Lecture Notes on Algorithmic Randomness

Jan Reimann*

Department of Mathematics
University of California at Berkeley

Notation

$X, Y, Z, \ldots$	Infinite binary sequences
2^ω	Cantor space, set of all infinite binary sequences
$\sigma, \tau, \ldots, x, y, z, \ldots$	Finite binary strings
$X \upharpoonright_n$	Length n initial segment of X, $X(0) \ldots X(n-1)$.
$2^{<\omega}$	Set of all finite binary strings
$[\sigma]$	Open cylinder defined by σ
$[U]$	Open set defined by $U \subseteq 2^{<\omega}$.
λ	Lebesgue measure

*reimann@math.berkeley.edu

Lecture 1 Measure Theory on Cantor Space

1.1 Cantor space

We will study randomness for *infinite binary sequences*. The set of all such sequences, denoted by 2^ω, is called the *Cantor space*. Think of elements of 2^ω also as functions from $\mathbb{N}$ to $\{0,1\}$. This way you can interpret them as characteristic functions of subsets of the natural numbers, i.e. $x \in 2^\omega$ represents the set $S_x = \{n \in \mathbb{N} : x(n) = 1\}$.

Cantor space comes with a standard metric that is in many respects different from the usual metrics one encounters. Given $x, y \in 2^\omega$, $x \neq y$, let $x \cap y$ be the longest common initial segment of x and y (possibly the empty string $\varnothing$). For $x, y \in 2^\omega$, let

$$d(x,y) = \begin{cases} 2^{-N(x,y)} & \text{if } x \neq y, \text{ where } N(x,y) = \min\{n : x(n) \neq y(n), \\ 0 & \text{if } x = y. \end{cases}$$

► **Exercise.** Show that this actually defines a metric.

Given a set $A \subseteq 2^\omega$, we define its *diameter* $d(A)$ as

$$d(A) = \sup\{d(x,y) : x, y \in A\}.$$

The metric d is compatible with the *product topology* on $\{0,1\}^\mathbb{N}$, if $\{0,1\}$ is endowed with the discrete topology.

2^ω is a compact Polish space. A countable basis is given by the *cylinder sets*

$$[\sigma] = \{X : X \restriction_n = \sigma\},$$

where σ is a finite binary sequence. $2^{<\omega}$ denotes the set of all finite binary sequences. If $\sigma, \tau \in 2^{<\omega}$, we use $\subseteq$ to denote the usual prefix partial ordering. This extends in a natural way to $2^{<\omega} \cup 2^\omega$. Thus, $X \in [\sigma]$ if and only if $\sigma \subset X$. Finally, given $U \subseteq 2^{<\omega}$, we write $[U]$ to denote the open set induced by U, i.e. $[U] = \bigcup_{\sigma \in U} [\sigma]$.

1.2 Lebesgue measure on Cantor space

Over the real numbers, *Lebesgue measure* λ is characterized as the unique Borel measure that is translation invariant and assigns every interval (a, b) measure $|b - a|$, i.e. the measure of an interval is its length.

What should be the analogue to Lebesgue measure on 2^ω? The length of an interval in $\mathbb{R}$ is also its *diameter*. Lebesgue measure is also required to be a *Borel measure*, i.e. every Borel sets is assigned a measure. The Borel sets in $\mathbb{R}$ are the sets one obtains by closing the open sets under taking complements and countable unions. Open sets in $\mathbb{R}$ are countable unions of open intervals. For this reason, open intervals are also called *basic open sets*.

As we saw above, in Cantor space the basic open sets are given by the *cylinders*. The diameter of a cylinder is easily calculated: It is $2^{-|\sigma|}$, where $|\sigma|$ denotes the length of σ. Hence we obtain an analogue to Lebesgue measure in 2^ω if we require

$$\lambda[\sigma] = 2^{-|\sigma|}.$$

Some basic results of measure theory ensure that such a Borel measure λ on 2^ω actually exists. We will discuss this in some greater in a later lecture. We refer the interested reader to standard literature on measure theory (such as [Halmos, 1950]).

