Cantor's Diagonal Argument, Russell's Paradox, and Unsolvable Problems

November 13, 2007

1 Another Look at the Diagonal Argument and Uncountable Sets

Much the same argument used to prove that the set $\mathbf{R}$ of real numbers is uncountable also shows that the set $\mathcal{P}(\underline{\mathrm{Z}}^+)$ of subsets of the positive integers is uncountable. We can encode each subset X of $\mathbf{Z}^+$ as an infinite sequence of bits, where the i^{th} bit is 1 if and only if $i \in X$, for example

$$\{1, 3, 5, 7, 9, \ldots\}$$

is encoded by

$$10101010\ldots$$

Suppose we have a sequence $X_1, X_2, \ldots$ of subsets of $\mathbf{Z}^+$ encoded by sequences $s_1, s_2, \ldots$. We form a sequence of bits t whose i^{th} bit is the *opposite* of the i^{th} bit of s_i. This is the diagonalization trick. The sequence t is the encoding of the set

$$Y = \{i : i \notin X_i\}.$$

The set Y cannot be identical to any of the X_i. Why not? Suppose $Y = X_i$ for some i. Let's ask if $i \in Y$. If it is, then $i \in X_i$, so by the definition of Y, $i \notin Y$. But if $i \notin Y$, then $i \notin X_i$, so again by the definition, $i \in Y$. In other words, i belongs to y if and only if it doesn't belong to Y. What the...? This proves that Y is not equal to any X_i, and thus any list of subsets of $\mathbf{Z}^+$ cannot be complete. Thus $\mathcal{P}(\underline{\mathrm{Z}}^+)$ is uncountable.

The diagonal argument was discovered by Georg Cantor in the late nineteenth century.

2 Who Saves the Barber?

This is a whimsical argument used to illustrate diagonalization, and especially Russell's Paradox (below).

In a certain village, all the men are clean-shaven. One of the men is a barber, and the barber shaves all and only the men in the village who do not shave themselves.

Who shaves the barber?

If he shaves himself, then the criterion above is violated, since he is only supposed to shave the men who don't shave themselves. If he doesn't shave himself, then again by the above criterion, he does shave himself. If he does he doesn't, and if he doesn't he does. What the...? But what the paradox shows is that there can be no barber as described above.

3 Russell's Paradox

Bertrand Russell formulated this around 1900, after study of Cantor's diagonal argument. Some logical formulations of the foundations of mathematics allowed one great leeway in defining sets. In particular, they would allow you to define a set like

$$A = \{X : X \notin X\},$$

i.e., the set of all sets that are not elements of themselves.

Now is A an element of itself? Just like the barber and the set Y above, if it is, it isn't and if it isn't it is. But there is no easy way out this time, because the consequence is that a foundation for mathematics that allows this kind of set formation is inconsistent, and has to be completely overhauled.

4 An Undecidable Problem

Turing's proof of the existence of undecidable problems is based on the same diagonal argument. We can encode Turing machines as strings We denote the encoding of the machine M by $< M >$. It really doesn't matter what sort of encoding we use, but let's suppose for the sake of definiteness that the encoding is a string over the alphabet $\{0, 1\}$. We can now define the language

$$L = \{< M >: M doesnotaccept < M >\}.$$

In other words, L is the collection of encodings of Turing machines that do not accept their own encoding.

Is L turing recognizable? Well, suppose N is a Turing machine that recognizes L. Is $< N > \in L$? In other words, does N accept $< N >$? N is like that barber—it accepts its own encoding if and only if it doesn't accept its own encoding. So N simply cannot exist, and thus L is not Turing-recognizable.

On the other hand, the language

$$K = \{< M >: M accepts < M >\}$$

is Turing-recognizable. This depends on the existence of a Turing machine U that can read the encoding of a Turing machine M and simulate M. (U is a *universal Turing machine.*) But K is not decidable, because we cannot recognize when M does not accept $< M >$.