Martin-Löf randomness and Schnorr randomness

March 21, 2025

1 Martin-Löf randomness

Definition 1.1. A set $\mathscr{A} \subseteq 2^\omega$ has MEASURE 0 iff $\forall \varepsilon > 0$ there is an open set G_ε sets such that $\mu(G_\varepsilon) < \varepsilon$, and $\mathscr{A} \subseteq \bigcap_\varepsilon G_\varepsilon$.

Example 1.2. A singleton set $\{r\}$ has measure 0, since for every $\varepsilon > 0$, we can construct the sequence $\left(r - \frac{\varepsilon}{2}, r + \frac{\varepsilon}{2}\right)$. It is possible to extend the idea to show that countably infinite sets have measure 0. Consequently, rationals form a measure 0 set.

Example 1.3. We want to show that the set of all binary sequences in which *some* finite string is absent, has probability 0. This is also called the set of *non-disjunctive sequences.*

Consider the set of all binary sequences which does not contain a specific pattern, say 01. Define, for $i \geq 0$, $S_i : 2^\omega \to \{0,1\}$ by

$$S_i^{01}(X) = \begin{cases} 1 & \text{if } X_i X_{i+1} \neq 01 \\ 0 & \text{otherwise.} \end{cases}$$

Example 1.4. which attains 1 exactly on the set of sequences which do not have 01 at the i^{th} position. We want $P\left[\cap_{i \in \mathbb{N}} 1^{-1}\left(S_i^{01}\right)\right]$. This is not easy to compute exactly, since S_is are dependent - for example, 01 occurring in the first position forbids it occurring in the second position. However, it is easy to see that $S_0^{01}, S_2^{01}, S_4^{01}, \dots$ are independent random variables, since $P\left[S_{2\ell}^{01} = 1 | S_{2j_1}^{01}, \dots, S_{2j_k}^{01}\right] = P[S_{2\ell}^{01} = 1]$, for any finite collection of even indexed random variables $S_{2j_1}^{01}, \dots, S_{2j_k}^{01}$, where $S_{2\ell}^{01} \notin \left\{S_{2j_1}^{01}, \dots, S_{2j_k}^{01}\right\}$. Moreover, $P\left[\cap_i 1^{-1}\left(S_i^{01}\right)\right] \leq P\left[\cap_i 1^{-1}\left(S_{2i}^{01}\right)\right]$. We have, by independence,

$$P\left[\cap_i 1^{-1}\left(S_{2i}^{01}\right)\right] = \prod_i P\left(1^{-1}\left(S_{2i}^{01}\right)\right) = \lim_{n \to \infty} \prod_{i=0}^{n} P\left(1^{-1}\left(S_{2i}^{01}\right)\right) = \lim_{n \to \infty} \left(\frac{3}{4}\right)^n = 0,$$

hence $P\left[\cap_{i \in \mathbb{N}} 1^{-1}\left(S_i^{01}\right)\right] = 0$.

Since the number of finite strings is countable, taking a countable union over all such specific finite strings $w \in 2^{<\omega}$, (replacing appropriately, 3/4 in the above calculation with $\left(1 - \frac{1}{2^{|w|}}\right)$),we conclude that the set of non-disjunctive sequences, $\cup_{w \in 2^{<\omega}} \cap_{i \in \mathbb{N}} S_i^w$, has measure 0.

Martin-Löf effectivized the notion of a measure 0 set to define a *constructive* measure 0 set, by requiring first, that there is a uniform enumeration of the open sets G_m. Additionally, the measure of the open sets also decreases in an "effective" manner - we require that the measures of the sets have upper bounds uniformly computable in m, the index of the open set in the sequence.

Definition 1.5. A sequence of open sets $\langle G_m \rangle_{m \in \mathbb{N}}$ is called a MARTIN-LÖF TEST if the sequence is uniformly c.e. and for every $m \in \mathbb{N}$,we have $\mu(G_m) \leq 2^{-n}$. An infinite binary sequence $Z \in 2^\omega$ FAILS the test if $Z \in \bigcap_m G_m$.

