6 The Halting Problem

(6.1) Definition

- TM *is the set of all bitstrings which are valid encodings of Turing machines.*
- *If* y *is a valid encoding of a Turing machine, then* T_y *is the machine it encodes.*
- *If* M *is a Turing machine and* x *an input string, then we write* $M(x)\downarrow$ *if, on input* x*,* M *eventually halts, and* $M(x)\downarrow a$ *if, on input* x*,* M *eventually halts with output* a*. Also,* $M(x)\uparrow$ *if* M *loops on input* x*.*

The *halting problem* is:

> *Given a Turing machine* M *and an input string* x*, to determine if* M *halts on input* x*.*

(6.2) Definition

$$\text{HALTING} = \{x \in \{0,1\}^* : \ (\exists y \in \text{ TM })(\exists z \in \{0,1\}^*) \ (x = yz \wedge T_y(z)\downarrow)\}.$$

Q: What would be considered a solution to the Halting Problem? A: A Turing machine T such that, on input x,

$$\begin{cases} T(x)\downarrow 1 & \text{if } x \in \text{HALTING} \\ T(x)\downarrow 0 & \text{if } x \notin \text{HALTING} \end{cases}$$

(6.3) Theorem *Put this way, the halting problem has no solution.*

Proof. Otherwise, one could construct a TM M which on input x,

- M first 'doubles' its input to a string xx of twice the length, then applies the quintuples of T, i.e., decides whether xx is in HALTING; then M takes the following action, which will lead to contradictory behaviour:
- If $xx \in$ HALTING, $M(x)\uparrow$, and
- if $xx \notin$ HALTING, $M(x)\downarrow$.

The rest of the argument is that M differs from every known Turing machine T_y. Or rather, it is impossible that $M = T_c$ where $c \in$ TM. Let c be any string in TM.

Suppose $M(c)\uparrow$.

Then $cc \in$ HALTING, so $cc = yz$ where $y \in$ TM and $T_y(z)\downarrow$. so cc can be factored as yz where $y \in$ TM and $T_y(z)\downarrow$.

By the unique factorisation property mentioned in the previous section, $y = c$ and $z = c$ and $T_c(c)\downarrow$. Since $M(c)\uparrow$, $M \neq T_c$.

Suppose $M(c)\downarrow$. Then $cc \notin$ HALTING, so cc has no factorisation as yz where $y \in$ TM and $T_y(z)\downarrow$. In particular, cc is not such a factorisation: $T_c(c)\uparrow$ and $M(c)\downarrow$, so again $T_c \neq M$. ∎

6.1 Diagonalisation

This is 'diagonalisation' invented by Cantor, who used it to show that for no set X can any map $f : X \to \mathcal{P}X$ (the power set) be surjective.

Similarly, $\mathbb{R}$ is uncountable. It is enough to show that the set of real numbers $.a_1 a_2 \ldots$ where $2 \leqslant a_j \leqslant 7$ for $j = 1, 2, \ldots$, is uncountable.

Put it this way: for any list $a_1, a_2, \ldots$ of real numbers (in this range), each number having the expansion $a_{11}a_{12}a_{13}\ldots$, there is a number b not in this list:

$$b_i = 9 - a_{ii}$$