When denoting the measure of a set, we will often write λA instead of $\lambda(A)$.

If the above argument does not convince you that the measure we defined on 2^ω has anything to do with Lebesgue measure, consider the following argument.

Every infinite binary sequence can be identified with a real number via the dyadic representation of reals: Given $X \in 2^\omega$,

$$r(x) = \sum_{n=0}^{\infty} \frac{X(n)}{2^{n+1}}$$

is a real number in $[0, 1]$. Hence r yields a surjection of 2^ω onto $[0, 1]$. (It is not injective because, for instance, $1000000\ldots$ and $01111111\ldots$ map to the same real.) Let us compute the image of a cylinder $[\sigma]$ under this mapping. Assume σ is a string of length n. Then the 'leftmost' sequence in $[\sigma]$ is $\sigma^\frown 0^\infty$, σ continued by all zeros. The 'rightmost' sequence, on the other hand in $[\sigma]$ is $\sigma^\frown 1^\infty$. Now it is not hard to see that the image of $[\sigma]$ is precisely the *dyadic interval*

$$\left[\sum_{k=0}^{n-1} \sigma(k)/2^{k+1}, 2^n + \sum_{k=0}^{n-1} \sigma(k)/2^{k+1} \right].$$

The Lebesgue measure of this interval is 2^{-n}. Topologically, $[0,1]$ and 2^ω may be very different. But from a purely measure theoretic point of view, they are essentially the same.

I want to give you one more perspective on Lebesgue measure on Cantor space. 2^ω can be seen as a simple infinite product space: $\{0,1\}^{\mathbb{N}}$. This way of looking at 2^ω is probably closest to our intended application – describing outcomes of an infinite sequence of coin tosses. Each factor $\{0,1\}$ represents the possible results of one coin toss, 0 or 1. If the coin is fair, each outcome should have probability $1/2$. Now your basic knowledge in probability theory tells you that the probability of a specific outcome σ is $2^{-|\sigma|}$, which is precisely the Lebesgue measure of $[\sigma]$.

Later we will study measures other than Lebesgue measure. Then all three perspectives given here will be useful.

1.3 Nullsets

Nullsets are sets that are measure theoretically small, just as countable sets are small with respect to cardinality, or meager sets are topologically small. Intuitively, a nullset is a set that can be covered by open sets of arbitrary small measure.

Definition 1.1: A subset $A \subseteq 2^\omega$ is a **nullset** for Lebesgue measure (or has Lebesgue measure zero) if for every $\varepsilon > 0$ there exists an open set $U = \bigcup_{\sigma\in W}[\sigma]$ such that

$$A \subseteq U \quad \text{and} \quad \sum_{\sigma\in W} \lambda[\sigma] = \sum_{\sigma\in W} 2^{-|\sigma|} < \varepsilon.$$

In order to formulate Martin-Löf tests, it is convenient to recast this definition a little.

Proposition 1.2: *A set $A \subseteq 2^\omega$ is a nullset if and only if there exists a set $W \subseteq \mathbb{N}\times 2^{<\omega}$ such that, if we let $W_n = \{\sigma : (n,\sigma) \in W\}$, for all $n \in \mathbb{N}$,*

$$A \subseteq \bigcup_{\sigma\in W_n} [\sigma] \quad \textit{and} \quad \sum_{\sigma\in W_n} 2^{-|\sigma|} < 2^{-n}.$$

If you do not see the equivalence immediately, take a few minutes to verify it formally. Each $\bigcup_{\sigma\in W_n}[\sigma]$ defines an open subset of Cantor space. The

proposition says that A is contained in the intersection of a sequence of open sets whose measure goes to zero. Of course, given a set W such that the sequence (W_n) satisfies the right hand side of the last equation, then $\bigcap_n [W_n]$ is itself a nullset. Topologically, sets that are countable intersections of open sets are called **G_δ sets** or **Π^0_2 sets**.

Therefore, we have

Every nullset is contained in a G_δ nullset.

