Computation Theory 2005 - Paper 3 Question 7 (AMP)

(a) The Halting Problem: let S consist of pairs (A, D) where A is an algorithm and D is some input data for A. The Halting Problem is the subset P of S consisting of those (A, D) for which A run on D eventually halts.

Claim: there is no algorithm H such that

2 for all $(A,D) \in S$, $H(A,D) = \begin{cases} 1 & \text{if } (A,D) \in P \\ 0 & \text{if } (A,D) \notin P. \end{cases}$

Proof: suppose there were such an H. Use it

1 to construct an algorithm C:

"input A, compute H(A, A) and if it is equal

1 to 0 then output 1 & halt; otherwise loop forever."

So for all algorithms A

$C(A)$ halts $\iff H(A,A) = 0$

$\iff A(A)$ does not halt, by definition of H.

2 Taking A to be C, we get

$C(C)$ halts $\iff C(C)$ does not halt

6 contradiction. So no such H can exist.

(b) Two other algorithmically undeciable problems:

(1) Hilbert's Entscheidungsproblem: decide whether

2 any given statement of first order arithmetic is provable from Peano's axioms.

2 (2) Hilbert's 10^{th} Problem: decide whether any given Diophantine equation ($p(x_1, \dots, x_n) = 0$, where p is a polynomial with integer coefficients) has an integral solution ($(x_1, \dots, x_n) \in \mathbb{Z}^n$).

4

(c) $f \in Pfn(\mathbb{N}^n, \mathbb{N})$ is register machine computable iff there is a register machine M so that for all $(x_1, \dots, x_n) \in \mathbb{N}^n$ and $y \in \mathbb{N}$

$f(x_1, \dots, x_n) = y$ iff M started with $x_1, \dots, x_n$ in registers $R1, \dots, Rn$ & all other registers zeroed, halts with $R0$ containing value y.

2

To formalise the argument in part (a), we need to

1 (1) define a coding of lists of numbers $a_1, \dots, a_n$ as numbers

1 (2) define a coding of register machine programs Prog as numbers $\ulcorner Prog \urcorner$

1 (3) Write some register machine programs for operations on lists, using the coding from (1); specifically

(a) copying the contents of one register to another

(b) pushing the contents of one register onto the head of a(n encoded) list in another register.

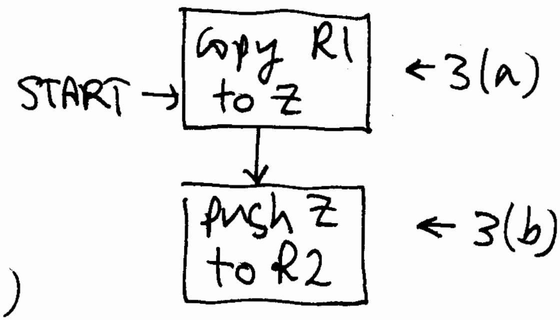
Then we can show:

There is no register machine H with the property that, started with R1 = e, R2 = code of $a_1, \ldots, a_n$, and all other registers zeroed, the computation of H always halts with R0 containing 0 or 1; moreover R0 contains 1 when H halts iff the registermachine with code e started with $R1 = a_1, \ldots, Rn = a_n$ (& all other registers zeroed)

1 does halt.

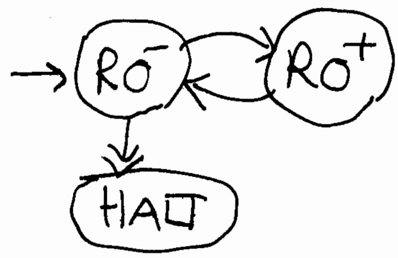
Proof ~~that~~ H cannot exist is as in part (a): to construct register machine C from H we

2 - replace START → by



(where Z is not mentioned in H's program)

2 - replace each HALT by



(10)