The probability distribution as a computational resource for randomness testing

BJØRN KJOS-HANSSEN

Abstract: When testing a set of data for randomness according to a probability distribution that depends on a parameter, access to this parameter can be considered as a computational resource. We call a randomness test *Hippocratic* if it is not permitted to access this resource. In these terms, we show that for Bernoulli measures μ_p, $0 \leqslant p \leqslant 1$ and the Martin-Löf randomness model, Hippocratic randomness of a set of data is the same as ordinary randomness. The main idea of the proof is to first show that from Hippocrates-random data one can Turing compute the parameter p. However, we show that there is no single Hippocratic randomness test such that passing the test implies computing p, and in particular there is no universal Hippocratic randomness test.

1   Introduction

The fundamental idea of statistics is that by repeated experiment we can learn the underlying distribution of the phenomenon under investigation. In this paper we partially quantify the amount of randomness required to carry out this idea. We first show that ordinary Martin-Löf randomness with respect to the distribution is sufficient. Somewhat surprisingly, however, the picture is more complicated when we consider a weaker form of randomness where the tests are *effective*, rather than merely *effective relative to the distribution*. We show that such *Hippocratic* randomness actually coincides with ordinary randomness in that the same outcomes are random for each notion, but the corresponding test concepts do *not* coincide: while there is a universal test for ordinary ML-randomness, there is none for Hippocratic ML-randomness.

For concreteness we will focus on the classical Bernoulli experiment, although as the statistical tools we need are limited to Chebyshev's inequality and the strong law of

large numbers, our result works also in the general situation of repeated experiments in statistics, where an arbitrary sequence of independent and identically distributed random variables is studied.

When using randomness as a computational resource, the most convenient underlying probability distribution may be that of a fair coin. In many cases, fairness of the proverbial coin may be only approximate. Imagine that an available resource generates randomness with respect to a distribution for which the probability of heads is $p \neq 1/2$. It is natural to assume that p is not a computable number if the coin flips are generated with contributions from a physical process such as the flipping of an actual coin. The non-computability of p matters strongly if an infinite sequence of coin flips is to be performed. In that case, the gold standard of algorithmic randomness is *Martin-Löf randomness*, which essentially guarantees that no algorithm (using arbitrary resources of time and space) can detect any regularities in the sequence. If p is non-computable, it is possible that p may itself be a valuable resource, and so the question arises whether a "truly random" sequence should look random even to an adversary equipped with the distribution as a resource. In this article we will show that the question is to some extent moot, as these types of randomness coincide. On the other hand, while there is a universal test for randomness in one case, in the other there is not. This article can be seen as a follow-up to Martin-Löf's paper where he introduced his notion of algorithmic randomness and proved results for Bernoulli measures [3].

It might seem that when testing for randomness, it is essential to have access to the distribution we are testing randomness for. On the other hand, perhaps if the results of the experiment are truly random we should be able to use them to discover the distribution for ourselves, and then once we know the distribution, test the results for randomness. However, if the original results are not really random, we may "discover" the wrong distribution. We show that there are tests that can be effectively applied, such that if the results are random then the distribution can be discovered, and the results will then turn out to be random even to someone who knows the distribution. While these tests can individually be effectively applied, they cannot be effectively enumerated as a family. On the other hand, there is a single such test (due to Martin-Löf) that will reveal whether the results are random for *some* (Bernoulli) distribution, and another (introduced in this paper) that if so will reveal that distribution.

In other words, one can effectively determine whether randomness for some distribution obtains, and if so determine that distribution. There is no need to know the distribution ahead of time to test for randomness with respect to an unknown distribution. If we suspect that a sequence is random with respect to a measure given by the value of a parameter (in an effective family of measures), there is no need to know the value

of that parameter, as we can first use Martin-Löf's idea to test for randomness with respect to *some* value of the parameter, and then use the fundamental idea of statistics to *find* that parameter. Further effective tests can be applied to compare that parameter q with rational numbers near our target parameter p, leading to the conclusion that if all *effective* tests for randomness with respect to parameter p are passed, then all tests *having access to p as a resource* will also be passed. But we need the distribution to know *which* effective tests to apply. Thus we show that randomness testing with respect to a target distribution p can be done by two agents each having limited knowledge: agent 1 has access to the distribution p, and agent 2 has access to the data X. Agent 1 tells agent 2 which tests to apply to X.