Theorem 1.6. *There is a universal Martin-Löf test.*

Proof. Let $\langle G^e_m \rangle_{e,m\in\mathbb{N}}$ be an uniform c.e. enumeration of open sets such that for every $e,m \in \mathbb{N}$, $\mu(G^e_m) \leq 2^{-m}$. Then define, for $b \in \mathbb{N}$, the set $U_b = \cup_{e\in\mathbb{N}} G^e_{e+b+1}$. Since it is a c.e. union of uniformly c.e. open sets, each U_b is c.e. open. It is also easy to see that U_bs are uniformly computably enumerable in b. Further, we have

$$\mu(U_b) \leq \sum_{e\in\mathbb{N}} \mu(G^e_{e+b+1}) \leq \sum_{e\in\mathbb{N}} 2^{e+b+1} = 2^b.$$

Now, suppose that $Z \in 2^\omega$ is not MLrandom. Then for some $e \in \mathbb{N}$, $Z \in \cap_m G^e_m$. By definition, for each $b \in \mathbb{N}$, $Z \in U_b$, *i.e.* $Z \in \cap_b U_b$. □

The universal Martin-Löf test defines the *largest* constructive measure 0 set, say $\mathscr{S}$. Since each test captures some "randomness deficiency", the set $\mathscr{S}$ is the set of sequences which have randomness deficiency identifiable by a "constructive" test, as realized by a Martin-Löf test. Hence, the complement of $\mathscr{S}$, the smallest constructive measure 1 set, is the set of all "random" sequences. This set of sequences are now called *Martin-Löf random sequences.*

Definition 1.7. A sequence is MARTIN-LÖF RANDOM *if it is an element of the smallest constructive measure 1 set.*

Example 1.8. Adapting the estimate in Example 1.3, we can show that the set of disjunctive sequences has constructive measure 0. [Exercise] This shows that every Martin-Löf random is disjunctive - *i.e.* every finite string appears in every Martin-Löf random.

Example 1.9. A computable $Z \in 2^\omega$ is not MLR. Consider $G_m = [Z \upharpoonright m]$. Then $\langle G_m \rangle_{m\in\mathbb{N}}$ is a Martin-Lof test: it is clear that G_ms are uniformly c.e. Moreover, for every $m \in \mathbb{N}$, $\mu(G_m) \leq 2^{-m}$.

The natural next question is whether we can show that every c.e. sequence is non-random. We introduce the notion of a LEFT-C.E. REAL. A real number r is left-c.e. if its left cut, the set of rationals less than r, is c.e. - *i.e.* $\{q \in \mathbb{Q} \mid q < r\}$ is c.e.

Let S be an infinite language. Then its characteristic sequence χ_S is defined by $\chi_S[i] = 1$ if the i^{th}string in the standard enumeration is an element of S, otherwise $\chi_S[i] = 0$. If S is computably enumerable, then χ_S is a left-c.e. real - consider, for every $k \in \mathbb{N}$, the set $S \upharpoonright k$ of the set of all strings of length at most k which is accepted within k steps by a fixed machine accepting S. Since S is infinite, it follows that $\chi_{S\upharpoonright k}$ is a rational which is strictly less than χ_S. The sequence $\chi_{S[k]}$, $k \in \mathbb{N}$, can be used to show that χ_S is left-c.e.

Now we pose the question: is every left-c.e. real non-random? We expect the answer to be yes, since such sequences are approximable from below by Turing machines, even though the rate of convergence to the limit may not be computable. Surprisingly, however, there are random left-c.e. reals. The most famous such example is Chaitin's Ω, described in the following example.

Example 1.10. It is not true that every left c.e. real is random. Consider the following sequence, called Chatin's Ω:

$$\Omega = \sum_{\substack{p\in\mathscr{P} \\ U(p)\downarrow}} \frac{1}{2^{|p|}}.$$

This is at most 1 by Kraft's inequality. Moreover, it is left c.e. by a series of approximations $\langle \Omega_s \rangle_{s\in\mathbb{N}}$ which consider the summands corresponding to programs that halt by the s^{th}step.

$$\Omega_s = \sum_{\substack{p\in\mathscr{P} \\ U(p)[s]\downarrow}} \frac{1}{2^{|p|}}.$$

Why is Ω incompressible? It is possible to show that given the first n bits of Ω, we can decide whether all programs of length $\leq n$ halt. [Homework] This then makes it possible to comptue the first string x in the standard ordering of strings with $K(x) > n$. But this is possible only for finitely many strings (see below, the discussion on K).

