [10], and a few years later, Bauwens proved that this direction does not actually hold for computable randomness [1].

However, in keeping with the analogy between stronger reductions and weaker forms of randomness described in Section 2, it turns out that this theorem holds for all three of these randomness notions if we apply a different relativization [20,21]. This suggests that while Martin-Löf randomness initially seems to satisfy one of our intuitions about randomness in a way that computable and Schnorr randomness simply don't, it seems that our intuition is satisfied for the latter two as well when we use a more appropriate framework. Whether this more appropriate framework is as natural, though, is not apparent.

3.2 Computational strength

Now we consider the computational strength of random sequences. It is fair to say that no random sequence should be computable: if it were, then we could predict it perfectly. Thus, random sequences should possess some noncomputable information. However, we can also argue that no random sequence should be very powerful computationally: if a sequence is random, then we should not be able to make any practical use of the information it possesses, and therefore it should not be contained in a powerful Turing degree.

However, Kučera proved that every Turing degree computing $\mathbf{0}'$ contains a Martin-Löf random sequence [14]. Furthermore, Stephan proved that the Martin-Löf random sequences that cannot compute $\mathbf{0}'$ are computationally weaker in another way: they are precisely the Martin-Löf random sequences that cannot compute a complete extension of Peano Arithmetic [29]. These results led to Hirschfeldt's argument that there are two types of Martin-Löf random sequences: those that are computationally weak and thus truly random, and those that are computationally strong and therefore "know enough" to pretend to be random (see [6], pp. 228–229).

If we take a measure of computational uselessness as a desideratum for a randomness notion, it is clear that not only does Martin-Löf randomness not meet this criterion, but neither do Schnorr and computable randomness since every Martin-Löf random sequence is Schnorr random and computably random. However, there are other randomness notions, and one of these satisfies this intuition perfectly.

Difference randomness was introduced by Franklin and Ng in [9]. This notion is most naturally defined using the test approach: while each component of a Martin-Löf test is a Σ_1^0 class, each component of a difference test is a difference of two Σ_1^0 classes. This means that, rather than creating a component by simply adding open neighborhoods $[\sigma]$ to the class, we create a component by adding such neighborhoods and then perhaps removing them or their subneighborhoods. Franklin and Ng further proved that the difference random sequences are precisely the Martin-Löf random sequences that cannot compute $\mathbf{0}'$ and thus that difference randomness satisfies this intuition in a way no other notion does [9].[1] However, difference randomness does not satisfy many of the other criteria we have discussed so far: while its test definition is straightforward to state, its martingale definition is rather complicated, and no Kolmogorov complexity-based definition of it is known at this point.

3.3 Applications

Finally, we turn our attention to the last desideratum: we would like our notion of randomness to appear naturally in other branches of computability theory. We consider the case of computable analysis, the subfield that is most closely connected to algorithmic randomness as of this writing. Since many theorems in analysis hold on a conull set and all but measure 0 many points in a space

[1] We note that there are other randomness notions that also exhibit computational weakness, e.g., weak 2-randomness. However, we discuss difference randomness here because the difference random sequences can be identified as the Martin-Löf random sequences that are computationally weak in these two standard senses.

are random by any reasonable definition of randomness, it is natural to try to characterize the points in a computable probability space for which a certain theorem holds as the points in that space that are random under a certain definition.[2]

We consider several theorems as case studies, beginning with Birkhoff's ergodic theorem; this theorem states that for any measurable subset of a probability space, an ergodic transformation will map almost every point into that subset with a frequency proportional to the measure of the subset.

Theorem 3 (Birkhoff's ergodic theorem). *Let (X, μ) be a probability space, let $T : X \to X$ be ergodic, and let E be a measurable subset of X. Then for almost all $x \in X$,*

$$\lim_{n\to\infty} \frac{|\{i \mid i < n \text{ and } T^i(x) \in E\}|}{n} = \mu(E).$$

To connect this theorem to algorithmic randomness, we must first frame it as a statement about individual points in the space. While the definition of a Birkhoff point arises naturally from Birkhoff's ergodic theorem, weak Birkhoff points are appropriate for a generalization of Birkhoff's ergodic theorem for measure-preserving functions.

Definition 4. *A point $x \in X$ is a* Birkhoff point for T *with respect to a class of sets $\mathcal{C}$ if for all $E \in \mathcal{C}$,*

$$\lim_{n\to\infty} \frac{|\{i \mid i < n \text{ and } T^i(x) \in E\}|}{n} = \mu(E).$$

A point $x \in X$ is a weak Birkhoff point for T *with respect to a class of sets $\mathcal{C}$ if for all $E \in \mathcal{C}$, the above limit simply exists.*

We can now consider a theorem template; note that in order to state such a theorem precisely, we must include the type of transformation under consideration (ergodic or measure preserving) and the class of sets under consideration (computable or lower semicomputable).