The more specific point is that the information about the distribution p required for randomness testing can be encoded in a set of effective randomness tests; and the encoding is intrinsic in the sense that the ordering of the tests does not matter, and further tests may be added: passing any collection of tests that include these is enough to guarantee randomness. From a syntactic point of view, whereas randomness with respect to p is naturally a $\Sigma_2^0(p)$ class, our results show that it is actually an intersection of Σ_2^0 classes.

2   Definitions

If X is a $2 = \{0, 1\}$ valued random variable such that $\mathbb{P}(X = 1) = p$ (where $\mathbb{P}$ denotes probability) then X is called a Bernoulli(p) random variable. The Bernoulli measure μ_p on 2^ω is defined by the stipulation that for each $n \in \omega = \{0, 1, 2, \ldots\}$,

$$\mu_p(\{X : X(n) = 1\}) = p,$$
$$\mu_p(\{X : X(n) = 0\}) = 1 - p,$$

and $X(0), X(1), X(2), \ldots$ are mutually independent random variables.

Definition 2.1   A μ_p-ML-randomness test is a sequence $\{U_n^p\}_n$ that is uniformly $\Sigma_1^0(p)$ with $\mu(U_n^p) \leqslant 2^{-n}$, where 2^{-n} may be replaced by any computable function that goes to zero effectively.

A μ_p-ML-randomness test is *Hippocratic* if there is a Σ_1^0 class $S \subseteq 2^\omega \times \omega$ such that $S = \{(X, n) : X \in U_n^p\}$. Thus, $U_n = U_n^p$ does not depend on p and is uniformly Σ_1^0. If X passes all μ_p-randomness tests then X is μ_p-*random*. If X passes all Hippocratic tests then X is *Hippocrates μ-random*.

To explain the terminology: Andrzej Szczeklik, in "Catharsis: on the art of medicine" ([7], page 18) writes

> On his native island of Kos, only about three hundred kilometers from Delphi, Hippocrates did not consult the oracle to seek out the harbingers of fate, but looked at his patient's features instead.

In the definition of Hippocratic randomness, like the ancient medic Hippocrates we are not consulting the oracle of Delphi (i.e., an oracle for the real number p) but rather looking for "natural causes". This level of randomness recently arose in the study of randomness extraction from subsets of random sets [1].

We will often write μ_p-*random* instead of μ_p-*ML-random*, as we work in the Martin-Löf mode of randomness throughout, except when discussing a conjecture at the end of this paper.

3   Chebyshev's inequality

We develop this basic inequality from scratch here, in order to emphasize how generally it holds. For an event A in a probability space, we let $\mathbf{1}_A$, the indicator function of A, equal 1 if A occurs, and 0 otherwise. The *expectation* of a discrete random variable X is

$$\mathbb{E}(X) = \sum_x x \cdot \mathbb{P}(X = x).$$

where the sum is over all outcomes in the sample space. Thus $\mathbb{E}(X)$ is the average value of X over repeated experiments. It is immediate that

$$\mathbb{E}(\mathbf{1}_A) = \mathbb{P}(A).$$

Next we observe that the random variable that is equal to a when a nonnegative random variable X satisfies $X \geqslant a$ and 0 otherwise, is always dominated by X. That is,

$$a \cdot \mathbf{1}_{\{X \geqslant a\}} \leqslant X.$$

Therefore, taking expectations of both sides,

$$a \cdot \mathbb{P}\{X \geqslant a\} \leqslant \mathbb{E}(X).$$

In particular, for any random variable X with $\mathbb{E}(X) = \xi \in \mathbb{R}$ we have

$$a^2 \cdot \mathbb{P}\{(X - \xi)^2 \geqslant a^2\} \leqslant \mathbb{E}((X - \xi)^2).$$

Let σ^2 denote variance: $\sigma^2 = \mathbb{E}((X - \xi)^2)$. Then

$$\mathbb{P}\{|X - \xi| \geqslant |a|\} \leqslant \sigma^2/a^2.$$

If we let $k \in \omega$ and replace a by $k\sigma$, then

$$\mathbb{P}\{|X - \xi| \geqslant k\sigma\} \leqslant \sigma^2/(k\sigma)^2 = 1/k^2.$$

This is Chebyshev's inequality, which in words says that the probability that we exceed the mean ξ by k many standard deviations σ is rather small.

4 Results for ordinary randomness

We first prove a version of the phenomenon that for samples of sufficiently fast growing size, the sample averages almost surely converge quickly to the mean.