Example 1.10 shows perhaps that the notion of Martin-Lof randomness is not a very "strong" notion of randomness. We will see when we study the interaction of Turing reducibility and Martin-Lof randomness, another sense in which this notion has some weakness.

2 Equivalent characterizations of Martin-Löf randoms

2.1 Characterization using martingales

We defined ML non-randoms using constructive measure 0 sets. Another very useful way to look at ML non-randoms is that there are betting strategies which can succeed in making unbounded amounts of money by betting on them. This approach uses the notion of "martingales", which are fair betting strategies.

In the following exposition, we will not give the general definition of a martingale, which requires measure theory, and the notion of filtrations of σ-algebras. We will, instead, use the definition specialized for 2^{ω}, as defined by Schnorr, and independently developed in the works of J. Lutz and others.

Definition 2.1. A MARTINGALE $m : 2^{<\omega} \to [0,\infty)$ is a function which satisfies the following conditions:

1. [finite initial capital] $m(\lambda) \leq 1$

2. [fairness] for every $w \in 2^{<\omega}$, we have $m(w) = \frac{m(w0)+m(w1)}{2}$.

If condition 2 is replaced by $m(w) \geq \frac{m(w0)+m(w1)}{2}$, then m is called a SUPERMARTINGALE.

The intuition is that a martingale is a "fair betting" strategy, betting on the binary tree. The martingale m starts with a finite initial capital, $m(\lambda)$, which is upper bounded by 1. At any string $w \in 2^{<\omega}$, the martingale m bets on its extensions $w0$ and $w1$. The fairness condition (condition 2) says that the expected amount of money after the next bet, *i.e.* $\frac{m(w0)+m(w1)}{2}$, is equal to the present capital, $m(w)$. Thus on an average, m neither loses nor wins money.

Of course, this does not prevent m from making unbounded amounts of money on some specific paths along the binary tree, as long as the set of those paths have 0 measure. This observation establishes a connection between measure 0 sets and the success of martingales. We formally define the notion of a martingale succeeding, as follows.

Definition 2.2. A martingale $m : 2^{<\omega} \to [0,\infty)$ SUCCEDS on $Z \in 2^{\omega}$ if

$$\limsup_{n\to\infty} m(Z \upharpoonright n) = \infty.$$

The following inequality bounds the probability of success of a martingale.

Lemma 2.3. *(Kolmogorov inequality) Let* $m : 2^{<\omega} \to [0,\infty)$ *be a martingale. Then* $\mu\left(Z \in 2^{\omega} \mid \exists n\ m(Z \upharpoonright n) > N\right) < \frac{1}{N}$.

Definition 2.4. The above notion is classical, and we now impose computability restrictions on it. Contrary perhaps to our expectation, we do not insist that the martingale is computable, but only that there are computable approximations to the value from below.

Definition 2.5. A martingale $m : 2^{<\omega} \to [0,\infty)$ is called LOWER SEMICOMPUTABLE (or CONSTRUCTIVE) if there is a total computable function $\hat{m} : 2^{<\omega} \times \mathbb{N} \to [0,\infty) \cap \mathbb{Q}$ such that the following conditions hold.

1. [monotonicity from below] For every $w \in 2^{<\omega}$ and every $n \in \mathbb{N}$, we have $\hat{m}(w,n) \leq \hat{m}(w,n+1) \leq m(w)$.

2. [(non-effective) convergence] For every $w \in 2^{<\omega}$, we have $\lim_{n\to\infty} \hat{m}(w,n) = m(w)$.

Lemma 2.6. *For every lower semicomputable martingale* $m : 2^{\omega} \to [0,\infty)$*, there is a Martin-Löf test* $\langle G_i \rangle_{i\in\mathbb{N}}$ *such that every infinite binary sequence on which m succeeds, is in* $\cap_{i\in\mathbb{N}} G_i$*. Conversely, for every Martin-Löf test* $\langle G_i \rangle_{i\in\mathbb{N}}$*, there is a lower semicomputable martingale* $m : 2^{\omega} \to [0,\infty)$ *which succeeds on every infinite sequence in* $\cap_{i\in\mathbb{N}} G_i$*.*

Proof. Denote, for every $x \in 2^{<\omega}$, the set of all infinite binary sequences with x as a prefix, by $[x]$.