Later on it will be nice to have the property that the sequence $U_n = [W_n]$ of open sets is actually *nested*, i.e. $U_n \supseteq U_{n+1}$.

► **Exercise.** Show that if $E \subseteq 2^\omega$ is a nullset, then there exists a nested sequence (U_n) of open sets such that $\lambda U_n < 2^{-n}$ and $E \subseteq \bigcap_n U_n$.

The important thing about the reformulation is that G_δ sets can be easily effectivized. In fact, if you look at Proposition 1.2, you see that what 'codes' a G_δ set in Cantor space is a subset of $\mathbb{N} \times 2^{<\omega}$. But on such sets we can easily impose effectivity conditions, e.g. require that they are *recursively enumerable*. This is precisely what we will do to define Martin-Löf tests.

1.4 Martin-Löf tests

Definition 1.3: (1) A **Martin-Löf (ML) test** (for Lebesgue measure) is a recursively enumerable set $W \subseteq \mathbb{N} \times 2^{<\omega}$ such that, if we let $W_n = \{\sigma : (n, \sigma) \in W\}$, for all $n \in \mathbb{N}$,

$$\sum_{\sigma \in W_n} 2^{-|\sigma|} < 2^{-n}.$$

(2) A set $A \subseteq 2^\omega$ is **Martin-Löf null** if it is covered by a Martin-Löf test, i.e. if there exists a Martin-Löf test W such that $A \subseteq \bigcap_n [W_n]$.

(3) A sequence $X \in 2^\omega$ is **Martin-Löf random** if $\{x\}$ is not Martin-Löf null.

Before we go on to study Martin-Löf random sequences we ought to make sure that it is a meaningful concept, in particular, that Martin-Löf random sequences exist.

As we saw in the previous section, every Martin-Löf test W describes a G_δ nullset, with the additional requirement that it is effectively presented (W is r.e.). There are only countably many r.e. sets, and hence only countably many Martin-Löf

tests. Being random means not being contained in the union of all G_δ sets defined by any Martin-Löf test. Formally, if $\{W^{(k)} : W^{(k)} \subseteq \mathbb{N} \times 2^{<\omega}, k \in \mathbb{N}\}$ is the set of all Martin-Löf tests, then x is not random if and only if

$$x \in \bigcup_k \bigcap_n [W_n^{(k)}].$$

But a basic result of measure theory says that a countable union of nullsets is again a nullset (again, consult your favorite analysis book - it is the standard "$\varepsilon/2^n$-proof"). Therefore, the set of all non-random sequences is a nullset, and consequently, λ-almost every sequence *is* Martin-Löf random.

Universal Martin-Löf tests

We we argued that ML-random sequences exist, we used that a *countable union of nullsets is a nullset*. It turns out that even more is true: The union of all ML-tests is again a ML-test, a *universal test*.

Proposition 1.4: *There exists a ML-test (U_n) such that X is ML-random if and only if X is not covered by (U_n).*

In other words, the ML-random sequences are precisely the ones in the complement of $\bigcap_n [U_n]$. The ML-random sequences form the *largest* effective (in the sense of Martin-Löf) set of measure 1.

Sketch. Start uniformly enumerating all r.e. subsets $W^{(e)}$ of $\mathbb{N} \times 2^{<\omega}$. Once we see that the measure condition of some $W_n^{(e)}$ is violated, we stop enumerating it.

This yields a uniform enumeration of all tests $(\tilde{W}_n^{(e)})$ (with possible repetitions). Now define a universal test (U_n) by letting

$$U_n = \bigcup_e \tilde{W}_{n+i+1}^{(e)}$$

□

This construction is essentially due to Kucera. Later we will encounter other ways to define universal tests.

Basic Properties of Random Sequences

We list here as an exercise some basic properties of ML-random sequences. The following assertions can be proved directly by defining a suitable test. But we will prove different characterizations of random sequences which may make this easier. So if you cannot figure them out right away, you may read on a bit and try again.

► **Exercise.** (1) Show that the set of Martin-Löf random reals is invariant under the following operations:

- adding a finite prefix,
- deleting a finite prefix,
- replacing a finite prefix by an arbitrary string of the same length.