Proposition 4.1 *Consider a sequence* $Y = \{Y_n\}_{n \in \omega}$ *of independent Bernoulli(p) random variables, with the sample average*

$$\overline{Y}_n := \frac{1}{n} \sum_{i=0}^{n-1} Y_i.$$

Let $N(b) = 2^{3b-1}$ *and let*

$$U_d^p = \bigcup_{b \geqslant d} \{Y : |\overline{Y}_{N(b)} - p| \geqslant 2^{-b}\}.$$

Then U_d^p *is uniformly* $\Sigma_1^0(p)$, *and* $\mu_p(U_d^p) \leqslant 2^{-d}$, *i.e.,* $\{U_d^p\}_{d \in \omega}$ *is a* μ_p-*ML-test.*

The idea of the proof is to use Chebyshev's inequality and the fact that the variance of a Bernoulli(p) random variable is bounded (in fact, bounded by $1/4$).

Proof The fact that U_d^p is $\Sigma_1^0(p)$ is immediate, so we prove the bound on its μ_p-measure. We have

$$\mathbb{E}(\overline{Y}_n) = p \text{ and } \sigma^2(\overline{Y}_n) = \sigma^2/n,$$

where $\sigma^2 = p(1-p) \leqslant 1/4$ is the variance of Y_0 and $\sigma^2(\overline{Y}_n)$ denotes the variance of $\overline{Y}_n$. Thus $\sigma \leqslant 1/2$, and

$$\mathbb{P}\left\{|\overline{Y}_n - p| \geqslant k \cdot \sigma(\overline{Y}_n)\right\} \leqslant 1/k^2,$$

so

$$\mathbb{P}\left\{|\overline{Y}_n - p| \geqslant \frac{k}{2\sqrt{n}}\right\} \leqslant \mathbb{P}\left\{|\overline{Y}_n - p| \geqslant \frac{k \cdot \sigma}{\sqrt{n}}\right\} \leqslant 1/k^2.$$

Let b be defined by $2^{-(b+1)} = 1/k^2$. Now, we claim that $2^{-b} \geqslant \frac{k}{2\sqrt{n}}$ by taking n large enough as a function of b:

$$n \geqslant k^2 4^{b-1} = 2^{b+1} 4^{b-1} = 2^{3b-1}.$$

Thus, if $n \geqslant N(b) := 2^{3b-1}$,

$$\mathbb{P}\left\{|\overline{Y}_n - p| \geqslant 2^{-b}\right\} \leqslant 2^{-(b+1)},$$

so

$$\mathbb{P}\left\{|\overline{Y}_{N(b)} - p| \geqslant 2^{-b} \text{ for some } b \geqslant d\right\} \leqslant \sum_{b \geqslant d} 2^{-(b+1)} = 2^{-d}.$$

$\square$

Brief review of computability-theory

More details can be found in standard textbooks such as Nies [4] and Soare [6] but we provide some information here. Uppercase Greek letters such as Φ will be used for *Turing functionals*, which are partial functions $B \mapsto \Phi^B$ from 2^ω to 2^ω computed by oracle Turing machines. We write $A = \Phi^B$ if $A \in 2^\omega$ is computed from the oracle $B \in 2^\omega$ using the Turing functional Φ. Then $A(n) = \Phi^B(n)$ is the nth bit of A. An oracle Turing machine may, or may not, halt with oracle B on an input n; this is written $\Phi^B(n) \downarrow$, and $\Phi^B(n) \uparrow$, respectively.

The *Turing jump* A' is the halting set (the set of solutions to the halting problem) for oracle machines with A on the oracle tape. In terms of Turing reducibility $\leqslant_T$, the relativized halting problem remains undecidable in the sense that $A' \not\leqslant_T A$ (in fact $A <_T A'$). The Turing jump is not injective, even on Turing degrees (equivalence classes of the intersection $\equiv_T$ of the relations $\leqslant_T$ and $\geqslant_T$). Indeed, there are noncomputable sets A (so $C <_T A$ for computable sets C) such that $A' \equiv_T C'$. It is customary to pick the computable set $\varnothing$ for the notation here and simply write $A' \leqslant_T \varnothing'$. Such sets A are called *low*.