Let $\langle G_i \rangle_{i\in\mathbb{N}}$ be the universal Martin-L{̈o}f test. For each $i \in \mathbb{N}$, define $m_i : 2^{<\omega} \to [0,\infty)$ by

$$m_i(x) = \mu(G_i \cap [x])2^{|x|}.$$

Then $m_i(\lambda) \leq 2^{-i}$, and for every $x \in 2^{<\omega}$, we have

$$\frac{m(x0)+m(x1)}{2} = \frac{\mu(G_i \cap [x0])2^{|x0|} + \mu(G_i \cap [x1])2^{|x1|}}{2} = \frac{\mu(G \cap [x0]) + \mu(G \cap [x1])}{2}2^{|x|+1} = \frac{\mu(G \cap [x])}{2}2^{|x|+1} = m(x),$$

where the third equality follows since μ is a probability measure. Hence m_i is a martingale.

Note that for every $X \in 2^\omega$, for every prefix x of X inside G_i, we have $m_i(x) = \mu(G_i \cap [x])2^{|x|} = \mu([x])2^{|x|} = 1$.

Now, define the function $m : 2^\omega \to [0,\infty)$ by $m = \sum_{i\in\mathbb{N}} m_i$. We can easily verify that m is a lower semicomputable martingale. Also, if $X \in \cap_{i\in\mathbb{N}} G_i$. Then, for each $i \in \mathbb{N}$, we conclude that $\limsup_{n\to\infty} m(x) = \infty$.

Conversely, let $m : 2^\omega \to [0,\infty)$ be a lower semicomputable martingale. Then, for every $i \in \mathbb{N}$ consider the set $G_i = \{Z \in 2^\omega \mid \exists n\ m(Z \restriction n) > 2^i\}$. It is easy to verify that G_is are uniformly c.e. open in i. Moreover, by the Kolmogorov inequality, $\mu(G_i) \le 2^i$. If $\limsup_n m(Z \restriction n) = \infty$, then $Z \in \cap_{i\in\mathbb{N}} G_i$. □

Corollary 2.7. *There is a universal semicomputable martingale.*

Proof. This is the martingale which corresponds to the universal MLtest. □

Since a sequence is Martin-Löf random if and only if it fails the universal MLtest, we have the following.

Theorem 2.8. *X is Martin-Löf random if and only if the universal constructive martingale fails on it.*

2.2 Characterization using incompressibility

Let $\mathscr{P} \subseteq 2^{<\omega}$ be a prefix-free set, *i.e.* if a string x is in $\mathscr{P}$, then no proper prefix of x, or a proper extension of x can be in $\mathscr{P}$.

Example 2.9. The set $\{0^n1 \mid n \in \mathbb{N}\}$ is an infinite prefix-free set.

...

Prefix-free sets are quite sparse. The following lemma is an important property of prefix-free sets, and captures a sense in which they are sparse.

Lemma 2.10. *(Kraft inequality) If $\mathscr{P} \subseteq 2^\omega$ is a prefix-free set, then we have $\sum_{x\in\mathscr{P}} 2^{-x} \le 1$.*

Proof. Consider the following experiment: we toss an unbiased fair coin multiple times, marking the outcome as 1 if Heads, and 0 if tails until we either hit an element in $\mathscr{P}$ and stop, or we toss forever. Then the probability of hitting an $x \in \mathscr{P}$is exactly 2^{-x}. By the prefix-free property, along any one sequence of trials, we can hit at most one element of $\mathscr{P}$. Thus, the probability that our experiment halts and produces some element of $\mathscr{P}$ is exactly $\sum_{x\in\mathscr{P}} 2^{-|x|}$. Since this is the probability of an event in a well-defined probability space, it is at most 1. □

Fix a prefix-free machine M. Consider the following cylinder sets:

$$R_b^M = \left[\left\{x \in 2^{<\omega} \mid K_M(x) \le |x| - b\right\}\right].$$

This is the set of all infinite binary sequences with some b-compressible prefix.