(2) Show that if $Z \subseteq \omega$ is computable, then the real given by the characteristic function of Z is not Martin-Löf random.

(3) Show that if $Z \subseteq \omega$ is computably enumerable, then the real given by the characteristic function of Z is not Martin-Löf random.

(4) Show that any finite string appears somewhere in a Martin-Löf random real.

(5) Show that any finite string appears *infinitely often* in a Martin-Löf random real.

(6) Show that for every Martin-Löf random sequence $X \in 2^\omega$,

$$\lim_n \frac{\sum_{k=0}^{n-1} X(i)}{n} = \frac{1}{2}.$$

Hint: Chebyshev's inequality or *Chernoff* bound.

1.5 Other test notions

There is a certain arbitrariness in the way Martin-Löf tests effectivize nullsets. One can give effective representations of G_δ nullsets other than the one of Proposition 1.2. We will address two alternatives here and mention others later on in the course.

Note that a Martin-Löf test has to fulfill two effectivity requirements. One is the recursive enumerability of W (yielding the uniformly enumerable sequence

(W_n) of effective open sets, the other is that the measure of the W_n converges to 0 *effectively*, as reflected by the condition that $\lambda[W_n] \leq 2^{-n}$. We could ease the latter by simply requiring in Definition 1.3 that $\lambda \bigcap_n [W_n] = 0$. The resulting randomness concept is called (for reasons you can read about in Nies [20xx] or Downey and Hirschfeldt) **weak 2-randomness**.

On the other, one may consider the effectiveness of the convergence given by $\lambda[W_n] \leq 2^{-n}$ as *still too weak*. How about requiring that we actually have $\lambda[W_n] = 2^{-n}$? You should check that this is not too restrictive.

► **Exercise.** (1) Show that for every nullset A there exists a G_δ set $U = \bigcap_n U_n$, each U_n open, such that $\lambda U_n = 2^{-n}$.

(2) Show that W is a Martin-Löf test such that for each n, λW_n is a computable real number (uniformly in n) [1]), then there exists a Martin-Löf test V such that for each n, $\lambda V_n = 2^{-n}$.

Martin-Löf tests with this property are called **Schnorr tests**.

Obviously, we have the following implications

weak 2-random ⇒ Martin-Löf random ⇒ Schnorr random

One can show that the implications are proper.

There is an alternative approach to randomness tests using integrals. Before we discuss it we need to review some basic results of measure theory.

1.6 Finite Borel measures in Cantor space

A measure is a monotone, additive set function on a σ-algebra. There are several ways how to obtain Borel measures on 2^ω. We will discuss later an approach using *outer measures*. When we defined Lebesgue measure, we set its values only on the cylinder sets. It turns out this is sufficient for other measures, too, if the measures obey a simple algebraic rule: For all σ,

$$\mu[\sigma] = \mu[\sigma^\frown 0] + \mu[\sigma^\frown 1].$$

Furthermore, we require that $0 < \mu[\varnothing] < \infty$. Think of a measure as a *flow* through the full binary tree. We start at the "sink" $\varnothing$ with a mass of $\mu[\sigma]$

[1] Recall that a real number x is *computable* if there exists a recursive function $g : \mathbb{N} \to \mathbb{Q}$ such that for all n, $|g(n) - x| < 2^{-n}$, i.e. you can approximate x effectively by rationals.

and start distributing it along the tree. The condition simply says that at each splitting, the total mass is preserved. This simple requirement is actually sufficient to guarantee the existence of a unique extension of μ to all Borel sets.

We will discuss measures later in somewhat greater detail, for the moment this suffices.

1.7 Martingales

A random outcome of fair coin toss should be *unpredictable*. Of course we could imagine some supreme being (or just someone endowed with incredible computational power) able to predict any process in the physical world. Let us try to make precise what we should understand by "unpredictability". We resort to the world of gambling.

Definition 1.5: A **betting strategy** b is a function $b : 2^{<\omega} \to [0,1] \times \{0,1\}$.

