Incompleteness

Note Title 9/20/2015

Gödel's THEOREM. Any sufficiently powerful axiomatic system (i.e. formalization of mathematics) is either inconsistent (i.e. $\exists$ statement S s.t. both S and its negation can be proven), OR it has a true statement that cannot be proven.

"sufficiently powerful" = can encode Turing machines.

HALT(M,x): TM M halts on input x.

Can be written in the system

A1. If M halts on x, there is a proof P_x of HALT(M,x).

A2. If M loops on x, there is a proof $\overline{P}_x$ of $\overline{\text{HALT}}(M,x)$.

TM D:

Given $\langle M \rangle$ as input:

enumerate proofs P

check if P is a proof of HALT(M, $\langle M \rangle$)
then loop forever

else if P is a proof of $\overline{\text{HALT}}(M, \langle M \rangle)$
halt.

What does D do input $\langle D \rangle$?

If D halts on $\langle D \rangle$ and there is a proof that it does, then D will find it and loop forever.

If D does not halt on $\langle D \rangle$ and there is a proof that it does not halt, then D will halt.

$\therefore$ There is no proof (within the system) that D will halt or D will not halt on input $\langle D \rangle$.

so there is also a proof that D will not halt on $\langle D \rangle$ $\Rightarrow$ inconsistent system.

We can also deduce this (and other unprovable facts) from Kolmogorov sets.

Recall $L_K = \{ x : K(x) \geq |x| \}$ is an infinite undecidable language.

$K(x) = \min \{ |\langle M \rangle| + |y| :$ M is a TM that on input y outputs x $\}$

Take any axiomatic system in which we can express "$K(x) \geq n$".

<u>Assume</u> it can be verified whether or not a string P is a proof of a statement in the system.

<u>Thm</u>. $\exists$ true statements that are unprovable within any consistent system.

OR, more concretely $\exists n, x$ s.t. "$K(x) \geq n$" is true but cannot be proven.

<u>Pf.</u> Suppose that for each x and each n if "$K(x) \geq n$" it has a proof. Any candidate proof P of a statement S can be verified.

But this gives us the ability to find incompressible strings:

TM M: On input n:

enumerate pairs (s, p) of integers

For each (s, p):

enumerate strings x of length s and proofs P of length p

Check if P is a proof that "$K(x) \geq n$".

If yes, output x and stop.

If x, P exist for n, then M outputs x for which

$$n \leq K(x) \leq C + \log n$$

$\therefore \exists n_0$ s.t. $\forall n \geq n_0$, "$K(x) \geq n$" has no proof!

This is particularly striking since it is easy to produce strings x for which $K(x) \geq n$.

Pick random strings of length $n+1$.

then w.p. $\geq \frac{1}{2}$, $K(x) \geq n$