Lemma 2.11. *$\langle R_b^M \rangle_{b\in\mathbb{N}}$ is a Martin-Löf test.*

Proof. The condition $K_M(x) \le |x| - b$ is equivalent to checking that there is some prefix-free program σ such that $M(\sigma) = x$, and $|\sigma| \le |x| - b$. Hence the sets R_b^M are c.e. uniformly in b**.**

Now we show that $\mu(R_b^M) \le 2^{-b}$. Consider $S_b^M = \{x \in 2^{<\omega} \mid K_M(x) \le |x| - b\}$, and let $V_b^M \subset S_b^M$ be the subset of strings which are minimal under the prefix ordering - that is, if x, y are both in S_b^M and y extends x, then $y \notin V_b^M$. Then

$$\sum_{x\in V_b^M} \frac{1}{2^{|x|}} = \mu(R_b^M).$$

Let $x \in V_b^M$ and let σ_x be a shortest M-description of x. Since $|\sigma_x| \le |x| - b$,we have $2^{-|\sigma_x|} \ge 2^b 2^{-|x|}$. Then

$$1 \ge \sum_{x\in V_b^M} \frac{1}{2^{|\sigma_x|}} \ge 2^b \sum_{x\in V_b^M} \frac{1}{2^{|x|}} = 2^b \mu(R_b^M),$$

from which it follows that $\mu(R_b^M) \le 2^{-b}$. □

The following result relies on a technique called Levin's coding theorem. See Nies 09 for an exposition. We skip the proof of Levin's coding theorem since it is technical.

Theorem 2.12. *A sequence $X \in 2^\omega$ is Martin-Löf random iff $\exists b \forall n \; K(X \upharpoonright n) > n - b$, equivalently, $X \notin R_b^M$.*

Proof. By the previous lemma, $\langle R_b^M \rangle_{b \in \mathbb{N}}$is a Martin-Löf test. Hence, if there is a b such that $X \notin R_b^M$, then X is MLrandom.

Now, suppose $\langle G_m \rangle_{m \in \mathbb{N}}$ is a Martin-Löf test and $X \in \cap_m G_m$. We can assume that $\mu(G_m) \leq 2^{-2m}$.

We form a BOUNDED REQUEST SET L.

We obtain, uniformly in m, an antichain $\langle x_i^m \rangle_{i < N_m}$, such that $G_m = [\{x_i^m \mid i < N_m\}]$.

Let

$$L = \{(x_i^m, |x_i^m| - m + 1) \;\mid\; m \in \mathbb{N}, i < N_m\}\,.$$

Since $\mu(G_m) \leq 2^{-2m}$, the contribution of G_m to L is at most $2^{-2m+m-1} = 2^{-m-1}$, hence L is a bounded request set.

Let M_d be the prefix-free machine for L given by Levin's coding theorem. Fix $b \in \mathbb{N}$ and let $m = b + d + 1$. Since $X \in G_m$, we have a prefix x_i^m of X for some i. Thus, $K(x_i^m) \leq |x_i^m| - m + 1 + d = |x| - b$. □

3 Facts about Martin-Löf randoms

This material is adapted from Section 3.2 of Nies 2009. We formulate the proofs in terms of Martin-Löf tests, whereas Nies uses K-incompressibility.

Definition 3.1. $Z \in 2^\omega$ satisfies the strong law of large numbers if

$$\lim_{n \to \infty} \frac{\sum_{i=0}^{n-1} Z_i}{n} = \frac{1}{2}.$$

Theorem 3.2. Every Martin-Löf random satisfies the strong law of large numbers.\

Proof. For $m, n \in \mathbb{N}$, define

$$B_{m,n} = \left\{ w \in 2^n \mid \left| \sum_{i=0}^{n-1} w_i - \frac{n}{2} \right| \geq \frac{1}{2^m} \right\}.$$

Using Chernoff bound (see, for example, Corollary 4.6 of Mitzenmacher, Upfal, second edition), we have

$$P(B_{mn}) \leq 2e^{-n/2 \times (2^{-2m}/3)}.$$

Let $B_m = \cup_{n \in \mathbb{N}} B_{m,n}$. Then, we have

$$P(B_m) = P\left(\bigcup_{n \in \mathbb{N}} B_{m,n} \right) \leq \sum_{n \in \mathbb{N}} 2e^{-n/2 \times (2^{-2m}/3)} = 2e^{-2m/6}.$$

Hence, C_m defined to be □

Theorem 3.3. *Suppose $Y \in 2^\omega$ is a tail of $Z \in 2^\omega$. Then Y is ML-random if and only if Z is ML-random*

Proof. Suppose G_m is an open set containing Z with measure less than 2^{-m}, and $Z = \sigma Y$ for some finite string σ. Let $T : [0,1] \to [0,1]$ denote the left-shift defined by $Tx = 2x \mod 1$. We observe that $T^{|\sigma|} Z = Y$.