Theorem template 1 *A point is a (weak) Birkhoff point for computable ______ T with respect to ______ sets if and only if it is ______ random.*

We synthesize the known results in Table 1.

We now turn our attention to differentiability and convergence of Fourier series; differentiability is considered in more depth in this context by Porter in [24]. We again have a theorem template, and in these cases, we only need to know what sort of functions we are considering the differentiability of or the Fourier series of.

[2] The reader may have noted that we are working in a general computable probability space rather than the Cantor space. This is possible because any computable probability space is isomorphic to the Cantor space in every relevant way and our notions of randomness transfer naturally [13].

Table 1. Birkhoff's ergodic theorem and randomness

	Transformation	
	Ergodic	Measure-preserving
Computable	Schnorr [12]	Martin-Löf [31,11]
Lower semicomputable	Martin-Löf [2,7]	?

Theorem template 2 *Every computable ______ function f is differentiable at $z \in [0,1]$ if and only if z is ______ random.*

Theorem template 3 *Every computable ______ function f's Fourier series converges at t_0 if and only if t_0 is ______ random.*

Brattka, J. Miller, and Nies proved that each computable nondecreasing function $f : [0,1] \to \mathbb{R}$ is differentiable at a point z if and only if z is computably random and that each computable function $f : [0,1] \to \mathbb{R}$ of bounded variation is differentiable at a point z if and only if z is Martin-Löf random [3]; Rute has a similar result for Schnorr randomness that is more complicated to state [25]. Later, Franklin, McNicholl, and Rute proved that the convergence of a Fourier series for a computable function f in $L^p[-\pi,\pi]$ at a point t_0 is essentially equivalent to the Schnorr randomness of t_0 [8].[3]

Both Schnorr randomness and Martin-Löf randomness make repeated appearances in this area; computable randomness has appeared less often. It does not appear that Martin-Löf randomness is primary in this context, and in fact Rute has argued that Schnorr randomness "stands out" as having "very strong connections to constructive and computable measure theory" ([26], p. 60).

4 Conclusion

It seems clear that Martin-Löf randomness does not hold the primacy of place in the context of algorithmic randomness that Turing functionals do in the context of basic computability. While Turing functionals are by far the most useful kind in classical computability theory, it seems that the same is not true for Martin-Löf random sequences in algorithmic randomness. While Martin-Löf randomness is straightforwardly defined in all the frameworks we consider and Martin-Löf random sequences can be decomposed or combined into other Martin-Löf random sequences as expected, it lacks the desired computational weakness and certainly does not stand out in the context of applications to computable analysis.

This suggests that giving a formal definition of Martin-Löf randomness is not the correct way to complete our statement S. It does not seem, though, that a formal definition of any other randomness notion would be correct, either: there is no more consistent evidence for any of the other notions we've discussed. Therefore, one of the most important forms of evidence for the Church-Turing thesis

[3] There is a subtlety in this result in that an incomputable function may be computable as a vector, hence the "essentially."

is missing in the context of algorithmic randomness, and we cannot reasonably provide an equivalent version for this context.

I suggest that this failure is due to the fact that randomness is a higher-order property than computability. To define a randomness notion formally, we need to state the level of computability of the measures of the test components, the measures of the prefix-free machines, or the martingales and we may need consider the martingale's rate of growth. Porter presents an excellent analysis of the ingredients of a formal definition of a randomness notion in [23]: each definition must have a *hallmark of randomness*, a *collection of underlying resources*, and an *implementation of these resources*. With so many factors in play, it seems unlikely that we will ever have consensus around a version of the Church-Turing thesis for algorithmic randomness.