The *low basis theorem* of Jockusch and Soare asserts that each nonempty Π^0_1 class (meaning, subset of 2^ω that is Π^0_1 definable in arithmetic) has a low element. There is similarly a *hyperimmune-free basis theorem* which asserts that each nonempty Π^0_1 class contains an element A such that each function $f \in \omega^\omega$ computable from A is dominated by some computable function in ω^ω.

These basis theorems cannot be combined, as on the one hand each low hyperimmune-free set is computable, and on the other hand there are Π^0_1 classes without computable

elements (such as the set of all completions of Peano Arithmetic, or the set complement of a component U_n of a Martin-Löf randomness test). These facts will be used in Theorem 5.4.

We are now ready for a result which in a sense sums up the essence of statistics.

Theorem 4.2 *If Y is μ_p-ML-random then Y Turing computes p.*

Proof We may assume p is not computable, else there is nothing to prove; in particular we may assume p is not a dyadic rational.

Let $\{U_d^p\}_{d \in \omega}$ be as in Proposition 4.1. Since Y is μ_p-random, $Y \notin \cap_d U_d^p$, so fix d with $Y \notin U_d^p$. Then for all $b \geqslant d$, we have

(1) $$|\overline{Y}_{N(b)} - p| < 2^{-b}$$

where $N(b) = 2^{3b-1}$.

If the real number p is represented as a member of 2^ω via

$$p = \sum_{n \in \omega} p_n 2^{-n-1} = .p_0 p_1 p_2 \cdots$$

in binary notation, then we have to define a Turing functional Ψ_d such that $p_n = \Psi_d^Y(n)$.

We pick $b \geqslant \max\{n+1, d\}$, such that $\overline{Y}_{N(b)} = .y_0 \cdots y_n \cdots$ is not of either of the forms

$$.y_0 \cdots y_n 1^{b-(n+1)} \cdots$$
$$.y_0 \cdots y_n 0^{b-(n+1)} \cdots$$

where as usual 1^k denotes a string of k ones. Since p is not a dyadic rational, such a b exists. Then by (1) it must be that the bits $y_0 \cdots y_n$ are the first $n+1$ bits of p. In particular, $y_n = p_n$. So we let $\Psi_d^Y(n) = y_n$. $\qquad \square$

5 Hippocratic results

In the last section we made it too easy for ourselves; now we will obtain the same results assuming only Hippocratic randomness.

Theorem 5.1 *There is a Hippocratic μ_p-test such that if Y passes this test then Y computes an accumulation point q of the sequence of sample averages*

$$\{\overline{Y}_n\}_{n \in \omega}.$$

Proof   The point is that the usual proof that each convergent sequence is Cauchy gives a Σ_1^0 class that has small μ_p-measure for all p simultaneously. Namely, let

$$V_d := \{Y : \exists a, b \geqslant d \; |\overline{Y}_{N(a)} - \overline{Y}_{N(b)}| \geqslant 2^{-a} + 2^{-b}\},$$

where $N(b) = 2^{3b-1}$. Then $\{V_d\}_{d \in \omega}$ is uniformly Σ_1^0. Recall from Proposition 4.1 that we defined

$$U_d^p = \{Y : \exists b \geqslant d \; |\overline{Y}_{N(b)} - p| \geqslant 2^{-b}\}.$$

If there is a p such that $|\overline{Y}_{N(b)} - p| < 2^{-b}$ for all $b \geqslant d$, then

$$|\overline{Y}_{N(a)} - \overline{Y}_{N(b)}| \leqslant |\overline{Y}_{N(a)} - p| + |p - \overline{Y}_{N(b)}| < 2^{-a} + 2^{-b}$$

for all $a, b \geqslant d$; thus we have

$$V_d \subseteq \cap_p U_d^p$$

and therefore

$$\mu_p(V_d) \leqslant \mu_p(U_d^p) \leqslant 2^{-d}$$

for all p. Thus if Y is Hippocrates μ_p-random then $Y \notin V_d$ for some d. We next note that for any numbers $c > b$,

$$|\overline{Y}_{N(b)} - \overline{Y}_{N(c)}| < 2^{-b} + 2^{-c} < 2^{-(b-1)},$$

so $\{\overline{Y}_{N(c)}\}_{c \geqslant d}$ will remain within $2^{-(b-1)}$ of $\overline{Y}_{N(b)}$ for all $c > b$. Thus $\{\overline{Y}_{N(n)}\}_{n \geqslant d}$ is a Cauchy sequence and $q := \lim_n \overline{Y}_{N(n)}$ exists. Write $q = .q_0 q_1 q_2 \cdots$. Then

$$|\overline{Y}_{N(b)} - q| < 2^{-(b-1)}, \text{ so}$$
$$|\overline{Y}_{N(b+1)} - q| < 2^{-b};$$

if we define Θ_d as Ψ_d in the proof of Theorem 4.2 except with $N(\cdot)$ replaced by $N(\cdot + 1)$, then

$$q_n = \Theta_d^Y(n),$$

and so Y computes q using the Turing reduction Θ_d. $\square$

To argue that the accumulation point q of Theorem 5.1 is actually equal to p under the weak assumption of Hippocratic randomness, we need:

An analysis of the strong law of large numbers.