Since G_m contains Z, it follows that $T^{|\sigma|}(G_m)$ contains Y. By induction on the length of any finite string τ, it is possible to show that $\mu\left[T^{|\tau|}(G_m)\right] \leq 2^{|\tau|} \mu[G_m]$.

Hence, $\left\langle T^{|\sigma|}(G_{m+|\sigma|}) \right\rangle_{m \in \mathbb{N}}$ is a Martin-Löf test for Y. □

Generalizing the technique, we get the following theorem.

Lemma 3.4. *Suppose $f : \mathbb{N} \to \mathbb{N}$ is a computable 1-1 function. If $X \in 2^\omega$ is MLrandom, then so is $f^{-1}(X)$.*

4 van Lambalgen's Theorem

<to be added>

5 The Kučera-Gács Theorem

This theorem shows a surprising interaction between Turing reducibility and Martin-Löf randomness. Intuitively, we do not expect any meaningful data (*e.g.* non-random data) to be computed from random data - for example, van Lambalgen's theorem implies that the bits in the even bits of a Martin-Löf random are themselves Martin-Löf random. On the other hand, the following theorem shows that for *any* data, there is *some* Martin-Löf random from which we can compute it.

We follow the proof by Merkle and Mihailovic, which utilizes martingales. The overview of the martingale argument is as follows: pick the universal constructive martingale. Since it wins only on a measure 0 subset of 2^ω, any finite string r must have two extensions on which the the martingale loses money, a left path and a right path. We define an infinite sequence R by finite extension along one of these losing paths at each stage. If our given infinite sequence X has 0 at the current position, then R chooses the left path, otherwise, R chooses the right path. Since the martingale loses money, R is random, and by construction, $X \leq_T R$.

Lemma 5.1. *(Space Lemma) Given a rational $\delta > 1$ and an integer k>0, we can compute a length $\ell(\delta,k)$ such that for any martingale $m : 2^{<\omega} \to [0,1)$ and any σ,*

$$\left|\left\{\tau \in 2^{\ell(\delta,k)} \mid m(\sigma\tau) \leq \delta m(\sigma)\right\}\right| \geq k.$$

Proof. By Kolmogorov inequality, we have

$$\frac{\left|\left\{\tau \in 2^{\ell(\delta,k)} \mid m(\sigma\tau) > \delta m(\sigma)\right\}\right|}{2^{\ell(\delta,k)}} \leq \frac{1}{\delta}.$$

Let $\ell(\delta,k) = \lceil \log \frac{k}{1-\frac{1}{\delta}} \rceil$. Then

$$\left|\left\{\tau \in 2^{\ell(\delta,k)} \mid m(\sigma\tau) \leq m(\sigma)\right\}\right| \leq 2^{\ell(\delta,k)} - \frac{2^{\ell(\delta,k)}}{\delta} = \frac{k}{1-\delta^{-1}} - \frac{k}{\delta(1-\delta^{-1})} = \frac{k}{1-\delta^{-1}}\left(1-\delta^{-1}\right) = k.$$

□

We want to encode an arbitrary sequence $X \in 2^\omega$ into an MLR Y. Clearly, X cannot be coded into Y as a subsequence at easily recognized locations. Thus, it is difficult to try $X \leq_m$R. However, we show that $X \leq_{\text{wtt}} R$. The idea is to encode X at the "bad" locations for the universal martingale as provided by the Space Lemma above.

Theorem 5.2. *For any $X \in 2^\omega$, there is a Martin-Löf random $R \in 2^\omega$ such that $X \leq R$.*

Proof. Let $m : 2^\omega \to [0,\infty)$ be a universal c.e. martingale. Assume that $\liminf_n m(R \upharpoonright n) < \infty$.