References

1. Bauwens, B.: Uniform van Lambalgen's theorem fails for computable randomness. ArXiv e-prints (Oct 2015)
2. Bienvenu, L., Day, A., Mezhirov, I., Shen, A.: Ergodic-type characterizations of Martin-Löf randomness. In: 6th Conference on Computability in Europe (CiE 2010), Lecture Notes in Comput. Sci., vol. 6158, pp. 49–58. Springer, Berlin (2010)
3. Brattka, V., Miller, J.S., Nies, A.: Randomness and differentiability. Trans. Amer. Math. Soc. **368**(1), 581–605 (2016). https://doi.org/10.1090/tran/6484, http://dx.doi.org.ezproxy.hofstra.edu/10.1090/tran/6484
4. Chaitin, G.J.: A theory of program size formally identical to information theory. J. Assoc. Comput. Mach. **22**, 329–340 (1975)
5. Downey, R.G., Griffiths, E.J.: Schnorr randomness. J. Symbolic Logic **69**(2), 533–554 (2004)
6. Downey, R.G., Hirschfeldt, D.R.: Algorithmic Randomness and Complexity. Springer (2010)
7. Franklin, J.N., Greenberg, N., Miller, J.S., Ng, K.M.: Martin-Löf random points satisfy Birkhoff's ergodic theorem for effectively closed sets. Proc. Amer. Math. Soc. **140**(10), 3623–3628 (2012)
8. Franklin, J.N., McNicholl, T.H., Rute, J.: Algorithmic randomness and Fourier analysis. Theory Comput. Syst. **63**(3), 567–586 (2019). https://doi.org/10.1007/s00224-018-9888-8, https://doi-org.ezproxy.hofstra.edu/10.1007/s00224-018-9888-8
9. Franklin, J.N., Ng, K.M.: Difference randomness. Proc. Amer. Math. Soc. **139**(1), 345–360 (2011)
10. Franklin, J.N., Stephan, F.: Van Lambalgen's Theorem and high degrees. Notre Dame J. Formal Logic **52**(2), 173–185 (2011)
11. Franklin, J.N., Towsner, H.: Randomness and non-ergodic systems. Mosc. Math. J. **14**(4), 711–744 (2014)
12. Gács, P., Hoyrup, M., Rojas, C.: Randomness on computable probability spaces—a dynamical point of view. Theory Comput. Syst. **48**(3), 465–485 (2011). https://doi.org/10.1007/s00224-010-9263-x, http://dx.doi.org/10.1007/s00224-010-9263-x

13. Hoyrup, M., Rojas, C.: Computability of probability measures and Martin-Löf randomness over metric spaces. Inform. and Comput. **207**(7), 830–847 (2009). https://doi.org/10.1016/j.ic.2008.12.009, http://dx.doi.org/10.1016/j.ic.2008.12.009
14. Kučera, A.: Measure, Π^0_1-classes and complete extensions of PA. In: Recursion theory week (Oberwolfach, 1984), Lecture Notes in Math., vol. 1141, pp. 245–259. Springer, Berlin (1985)
15. van Lambalgen, M.: The axiomatization of randomness. J. Symbolic Logic **55**(3), 1143–1167 (1990)
16. Levin, L.A.: Some Theorems on the Algorithmic Approach to Probability Theory and Information Theory. Ph.D. thesis, Moscow University (1971)
17. Levin, L.A.: Laws on the conservation (zero increase) of information, and questions on the foundations of probability theory. Problemy Peredači Informacii **10**(3), 30–35 (1974)
18. Lévy, P.: Téorie de l'Addition des Variables Aléatoires. Gauthier-Villars, Paris (1937)
19. Martin-Löf, P.: The definition of random sequences. Information and Control **9**, 602–619 (1966)
20. Miyabe, K.: Truth-table Schnorr randomness and truth-table reducible randomness. MLQ Math. Log. Q. **57**(3), 323–338 (2011). https://doi.org/10.1002/malq.200910128, http://dx.doi.org/10.1002/malq.200910128
21. Miyabe, K., Rute, J.: van Lambalgen's theorem for uniformly relative Schnorr and computable randomness. In: Downey, R., et al. (eds.) Proceedings of the Twelfth Asian Logic Conference, pp. 251–270. World Scientific (2013)
22. Nies, A.: Computability and Randomness. Clarendon Press, Oxford (2009)
23. Porter, C.P.: The equivalence of definitions of algorithmic randomness. Philosophia Mathematica To appear.
24. Porter, C.P.: On analogues of the Church-Turing thesis in algorithmic randomness. Rev. Symb. Log. **9**(3), 456–479 (2016). https://doi.org/10.1017/S1755020316000113, https://doi-org.ezproxy.hofstra.edu/10.1017/S1755020316000113
25. Rute, J.: Topics in Algorithmic Randomness and Computable Analysis. Ph.D. thesis, Carnegie Mellon University (2013)
26. Rute, J.: Algorithmic randomness and computable measure theory. In: Franklin, J.N., Porter, C.P. (eds.) Algorithmic Randomness: Progress and Prospects, pp. 58–114. Cambridge University Press, New York, NY (2020)
27. Schnorr, C.: A unified approach to the definition of random sequences. Math. Systems Theory **5**, 246–258 (1971)
28. Schnorr, C.: Zufälligkeit und Wahrscheinlichkeit, Lecture Notes in Mathematics, vol. 218. Springer-Verlag, Heidelberg (1971)
29. Stephan, F.: Martin-Löf Random and PA-complete Sets. Tech. Rep. 58, Matematisches Institut, Universität Heidelberg, Heidelberg (2002)
30. Turing, A.M.: Intelligent machinery. Tech. rep., National Physical Laboratory (1948)
31. V′yugin, V.V.: Effective convergence in probability, and an ergodic theorem for individual random sequences. Teor. Veroyatnost. i Primenen. **42**(1), 35–50 (1997). https://doi.org/10.1137/S0040585X97975915, http://dx.doi.org/10.1137/S0040585X97975915