The should be interpreted as follows. A string σ represents the outcomes of a 0-1-valued (infinite) process (e.g. a coin toss). $b(\sigma) = (i, \alpha)$ then tells the gambler on which outcome to bet next, i, and what percentage of his current capital to bet on this outcome, α.

When the next bit of the process is revealed and agrees with i, the gambler receives 2α as his win, if it is different from i, the gambler loses his bet, i.e. his capital is multiplied by $(1-\alpha)$. This is just how bets like pair/impair or rouge/noir for roulette work (if we disregard the possibility of 0 or 00 for now).

Given a betting function $b(\sigma) = (i_\sigma, \alpha_\sigma)$, we can easily calculate the capital F the player holds after some finite sequence of outcomes σ. We fix his initial capital, say $F(\varnothing) = 1$. Let $F : 2^{<\omega} \to [0,1]$ the be inductively defined as

$$F(\sigma^\frown i_\sigma) = F(\sigma)(1+\alpha_\sigma), \qquad F(\sigma^\frown(1-i_\sigma)) = F(\sigma)(1-\alpha_\sigma). \tag{1.1}$$

The function F satisfies the following equality.

$$\text{For all } \sigma,\ F(\sigma) = \frac{F(\sigma^\frown 0) + F(\sigma^\frown 1)}{2} \tag{1.2}$$

This reflects the property that the game is *fair* – the expected value of the capital after the next round is the same as the player's capital before he makes his bet.

Any function $F : 2^{<\omega} \to [0,\infty)$ satisfying (1.2) is called a **martingale**. Given a martingale, we can reconstruct the accordant betting function from it.

► **Exercise.** Given a martingale F, show that there is a unique betting function $b(\sigma) = (i_\sigma, \alpha_\sigma)$ such that, if we define $G(\varnothing) = F(\varnothing)$ and inductively $G(\sigma)$ as in (1.1), we have $G = F$.

Now, what does it mean for a player to have a successful betting strategy? Surely it should be formulated in terms of capital gain, so we could say that a betting strategy is **successful** on an infinite sequence X if

$$\lim_{n\to\infty} F(X\restriction_n) = \infty,$$

i.e. if X is the outcome of infinitely many rounds of the game, the player will become infinitely rich. For technical reasons we will replace the lim by a lim sup, i.e. a successful player will be infinitely rich, but there can be times where he may be very poor.

Passing from lim to lim sup does not really make it easier for a martingale to win. If you manage your capital cleverly, you can pass from lim sup to lim again.

► **Exercise.** For every martingale F there exists a martingale G such that for all X,

$$\limsup_n F(X\restriction_n) = \infty \quad \text{implies} \quad \lim_n G(X\restriction_n) = \infty.$$

(*Hint:* Set some money aside regularly.)

Let us sum up in the following definition

Definition 1.6: A **martingale** is a function $F : 2^{<\omega} \to [0,\infty)$ such that for all strings σ,

$$F(\sigma) = \frac{F(\sigma^\frown 0) + F(\sigma^\frown 1)}{2}$$

We say F **succeeds** on a sequence $X \in 2^\omega$ if

$$\limsup_n F(X\restriction_n) = \infty.$$

On how many sequences can a martingale be successful? Well, apparently not too many, otherwise we would probably spend the rest of our lives in casinos.

It is easy to see that no martingale can succeed on *all* sequences: For any σ, on one extension, $\sigma^\frown 0$ or $\sigma^\frown 1$, F will not increase its capital. Otherwise the fairness condition (1.2) would be violated. By following these extension inductively we can construct an infinite sequence along which F never increases.

However, much more is true. This is reflected by the following theorem, a special case of the fundamental *martingale convergence theorem*.

Theorem 1.7 (Doob)**:** *For any martingale F, the set of sequences $X \in 2^\omega$ such that*

$$\limsup_{n\to\infty} F(X\upharpoonright_n) = \infty \tag{1.3}$$

has λ-measure zero.

This means that sequences on which a martingale succeeds are actually extremely rare. Later, we will prove an effective version of this theorem.