Let $r_0 > r_1 > \ldots$ be a sequence of positive rationals so that $\prod_{i\in\mathbb{N}} r_i$ converges. For each stage s, let $\ell_s = \ell(r_s, 2)$ as in the Space Lemma. Then, for every stage s, there are at least two strings τ of length ℓ_s where $m(\sigma\tau) \leq r_s m(\sigma)$.

Let X be given. We now construct R that wtt-computes X. At stage s, if $X[s] = 0$, then R_{s-1} is extended by a string τ_s which is either the leftmost path above, or the rightmost path from the Space Lemma.

Also observe that R is random, since the capital of the martingale is infinitely often upper bounded by $\prod_i r_i < \infty$.

We now show how to compute X from R. Suppose, inductively, that we have computed the prefix $X \upharpoonright s$ from $R \upharpoonright \left(\sum_{i=1}^{s-1} \ell_{s-1}\right)$. We know that the next extension of R, namely, τ, is either the leftmost path from the Space Lemma, or the rightmost path from the Space Lemma. We simulate the martingale m on all extensions of $R \upharpoonright \left(\sum_{i=1}^{s-1} \ell_{s-1}\right)$ of length ℓ_s until either all paths to the left of τ have capital $\geq \delta m\left(R \upharpoonright \left(\sum_{i=1}^{s-1} \ell_{s-1}\right)\right)$ or all paths to the right of τ have capital $\geq \delta m\left(R \upharpoonright \left(\sum_{i=1}^{s-1} \ell_{s-1}\right)\right)$. By construction, exactly one of these must happen, and this can be detected since m is a c.e. martingale. In the first case, τ must be the leftmost path, hence $X[s+1] = 0$, otherwise $X[s+1] = 1$. □

6 Degrees containing randoms

As an easy consequence of the *proof* of the Kučera-Gács theorem, we have the following result about what kind of degrees contain a Martin-Löf random.

Theorem 6.1. *If* $0' \leq \mathbf{a}$*, then* $\mathbf{a}$ *contains a Martin-Löf random.*

Proof. Let $\mathbf{a} \geq 0'$ and let $X \in \mathbf{a}$. It suffices to show that there is a Martin-Löf random which is Turing-equivalent to X.

Let R be the random constructed as in the proof of the Kučera-Gács theorem, which computes X. Then $X \leq R$.

We now show that $R \leq X \oplus \emptyset'$. Observe that to compute the bits of R, it suffices to know the bits of X together with the knowledge of which sets are s-admissible for each s. This can be computed from X and $\emptyset'$. Thus, $R \leq X \oplus \emptyset'$. Since $X \geq \emptyset'$, it follows that $R \leq X$.

Hence, we conclude that $X \equiv R$, thus $R \in \mathbf{a}$. □

7 A counterexample by Ville

A selection rule is a partial function $f : 2^{\omega} \dashrightarrow \{\text{yes}, \text{no}\}$ which is the basis for the selection of an output subsequence from a given sequence. After observing a k-length prefix, for example, f may say whether to select the k^{th}bit into the output sequence or not. Define the partial function $s_f : 2^{\omega} \times \mathbb{N} \dashrightarrow \mathbb{N}$ by $s_f(\alpha, n) = k$ if k is the n^{th} prefix length k such that $f(\alpha \upharpoonright k) = \text{yes}$, if such a k exists, and is undefined otherwise. If $s_f(\alpha, n) = k$, then define $S_f(\alpha, n) = \sum_{i=0}^{n-1} \alpha[s_f(\alpha, i)]$, the number of 1s in the first n bits of the output sequence.

For the particular selection function f which always says yes at every prefix of every string, we denote $S_f(\alpha, n)$ by $S(\alpha, n)$.

The following theorem by Ville shows that for every selection process, there is some sequence such that the selected subsequence may not have some desirable randomness properties. The theorem is interesting: it does not, as we may expect, select a subsequence whose frequency of 1s differs from that of the input sequence. Rather, it says that the output sequence converges to the limit only from one side. This lopsided convergence is a behavior we can exploit to bet and win on it using a martingle.