We say that the strong law of large numbers (SLLN) is satisfied by $X \in 2^\omega$ for the parameter $p \in [0, 1]$ if $\lim_{n \to \infty} \overline{X}_n / n = p$. The strong law of large numbers is then the

statement that the set of those X that do not satisfy the SLLN for p has μ_p-measure zero.

Let $\{X_n\}_{n\in\omega}$ be independent and identically distributed random variables with mean 0, and let $S_n = \sum_{i=0}^{n} X_i$. Then S_n^4 will be a linear combination (with binomial coefficients as coefficients) of the terms

$$\sum_i X_i^4, \quad \sum_{i<j} X_i^3 X_j, \quad \sum_{i<j<k} X_i^2 X_j X_k, \quad \sum_{i<j<k<\ell} X_i X_j X_k X_\ell, \quad \text{and} \quad \sum_{i<j} X_i^2 X_j^2.$$

Since $\mathbb{E}(X_i) = 0$, and $\mathbb{E}(X_i^a X_j^b) = \mathbb{E}(X_i^a)\mathbb{E}(X_j^b)$ by independence, and each X_i is identically distributed with X_1 and X_2, we get

$$\mathbb{E}(S_n^4) = n\,\mathbb{E}(X_1^4) + \binom{n}{2}\binom{4}{2}\mathbb{E}(X_1^2 X_2^2) = n\,\mathbb{E}(X_1^4) + 3n(n-1)\mathbb{E}(X_1^2)^2.$$

Since $0 \leqslant \sigma^2(X_1^2) = \mathbb{E}(X_1^4) - \mathbb{E}(X_1^2)^2$, this is (writing $K := \mathbb{E}(X_1^4)$)

$$\leqslant (n + 3n(n-1))\mathbb{E}(X_1^4) = (3n^2 - 2n)K,$$

so $\mathbb{E}(S_n^4/n^4) \leqslant \frac{3K}{n^2}$. Now for any $a \in \mathbb{R}$,

$$S_n^4/n^4 \geqslant a^4 \cdot \mathbf{1}_{\{S_n^4/n^4 \geqslant a^4\}}$$

surely, so (as in the proof of Chebyshev's inequality)

$$\mathbb{E}(S_n^4/n^4) \geqslant a^4 \cdot \mathbb{E}(\mathbf{1}_{\{S_n^4/n^4 \geqslant a^4\}}) = a^4 \cdot \mathbb{P}(S_n^4/n^4 \geqslant a^4),$$

giving

$$\mathbb{P}(\overline{X}_n = S_n/n \geqslant a) \leqslant \frac{3K}{n^2 a^4}.$$

We now apply this to $X_n = Y_n - \mathbb{E}(Y_n) = Y_n - p$ (so that $K_p := K$ depends on p). Note that (writing $\overline{p} = 1 - p$)

$$K_p = \mathbb{E}[(Y_1 - p)^4] = \overline{p}^4 \cdot p + p^4 \cdot \overline{p} = p\overline{p}(\overline{p}^3 + p^3) \leqslant \frac{1}{4}\cdot 2 = \frac{1}{2},$$

so $\mathbb{P}(\exists n \geqslant N \, |\overline{Y}_n - p| \geqslant a)$ is bounded by

$$\sum_{n \geqslant N} \frac{3K_p}{n^2 a^4} \leqslant \frac{3}{2a^4} \sum_{n \geqslant N} \frac{1}{n^2} \leqslant \frac{3}{2a^4} \int_{N-1}^{\infty} \frac{dx}{x^2} = \frac{3}{2a^4(N-1)}.$$

This bound suffices to obtain our desired result:

Theorem 5.2 *If Y is Hippocrates μ_p-random then Y satisfies the strong law of large numbers for p.*