Does a converse of the theorem hold, i.e. given a nullset $E \subset 2^\omega$, can we find a martingale F such that F succeeds on every sequence $X \in E$? We will later see that is true, too.

Hence martingales give us a different way to describe nullsets. By imposing effectivity conditions on a martingale, we obtain randomness concepts.

1.8 Martingale randomness

What should the right effectivity requirement for martingales? Can we find one such that the randomness concept coincides with Martin-Löf randomness?

For the first question, as in the case of tests, a definite answer arguably does not exist. We will encounter several possible answers here.

We will deal first with *semi-computable* martingales, which correspond to ML-tests.

1.8.1 From ML-tests to martingales

How can we interpret a test as a betting function? Here is the basic idea: Given a ML-test (U_n), try to construct a martingale F such that whenever a string appears at level n of the test, F reaches a value of at least n. If a sequence X is covered at every level of the test, i.e. is not Martin-Löf random, F will succeed on X. Let us try to make this precise.

We start with a single string σ. Associate the following martingale with σ.

$$F_\sigma(\tau) = \begin{cases} 2^{-(|\sigma|-|\tau|)} & \text{if } \tau \subseteq \sigma, \\ 1 & \text{if } \tau \supseteq \sigma, \\ 0 & \text{otherwise.} \end{cases}$$

► **Exercise.** Verify that F_σ is in fact a martingale.

F_σ starts out with a capital of $2^{-|\sigma|}$ and doubles its capital every step along σ. If an outcome is not compatible with σ, its capital is lost. Once it reaches σ, it stops betting and henceforth remains at a capital of 1.

A ML-test, of course, may have more than one string per level. We need to blend the individual "string"-martingales into one. Here is a great thing about martingales: The sum of two martingales is again a martinagle. Inductively, any finite sum of martingales is a martingale. Even more is true:

► **Exercise.** If (F_n) is a sequence of martingales and $\sum_n F(\varnothing) < \infty$, then

$$F = \sum_n F_n$$

is a martingale.

Hence we can define

$$F_n(\tau) = \sum_{\sigma \in U_n} F_\sigma(\tau).$$

The only thing left to check is that the sum of the $F_\sigma(\varnothing)$ is finite. Since (U_n) is a ML-test,

$$\sum_{\sigma \in U_n} 2^{-|\sigma|} \leq 2^{-n}.$$

But $F_\sigma(\varnothing) = 2^{-|\sigma|}$, and hence

$$F_n(\varnothing) = \sum_{\sigma \in U_n} F_\sigma(\varnothing) \leq 2^{-n}.$$

The last inequality lets us combine the martingales for each U_n into one martingale F,

$$F(\sigma) = \sum_n F_n(\sigma).$$

Now we show that if $X \in \bigcap_n [U_n]$ then F succeeds on X.

First note that we always suppose that $[U_n] \supseteq [U_{n+1}]$. Hence if $X \in \bigcap_n [U_n]$, there exists a sequence (σ_n) such that for all n, $\sigma_n \in U_n$ and $\sigma_n \subset X$. It follows that $F_n(\sigma_n) \geq 1$. More important, by the definition of F_n, $F_n(\tau) \geq 1$ for all $\tau \supseteq \sigma$, hence in particular for all σ_m where $m \geq n$.

It follows that for all n,

$$F(\sigma_n) \geq \sum_{k=1}^{n} F_k(\sigma_n) \geq n.$$

Thus F is unbounded along X.

How complicated is it to compute F? For each string σ, the martingale F_σ is obviously a computable function from $2^{<\omega}$ to $[0, \infty)$. A real valued function F on strings is called **computable** if we can approximate it to an arbitrary degree of precision – this means there exists a function $g : 2^{<\omega} \times \mathbb{N} \to \mathbb{Q}$ such that for all σ and all n,

$$|F(\sigma) - g(\sigma, n)| \leq 2^{-n}.$$

F_σ is even more simple, since it takes only rational values and is constant above every string of length $|\sigma|$.

