Effective Randomness

organized by
Denis Hirschfeldt and Joseph Miller

Workshop Summary

Let $\mathcal{A} = \{a_1, a_2, \dots\}$ be an infinite sequence of 0s and 1s. What does it mean to say that this sequence is random? If we are given two such sequences, then what does it mean to say that one sequence is more random than the other?

These are fundamental questions, and are related to questions of computability theory. The connections between these two subject areas are the subject of the present workshop.

The idea of a random sequence finds its germ with A. Kolmogorov. Some say that he invented modern probability theory in order to deal with this problem. Intuitively speaking, a sequence should be random if it does not have any interesting (or "rare") properties. Roughly speaking, a property is *rare* if it has measure 0. The trouble is that any point has measure zero, so this is not the right definition. Instead we have a notion of "effective measure 0". A set is said to have *effective measure 0* if it is the decreasing limit of an effective sequence of open sets (in a suitable inductive topology) whose measures tend to zero. We may say that a point is random if it does not lie in any of these sets of measure zero.

One upshot of the measure-theoretic description of randomness that we have been outlining is that a random sequence should have roughly as many 0s as 1s. Richard von Mises analyzed this idea in terms of countable collections of stochastic properties. Alonzo Church made the connection with computability by positing that one should consider all *computable* stochastic properties. Martin-Löf then pushed the idea further by proposing that this gives rise to the idea of effectively measure zero sets. To summarize, if a property constitutes an effective null set, then a random set should not have this property. Thus a random set is a set with no effectively rare properties.

We have just given a rough description of the measure-theoretic paradigm for randomness. There are others. We shall briefly describe here the unpredictability paradigm and the incompressibility paradigm.

The Unpredictability Paradigm In this view of randomness, we say that a sequence is random if, given an initial string, we cannot predict the later behavior of the sequence. This property is rigorously expressed in terms of martingales (betting strategies).

The Incompressibility Paradigm This is essentially the original approach of Kolmogorov. We say in this view that a sequence is random if it has no short description, i.e., there is no short program to generate the string. This means that the only way that a machine can generate the string is if the entire string is hard-wired into it. This paradigm is most efficiently expressed in the language of Turing machines.

One of the key goals of the Effective Randomness workshop is to develop the connections between randomness and computability. A major player in this work has been Jack Lutz of Iowa State University. He was present at the workshop, and a vigorous participant. Lutz impacted the subject by coming up with a way of effectivizing the notion of Hausdorff dimension (a version of fractional, or "fractal" dimension) and packing dimension in terms of an idea called *gales*. Here a "gale" is a sort of martingale.

A natural object to examine, from Lutz's point of view, is the fractal dimension of a self-similar fractal. Falconer and others have been pioneers in such calculations. In the sense of effective randomness—described above—a single point can actually have positive dimension in a sense defined below. As a result, Lutz can show in many cases that the fractal dimension of a set S is actually equal to the supremum of the fractal dimensions of all its individual points.

We have alluded above to connections between the theory of randomness and complexity theory. One concrete connection is this. The traditional method for determining the complexity of an algorithm is to average over the complexity of all possible cases. But one could instead look at the complexity for a random input. Thus one needs a palpable means of identifying what "random" means in this context.

Certainly this workshop has some big problems in mind for study. These all center around finding new ways to understand randomness. We say that a sequence is *partially random* if

$$0 < \liminf_{n \to +\infty} \frac{\text{complexity of first } n \text{ bits}}{n} < 1 \, .$$

[This liminf is a way to define the notion of effective dimension mentioned above.] The question then is whether one can reconstruct full randomness from partial randomness (going in the other direction is fairly straightforward, as it amounts basically in forgetting information).

Another line of inquiry is to consider betting sequences which are non-monotone. That is to say, one does *not* place bets in linear order, but rather proceeds in a more arbitrary fashion. This gives rise to yet another notion of randomness, and one would like to know whether it is equivalent to the classical Martin-Löf idea of randomness.

Randomness is studied by theoretical computer scientists, by probabilists, and by logicians. It is a meeting ground for many fertile ideas. This workshop made a special effort to create a dialogue among the different groups. There was an especially large contingent of graduate students who hoped to learn new problems and new techniques.