Uniform Distribution and Algorithmic Randomness

Jeremy Avigad

Department of Philosophy and
Department of Mathematical Sciences
Carnegie Mellon University

November 2014

Contents

- Uniform distribution and a theorem of Weyl
- Algorithmic randomness
- Upper bounds
- Lower bounds

Uniform distribution

Definition. A sequence $(x_n)_{n\in\mathbb{N}}$ of real numbers is *uniformly distributed modulo one* (*UD mod 1*) if for every interval $I \subseteq [0,1]$,

$$\lim_{n\to\infty} \frac{|\{i < n \mid \{x_i\} \in I\}|}{n} = \lambda(I).$$

Here $\{x\} = x - \lfloor x \rfloor$, and λ is Lebesgue measure.

Weyl's theorem

Theorem. Let (a_n) be any sequence of distinct integers. Then for almost every x, $(a_n x)$ is UD mod 1.

A real number x is *absolutely normal* if for every base b, each pattern of digits $b_1 b_2 \cdots b_n$ occurs with with frequency b^{-n} in the limit.

Corollary. Almost every number x is absolutely normal to every base.

Weyl's criterion

Notation (Vinogradev). $e(x) = e^{2\pi i x}$.

Lemma. Given (x_n), TFAE:

1. (x_n) is UD mod 1
2. For any continuous $f : [0,1] \to \mathbb{R}$,
$$\lim_{n\to\infty} \frac{1}{n} \sum_{j<n} f(\{x_j\}) = \int_0^1 f(x).$$
3. For any $h \neq 0$,
$$\lim_{n\to\infty} \frac{1}{n} \sum_{i<n} e(hx_j) = 0$$

Corollary (Weyl). If α is irrational, $(\alpha j)_{j\in\mathbb{N}}$ is UD mod 1.

Proof of Weyl's theorem.

Let $(a_j)_{j\in\mathbb{N}}$ be any sequence of distinct integers. Want to show $(a_j x)$ is UD mod 1, a.e. x.

WLOG restrict to $x \in [0,1)$. Let $S_n(x) = \frac{1}{n}\sum_{j<n} e(a_j x)$.

By Weyl's criterion, we want to show that $S_n(hx) \to 0$ a.e. x, for every $h \neq 0$. WLOG h $= 1$.

Fact. Given $n^2 \leq m < (n+1)^2$, $|S_m(x)| \leq |S_{n^2}(x)| + 2/\sqrt{m}$.

So it suffices to show $\lim_{n\to\infty} S_{n^2}(x) = 0$ a.e. x.

Proof of Weyl's theorem.

Remember, $S_n(x) = \frac{1}{n}\sum_{j<n} e(a_j x)$.

Calculate:

$$\begin{aligned}\int_0^1 |S_n(x)|^2 &= \int_0^1 S_n(x)\overline{S_n(x)} \\ &= \frac{1}{n^2}\sum_{j,k<n}\int_0^1 e((a_j - a_k)x) \\ &= 1/n.\end{aligned}$$

Or: notice that the functions $e(a_j x)$ are orthogonal in the L^2 norm.

So $\int_0^1 |S_{n^2}(x)|^2 = \frac{1}{n^2}$. Remember: we want $S_n(x) \to 0$ as $n \to \infty$, for a.e. x

Proof of Weyl's theorem.

From $\int_0^1 |S_{n^2}(x)|^2 = \frac{1}{n^2}$ and the monotone convergence theorem:

$$\int_0^1 \sum_{n=1}^{\infty} |S_{n^2}(x)|^2 = \sum_{n=1}^{\infty} \int_0^1 |S_{n^2}(x)|^2 = \sum_{n=1}^{\infty} 1/n^2 < \infty.$$

So $\sum_{n=1}^{\infty} |S_{n^2}(x)|^2 < \infty$ almost everywhere.

So $S_{n^2}(x) \to 0$ a.e.