We cannot, however, expect F_n to be computable, since U_n is only required to be recursively enumerable. Furthermore, the U_n are generally infinite, which means that for F_n we have to evaluate an infinite sum.

Therefore, F_n is only **enumerable from below** or **left-enumerable**. This means that there exists, uniformly in σ, a recursive nondecreasing sequence $(q_k^{(\sigma)})$ of rational numbers such that $q_k^{(\sigma)} \to F(\sigma)$. (Note that in this case it is not required to have a computable bound on the convergence.) Equivalently, the **left cut** of $F(\sigma)$ is uniformly enumerable, i.e. the set

$$\{(q, \sigma) : q < F(\sigma)\}$$

is recursively enumerable.

To see that each F_n is left-enumerable, take each finite sum of martingales F_σ that corresponds to an enumeration of U_n up to any finite stage.

Furthermore, it is not hard to see that F is left-enumerable, too.

Summing up, we have the following result.

Proposition 1.8: *For any ML-test (U_n) there exists a left-enumerable martingale F such that if $X \in \bigcap_n [U_n]$, then F succeeds on X. In other words, if X is not ML-random, we can find a left-enumerable martingale that succeeds on X.*

1.8.2 From martingales to ML-tests

Does a converse of the preceding proposition hold? That is, given a left-enumerable martingale F, can we find a ML-test that covers every X on which F succeeds?

The idea is as follows: Whenever F first reaches a capital of 2^n on some string σ, enumerate σ into U_n. Since F is enumerable from below, this is an r.e. event. We only have to make sure that there are not too many such σ. This is guaranteed by the following inequality, commonly referred to as *Kolmogorov's inequality*.

Proposition 1.9 (Ville, 1939)**:** *Suppose F is a martingale. For any string σ and any prefix-free set W of strings extending σ,*

$$F(\sigma) \geq \sum_{\tau \in W} 2^{|\sigma|-|\tau|} F(\tau)$$

Note that if $W = \{\sigma^\frown 0, \sigma^\frown 1\}$, then the result follows immediately from the martingale equality (1.2).

► **Exercise.** Prove Kolmogorov's inequality. Use induction on the size of W to prove the result for finite W. Then argue that it is sufficient to consider only finite W.

From this we get the desired result.

Corollary 1.10: *Given a martingale F, let $C_k(F) = \{\sigma : F(\sigma) \geq k\}$. Then $\lambda[C_k(F)] \leq F(\varnothing)/k$.*

Proof. Let W be a prefix-free subset of $C_k(F)$ such that $[W] = [C_k(F)]$. Then

$$\lambda[C_k(F)] = \lambda[W] = \sum_{\tau \in W} 2^{-|\tau|}.$$

By Kolmogorov's inequality,

$$F(\varnothing) \geq \sum_{\tau \in W} 2^{-|\tau|} F(\tau) \geq \sum_{\tau \in W} 2^{-|\tau|} k,$$

that is,

$$\lambda[C_k(F)] \leq F(\varnothing)/k,$$

as required. □

There is a subtlety regarding the effectiveness of this argument. We said we would enumerate into U_n all minimal strings (respect to the prefix ordering) with $F(\sigma) \geq 2^n$, but we cannot be sure that these minimal strings actually occur first, i.e. it might be that some extension $\tau \supset \sigma$ is enumerated with $F(\tau) \geq 2^n$ before σ is. Enumerating σ in addition to τ could increase the weight of the cover U_n too much. We can remedy this as follows: By the time σ is enumerated with $F(\sigma) \geq 2^n$, we enumerate all "missing" extensions of σ into U_n, so that we have in U_n a complete cover of $[\sigma]$. For this argument to work it is important that λ is a *finite measure* on 2^ω, which implies that we can replace string with any cover-equivalent prefix-free set without changing the weight.

We have proved

Proposition 1.11: *For any left-enumerable martingale F there exists a ML-test that covers every X on which F succeeds.*

Propositions 1.8 and 1.11 combine to yield the **first main theorem** of algorithmic randomness, due to Schnorr and independently Levin.