Proof Let q_1, q_2 be rational numbers with $q_1 < p < q_2$. Let

$$W_N := \{Y : \exists n \geqslant N \ \overline{Y}_n \leqslant q_1\} \cup \{Y : \exists n \geqslant N \ \overline{Y}_n \geqslant q_2\}.$$

Then $\{W_N\}_{N \in \omega}$ is uniformly Σ^0_1, and $\mu_p(W_N) \to 0$ effectively:

$$\mu_p(W_N) \leqslant \frac{3}{2(p - q_1)^4(N - 1)} + \frac{3}{2(p - q_2)^4(N - 1)} = \text{constant} \cdot \frac{1}{N - 1}.$$

Thus if Y is Hippocrates μ_p-random then $Y \notin \cap_n W_n$, i.e., $\overline{Y}_n$ is eventually always in the interval (q_1, q_2). $\qquad\square$

Corollary 5.3 *If Y is Hippocrates μ_p-random then Y Turing computes p.*

Proof By Theorem 5.1, Y computes the limit of a subsequence $\{\overline{Y}_{N(b)}\}_{b \in \omega}$. By Theorem 5.2, this limit must be p. $\qquad\square$

Note that the randomness test in the proof of Theorem 5.2 depends on the pair (q_1, q_2), so we actually needed infinitely many tests to guarantee that Y computes p. This is no coincidence. Let $Y \geqslant_T p$ abbreviate the statement that Y Turing computes p, i.e., p is Turing reducible to Y.

Theorem 5.4 *For all p, if there is a Hippocratic μ_p-test $\{U_n\}_{n \in \omega}$ such that*

$$\{X : X \not\geqslant_T p\} \subseteq \cap_n U_n,$$

then p is computable.

Proof Let $\{U_n\}_{n \in \omega}$ be such a test. By standard computability theoretic basis theorems, the complement $2^\omega \setminus U_1$ has a low member X_1 and a hyperimmune-free member X_2. By assumption $X_1 \geqslant_T p$ and $X_2 \geqslant_T p$, so p is both low and hyperimmune-free, hence by another basic result of computability theory [6], p is computable. $\qquad\square$

Corollary 5.5 *There is no universal Hippocratic μ_p-test, unless p is computable.*

Proof If there is such a test then by Corollary 5.3 there is a test $\{U_n\}_{n \in \omega}$ as in the hypothesis of Theorem 5.4, whence p is computable. $\qquad\square$

Comparison with earlier work. Martin-Löf [3] states a result that in our terminology reads as follows.

Theorem 5.6 *There is a test that is a Hippocratic ML-test simultaneously for all μ_p, the passing of which implies that the Strong Law of Large Numbers is satisfied for some p.*

Levin [2] in fact states that a real x passes Martin-Löf's test from Theorem 5.6 if and only if x is (non-Hippocratically) μ_p-ML-random for some $p \in [0,1]$. This he obtains as a corollary of the following more general result: For any Π_1^0 class $\mathcal{C}$ of measures (such as the class of Bernoulli measures), there is a uniformly Σ_1^0 test $\{U_n\}_{n\in\omega}$, with $\mu(U_n) \leqslant 2^{-n}$ for each n and each $\mu \in \mathcal{C}$, such that a real $x \notin \cap_n U_n$ iff x is μ-ML-random with respect to some measure $\mu \in \mathcal{C}$.

Thus we see by Theorem 5.6 that we did not need infinitely many tests in the above proof of Theorem 5.2, in order to get the Strong Law of Large Numbers to be satisfied for *some p*; only to get it to be the *correct p*.

6   Coincidence of randomness notions

We now show that Hippocratic randomness is the same as ordinary randomness for Bernoulli measures. The main idea is that since each random sequence computes p, it should be possible to turn a $\Sigma_1^0(p)$ test into a Σ_1^0 test.

Definition 6.1 Let $\{O_n^p\}_{n\in\omega}$ be a universal μ_p-test for all p, i.e. $\mu_p(O_n^p) \leqslant 2^{-n}$ for all p and $\{(p,X,n) : X \in O_n^p\}$ is Σ_1^0, and if $\{\widehat{O}_n\}_{n\in\omega}$ is any other such test then $\cap_n \widehat{O}_n \subseteq \cap_n O_n$.

The existence of such a test follows from a relativization of the usual argument that there is a universal Martin-Löf test.