Contents

- Uniform distribution and a theorem of Weyl
- Algorithmic randomness
- Upper bounds
- Lower bounds

Algorithmic randomness

Question: What does it mean for a sequence of 0's and 1's to be random?

Kolmogorov: put a probability measure μ on the set of sequences. "A random string has property P" means $\{x \mid P(x)\}$ has measure 1.

So no sequence is really "random."

Martin-Löf used computability to recapture original intuition: a string is random if it passes all computable tests.

Algorithmic randomness

Definition. A set $G \subseteq \mathbb{R}$ is *effectively open* if there are computable sequences $(a_i)_{i \in \mathbb{N}}, (b_i)_{i \in \mathbb{N}}$ of rationals such that $G = \bigcup_i (a_i, b_i)$.

Definition. A *Martin-Löf test* is a uniformly effective sequence (G_j) of open sets such that for each j, $\lambda(G_j) \leq 2^{-j}$.

A real number *fails* the test if $x \in \bigcap_j G_j$, *passes* otherwise.

A real number x is Martin-Löf random if it passes every Martin-Löf test.

So, roughly, x is Martin-Löf *non*random if it is an element of an effective null G_δ set.

Fact. There is a *universal Martin-Löf test*.

Algorithmic randomness

Definition. A *Schnorr test* is a Martin-Löf test (G_j) such that $\lambda(G_j)$ is uniformly computable.

Definition. A *Kurtz test* is an effectively closed set of measure 0.

More restrictions on the test means that it is easier to pass. So

$$\text{Martin-Löf random} \Rightarrow \text{Schnorr random} \Rightarrow \text{Kurtz random.}$$

Kurtz random is very weak. For example, every “weakly 1-generic” real x is Kurtz random, but the fraction of 1’s in the binary expansion doesn’t converge.

UD randomness

Definition. Say a real number x is *UD random* if $(a_n x)$ is UD mod 1 whenever (a_n) is a *computable* sequence of distinct integers.

By Weyl's theorem, almost every real number is UD random.

Every UD random number is absolutely normal to every base.

Even better: if x is UD random, then for any base b, block of digits $b_1 b_2 \ldots b_k$, and computable sequence (p_i) of distinct positions,

$$\lim_{n\to\infty} \frac{|\{i < n \mid b_1 b_2 \ldots b_k \text{ occurs at position } p_i\}|}{n} = b^{-k}.$$

UD randomness

Question: How random is UD random?

Specifically:

- What randomness hypotheses on x are sufficient to ensure that x is UD random?
- What does UD randomness imply?

Upper bounds

Theorem. Every Schnorr-random real is UD random. There are Kurtz random reals that are not UD random.

The second claim follows easily from the observation that there are Kurtz random reals that fail the strong law of large numbers.

Proving the first claim is straightforward: extract a Schnorr test from the proof of Weyl's theorem.

Upper bounds

Theorem. For each i, let $(a^i_j)_{j\in\mathbb{N}}$ be a sequence of distinct integers, such that a^i_j is computable from i and j. Then there is a Schnorr test C such that for every x not in C and every integer i, $(a^i_j x)_{j\in\mathbb{N}}$ is UD mod 1.

For each i, rational $\varepsilon > 0$, and n define

$$A_{i,\varepsilon,m} = \{x \mid \exists n \geq m \, |S^i_{n^2}(x)| > \varepsilon\}.$$

$\lambda(A_{i,\varepsilon,m})$ decreases to 0 as m approaches infinity. Enumerate pairs (i_j, ε_j), and for each k and j choose $m_{j,k}$ large enough so that $\lambda(A_{i_j,\varepsilon_j,m_{j,k}}) < 2^{-(j+k+1)}$.

For each k, let

$$G_k = \bigcup_j A_{i_j,\varepsilon_j,m_{j,k}}.$$

Then (G_k) is the desired Schnorr test.