Theorem 7.1. *(Ville) Let E be any countable collection of selection functions. Then there is a sequence $\alpha \in 2^{\omega}$ such that the following hold.*

1. [Frequency stability of the whole sequence] $\lim_n \frac{S(\alpha,n)}{n} = \frac{1}{2}$.
2. [Frequency stability of every selected subsequence] For every $f \in E$ which selects infinitely many bits of α, $\lim_n \frac{S_f(\alpha,n)}{n} = \frac{1}{2}$.
3. [Monotone convergence from below for the whole sequence] For every n, $\frac{S(\alpha,n)}{n} \leq \frac{1}{2}$.

In the following discussion, we prove a weaker version of Ville's theorem, where the collection of selection functions is finite.

Proof. Without loss of generality, we assume that the function which selects every index is an element of E. This implies, first, that E is not empty, and further, condition 2 subsumes 1.

Consider $\alpha \upharpoonright n$. Let $C(n) = \{f \in E \mid f(\alpha \upharpoonright n) = \text{yes}\}$ be the set of functions which select the index n. Set $\alpha[n] = 0$ if the set $C(n)$ has appeared an even number of times in $C(0), C(1), \ldots, C(n)$, and set $\alpha[n] = 0$ otherwise. This ensures condition 3, since each 1 appearing in α can be uniquely matched with a preceding 0 in a previous position.

Now, suppose $n_0 < n_1 < \ldots$ is a strictly increasing sequence of positions selected by $f \in E$. For any $C \subseteq E$, let $n_{i_0} < n_{i_1} < \ldots$ be the possibly finite sequence of positions at which C appears as the set of functions selecting the position. We have $\alpha\left[n_{i_j}\right]$ is when j is even, and 1 when j is odd. Thus, the number of 1s among the first n bits of α selected by f differ by at most 1 for every subset of E. Thus

$$\left|\frac{n}{2} - S_f(\alpha, n)\right| \leq 2^{|E|},$$

and it follows that $\lim_n \frac{S_f(\alpha,n)}{n} = \frac{1}{2}$. □

8 Schnorr randomness

C. P. Schnorr in 1971 criticized that Martin-Löf tests are not sufficiently computable, and that the tests ought to be *computable* in a strict sense. This leads to a *weaker* notion of randomness, now called SCHNORR RANDOMNESS. Contrast this with Remark **??** where we said that the Kučera-Gács theorem indicates that we need a stronger notion of randomness. Thus both stronger and weaker notions of randomness than MLrandomness are justified, and are studied in the literature. Here, we cover the basics of Schnorr randomness.

Definition 8.1. A SCHNORR TEST is a ML test $\langle G_m \rangle_{m\in\mathbb{N}}$ such that $\mu(G_m)$ is computable, uniformly in m. $Z \in 2^\omega$ FAILS the test if $Z \in \cap_{m\in\mathbb{N}} G_m$, otherwise Z PASSES the test. A real $Z \in 2^\omega$ is SCHNORR RANDOM if it passes every Schnorr test.

The difference between a Schnorr test and a ML test is that the probability of G_m must be exactly known and be computable, whereas in an ML test, an upper bound suffices. (Since G_m is c.e. open, $\mu(G_m)$ is lower semicomputable.)

Since we are not in the setting of lower semicomputability, we do not expect there to be a universal Schnorr test. This is indeed the case.

Theorem 8.2. *There is no universal Schnorr test.*

It suffices to show that there is no single Schnorr test which covers all Schnorr non-randoms. In other words, for every Schnorr test, there is a Schnorr non-random which passes the test. Surprisingly, computable sets suffice for the argument.

Proof. Let Z be a computable set. Then $\langle [Z \upharpoonright m] \rangle_{m\in\mathbb{N}}$ is a sequence of clopen sets such that for every m, $\mu([Z \upharpoonright m]) = 2^m$, hence uniformly computable. Thus Z is not Schnorr random.

However, every Schnorr test is passed by a computable set. Let $\langle G_m \rangle_{m\in\mathbb{N}}$ be a Schnorr test. Let us focus on the complement of the first open set, G_1. We note that $2^\omega - G_1$ is a Π^0_1class having positive, computable measure. By Exercise ..., it follows that it has a computable path $Z \in 2^\omega$. But $Z \notin \cap_{m\in\mathbb{N}} G_m$, so Z passes the Schnorr test. □