Theorem 6.2 *If Y is Hippocrates μ_p-random then Y is μ_p-random.*

Proof Let $\mathcal{H}_p$ be the set of all Hippocrates μ_p-random reals and $2^\omega \setminus \mathcal{H}_p$ its complement. As in the proof of Theorem 5.1, let

$$V_d = \{Y : \exists a, b \geqslant d \ |\overline{Y}_{N(a)} - \overline{Y}_{N(b)}| \geqslant 2^{-a} + 2^{-b}\}$$

where $N(b) = 2^{3b-1}$. Let Θ_d denote the reduction from the proof of Theorem 5.1 under the assumption $Y \notin V_d$ there.

We have

$$\{Y : Y \notin V_d\} \subseteq \{Y : \Theta_d^Y \text{ is total }\} \subseteq \{Y : \Theta_d^Y = p\} \cup (2^\omega \setminus \mathcal{H}_p).$$

Let

$$D_n^{(d)} := \left\{ Y : \exists k \ \left(\Theta_d^Y \restriction k \downarrow \ \& \ Y \in O_n^{\Theta_d^Y \restriction k} \right) \right\}.$$

Then

$$D_n^{(d)} \subseteq O_n^p \cup \{Y : \Theta_d^Y \neq p\} \subseteq O_n^p \cup V_d \cup (2^\omega \setminus \mathcal{H}_p).$$

Of course, $\mu_p(2^\omega \setminus \mathcal{H}_p) = 0$. So

$$\mu_p(D_n^{(d)}) \leqslant \mu_p(O_n^p) + \mu_p(V_d) \leqslant 2^{-n} + 2^{-d}.$$

Form the diagonal $W_n = D_n^{(n)}$; then $\mu_p(W_n) \leqslant 2^{-(n-1)}$ which goes effectively to zero, so $\{W_n\}_{n \in \omega}$ is a Hippocratic μ_p-test.

Suppose for contradiction that Y is Hippocrates μ_p-random but not μ_p-random. Since Y is not μ_p-random, for all n, $Y \in O_n^p$. Since Y is Hippocrates μ_p-random, there is a d such that $Y \notin V_d$ and for this d, $\Theta_d^Y = p$; in fact for all $n \geqslant d$, $\Theta_n^Y = p$. Then $Y \in \cap_{n \geqslant d} D_n^{(n)}$. So Y is not Hippocrates μ_p-random. $\qquad\square$

An open problem. Randomness tests $\{U_n\}_{n \in \omega}$ can be made more effective by requiring that $\mu_p(U_n)$ is a number that is computable from p. This is essentially Schnorr randomness [5]. It is not hard to show that Schnorr randomness is sufficient for statistics to work, i.e. to ensure that a random sequence Y computes the parameter p. More radically, we could require that $\mu_p(U_n)$ be actually computable. If we then relax the other side and let U_n be $\Sigma_1^0(p)$, again a random sequence can be made to compute p, because one can "pad" U_n to make it have μ_p-measure equal to a computable number such as 2^{-n}.

Question 6.3 If we both require U_n to be (uniformly) Σ_1^0 and $\mu_p(U_n)$ to be (uniformly) computable, is it still true that a random sequence must compute p?

References

[1] Bjørn Kjos-Hanssen, *Infinite subsets of random sets of integers*, Math. Res. Lett. **16** (2009), no. 1, 103–110.

[2] L. A. Levin, *The concept of a random sequence*, Dokl. Akad. Nauk SSSR **212** (1973), 548–550 (Russian).

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

[4] André Nies, *Computability and randomness*, Oxford Logic Guides, vol. 51, Oxford University Press, Oxford, 2009; doi:10.1093/acprof:oso/9780199230761.001.0001.

[5] Claus-Peter Schnorr, *Zufälligkeit und Wahrscheinlichkeit. Eine algorithmische Begründung der Wahrscheinlichkeitstheorie*, Lecture Notes in Mathematics, Vol. 218, Springer-Verlag, Berlin, 1971.

[6] Robert I. Soare, *Recursively enumerable sets and degrees*, Perspectives in Mathematical Logic, Springer-Verlag, Berlin, 1987.

[7] Andrzej Szczeklik, *Catharsis: on the art of medicine*, The University of Chicago Press, 2005.

Department of Mathematics, University of Hawai'i at Mānoa, 2565 McCarthy Mall, Honolulu, HI 96822

bjoern@math.hawaii.edu

http://www.math.hawaii.edu/~bjoern