Theoretical interlude—
What is randomness?
My definitions

Finally, THE definition of randomness!!
Warning to the reader!

There’s only one definition of randomness (divided into the finite and the infinite case for technical reasons): something is random if it is algorithmically incompressible or irreducible. More precisely, a member of a set of objects is random if it has the highest complexity that is possible within this set. In other words, the random objects in a set are those that have the highest complexity. Applied to the set of all n-bit strings this gives one of our definitions, applied to infinite binary sequences this gives our second definition.

This is the basic, new fundamental idea in AIT, and it’s the source of the randomness that I discovered in the heart of pure mathematics, the randomness that Gödel and Turing encountered without realizing it! This one idea is the raison d'être of AIT. I want to understand randomness, I want to formulate the theory that defines it as well as I can.

But in Part III I’ll temporarily introduce a number of variant definitions just in order to show that they’re equivalent!

Don’t get confused!
What is randomness? Overview of six variant definitions

This chapter is a theoretical interlude; we’ll stop programming for a while and discuss definitions of randomness = incompressibility = irreducibility. One of the key contributions of AIT is the recognition that this program-size kind of randomness also implies that something is typical and undistinguished, that is, the more traditional statistical kind of randomness.

In this part we discuss five, really six, definitions of randomness: my two for bit strings (using absolute and relative complexity, respectively), and four for infinite binary sequences or, equivalently, for base-two real numbers. Two of the definitions for random real are statistical (Martin-Löf’s and Solovay’s), and two involve program size (my two: Chaitin and strong Chaitin randomness).

It turns out that the two definitions of a random bit string are equivalent, and that the four definitions for random reals are equivalent. That’s a very good sign; it confirms that we’ve captured the correct concept!

In this chapter we’ll show that my two definitions of random bit string are equivalent, but it’ll take us all of Part III to prove that the four definitions of a random real number are equivalent.

The common thread of my definitions is, as I said, that incompressible implies typical, and that a “random” string is one that has “close to” the highest possible complexity. So it turns out that a random n-bit string \( \beta \) is one for which \( H(\beta) \) is close to \( n + H(n) \), which is the greatest possible and also the typical complexity of an n-bit string.

\[
n\text{-bit } \beta \text{ is random } \iff H(\beta) \approx n + H(n)
\]

As the complexity of \( H(\beta) \) drops below this \( \beta \) becomes less and less random; it is a matter of degree.\(^1\)

For random infinite binary sequences \( x \), we consider the complexity \( H(x_n) \) of the first \( n \) bits of \( x \) as a function of \( n \), and we’ll demand that \( x_n \) always be random, as random as possible. Due, for example, to long

\(^1\)If you must pick a cutoff, it should be at around \( H(\beta) = n \).