A consequence

Corollary. Given $(a^i_j)_{j\in\mathbb{N}}$ as above, one can *compute* an x such that for every i, $(a^i_j x)_{j\in\mathbb{N}}$ is UD mod 1.

Lower bounds

Suppose x is UD random. Is x necessarily Schnorr random? Kurtz random?

If $x = 0.x_1x_2x_3\ldots$ in binary notation and x is "random," and $i \mapsto u_i$ is a computable injection, then

$$x_{u_1}x_{u_2}x_{u_3}\ldots$$

should also be "random". In particular, a block like 010 should occur with the expected frequency.

Lower bounds

Suppose x is UD random. Is x necessarily Schnorr random? Kurtz random?

If $x = 0.x_1 x_2 x_3 \ldots$ in binary notation and x is "random," and $i \mapsto u_i$ is a computable injection, then

$$x_{u_1} x_{u_2} x_{u_3} \ldots$$

should also be "random". In particular, a block like 010 should occur with the expected frequency.

But the UD "tests" — scale x and check membership in an interval — are "local". They involve only contiguous digits.

Lower bounds

Guess: there is a UD random real x with the following property: for every n, digit 2^{2n} is the same as digit 2^{2n+1}.

In other words, $x_1 = x_2$, $x_4 = x_8$, $x_{16} = x_{32}$, ...

Such a real is not even Kurtz random.

How can we construct such a thing?

Lower bounds

Guess: there is a UD random real x with the following property: for every n, digit 2^{2n} is the same as digit 2^{2n+1}.

In other words, $x_1 = x_2$, $x_4 = x_8$, $x_{16} = x_{32}$, …

Such a real is not even Kurtz random.

How can we construct such a thing?

Don't bother. Prove that almost every x with that property is UD random!

Lower bounds

Let

$$C = \{x \mid \text{for every } n,\ (x)_{2^{2n}} = (x)_{2^{2n+1}}\},$$

Let μ be the "uniform" probability measure on this set.

Theorem. Let (a_n) be any sequence of distinct integers. Then $(a_n x)$ is UD mod 1 for μ-a.e. x.

In other words, Weyl's theorem holds relative to C.

Lower bounds

The proof of Weyl's theorem relied on the fact that $\int_0^1 e(ux)\, d\lambda(x) = 0$ for $u \neq 0$.

Now we need to consider

$$\hat{\mu}(u) = \int_C e(ux)\, d\mu(x),$$

the *Fourier-Stieltjes coefficients* of the measure μ.

Lemma (Lyons). If the Fourier-Stieltjes coefficients of μ have the property that

$$\sum_{u=1}^{\infty} \frac{|\hat{\mu}(u)|}{u}$$

converges, then for any sequence (a_n) of distinct integers, $(a_n x)$ is UD mod 1 for μ-a.e. x.

Lower bounds

To prove our main claim, then, it suffices to show that C and μ above, we have $\hat{\mu}(u) = O(1/\sqrt{u})$.

For an intuition, draw a picture of $C' = \{x \mid x_4 = x_8\}$. C is "fractal" version.

C' looks fairly uniform, except some bits are "jittered" in blocks.

We want to show $\int_C e(ux)$ is small every u, i.e. we cannot "detect" the irregularity with sines and cosines of period $2\pi/u$.

The argument varies depends on whether u is close to 4 or 8, or in some other region.

Lower bounds

The calculation is fiddly, but follows this intuition.

If we divide the binary digits of x into blocks, C becomes a union, and $\int_C$ becomes a sum.

Reindexing, expressions $e(u \cdot \sum t_i)$ become products.

In each case, certain terms have to be small.

Conclusions

One can ask lots of other questions along these lines. For example:

> *Is there a UD random x such that every initial segment of the binary representation of x has at least as many 1's as 0's?*

> *Is there a real number x that is Church stochastic but not UD random?*

More generally:

Given two properties P_1 and P_2 that hold of "random" reals, how do they relate?