Theorem 1.12 (Schnorr, 1971, Levin, 1973)**:** *A sequence X is ML-random if and only if no left-enumerable martingale succeeds on it.*

References

K. Ambos-Spies and A. Kučera. Randomness in computability theory. In *Computability theory and its applications (Boulder, CO, 1999)*, volume 257 of *Contemp. Math.*, pages 1–14. Amer. Math. Soc., Providence, RI, 2000.

C. H. Bennett. Logical depth and physical complexity. In *The universal Turing machine: a half-century survey*, Oxford Sci. Publ., pages 227–257. Oxford Univ. Press, New York, 1988.

L. Bienvenu. Constructive equivalence relations on computable probability measures. In *Computer Science – Theory and Applications*, volume First International Computer Science Symposium in Russia, CSR 2006, St. Petersburg, Russia of *Lecture Notes in Comput. Sci.*, pages 92–103. Springer, 2006.

L. Bienvenu and W. Merkle. Effective randomness for computable probability measures. In *Third International Conference on Computability and Complexity in Analysis (CCA 2006)*, ta.

P. Billingsley. *Probability and measure*. Wiley Series in Probability and Mathematical Statistics. John Wiley & Sons Inc., New York, 1995.

O. Demuth. Remarks on the structure of tt-degrees based on constructive measure theory. *Comment. Math. Univ. Carolin.*, 29(2):233–247, 1988.

R. G. Downey and D. R. Hirschfeldt. Algorithmic randomness and complexity. Book, in preparation.

K. Falconer. *Fractal Geometry: Mathematical Foundations and Applications*. Wiley, 1990.

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

P. R. Halmos. *Measure Theory*. Van Nostrand, 1950.

C. G. Jockusch, Jr. and R. I. Soare. Π^0_1 classes and degrees of theories. *Trans. Amer. Math. Soc.*, 173:33–56, 1972. ISSN 0002-9947.

D. W. Juedes, J. I. Lathrop, and J. H. Lutz. Computational depth and reducibility. *Theoret. Comput. Sci.*, 132(1-2):37–70, 1994.

S. Kakutani. On equivalence of infinite product measures. *Ann. of Math.*, 49: 214–224, 1948. ISSN 0003-486X.

S. M. Kautz. *Degrees of Random sequences*. PhD thesis, Cornell University, 1991.

A. S. Kechris. *Classical Descriptive Set Theory*. Springer, 1995.

A. 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.

L. A. Levin. The concept of a random sequence. *Dokl. Akad. Nauk SSSR*, 212: 548–550, 1973.

A. A. Muchnik, A. L. Semenov, and V. A. Uspensky. Mathematical metaphysics of randomness. *Theoret. Comput. Sci.*, 207(2):263–317, 1998.

M. E. Munroe. *Introduction to measure and integration*. Addison-Wesley, Cambridge, MA, 1953.

A. Nies. Computability and randomness. Oxford University Press, to appear, 20xx.

P. G. Odifreddi. *Classical recursion theory. Vol. II*, volume 143 of *Studies in Logic and the Foundations of Mathematics*. North-Holland Publishing Co., Amsterdam, 1999. ISBN 0-444-50205-X.

C. A. Rogers. *Hausdorff Measures*. Cambridge University Press, 1970.

C.-P. Schnorr. *Zufälligkeit und Wahrscheinlichkeit. Eine algorithmische Begründung der Wahrscheinlichkeitstheorie*. Springer-Verlag, Berlin, 1971.

A. K. Shen. Relationships between different algorithmic definitions of randomness. *Dokl. Akad. Nauk SSSR*, 302(3):548–552, 1988. ISSN 0002-3264.

J. Ville. *Etude critique de la notion de collectif*. Gauthier-Villars, 1939.

V. G. Vovk. On a criterion for randomness. *Dokl. Akad. Nauk SSSR*, 294(6): 1298–1302, 1987. ISSN 0002-3264.

A. K. Zvonkin and L. A. Levin. The complexity of finite objects and the basing of the concepts of information and randomness on the theory of algorithms. *Uspehi Mat. Nauk*, 25(6(156)):85–127, 1970.