

Applies to NTMs too.

**Informal Def:** Say a TM  $M$  does "good housekeeping" if

- $M$  never writes blank(s) between non-blank chars, and  $\begin{bmatrix} q_{acc} \\ 1 \end{bmatrix}$  30 alphabet  $\Sigma \times \Gamma \cup \Gamma$
- whenever  $M$  intends to accept,  $M$  first erases all non-blank contents of all tapes and ends in the unique accepting ID  $\begin{bmatrix} q_{acc} \\ 1 \end{bmatrix}$ . 10 alphabet  $\Sigma \cup \Gamma$

(If the input tape  $x$  is read-only, we'll end in  $\begin{bmatrix} x \\ q_{acc} \end{bmatrix}$  instead.)

Given a 1-tape TM  $M = (Q, \Sigma, \Gamma, \delta, D, S, q_{acc}, q_{rej})$  (that does good housekeeping) define "tri-ominoes" of the form  $\begin{bmatrix} c & q & e \\ c' & d' & e' \end{bmatrix}$  is an instruction in  $\delta$  and:

And there are "edge" ones  $\begin{bmatrix} c & q \\ c' & d' \end{bmatrix}$ , plus we could make ones for visiting new cells at the left end.

For the end of the good housekeeping routine, we have erasure "dominoes" where the instruction is  $(q, d/D, L, r)$  (wlog needed only in the end stage before going to  $q_{acc}$ ).

Finally, we have "monominoes"  $\begin{bmatrix} c \\ c \end{bmatrix}$  for all  $c \in \Gamma$ , and initially just nothing for  $c \in \Sigma$ .

Plus  $\begin{bmatrix} \# \\ \# \end{bmatrix}$

**Post Correspondence Problem:** Given a set of "ominoes" and an initial configuration can it be completed so that the bottom is the same [length] as the top?

The more careful defn of PCP emulates the action of our two-tape DFA that checks computations.

Initial "domino"  $I_0(x)$  on bottom

end.

The 2-tape DFA has a valid completion of  $I_0(x) \iff M$  accepts  $x$ , so (this form of) PCP is undecidable.

Emil Post actually had in mind — in 1929! — a machine that acts as a queue and writes the bottom half of an "omino" to the queue and re-runs on the output until the queue empties.

In the next pic I have fixed my brain-blip of forgetting that the initial domino(s) put the initial ID  $I_0(x)$  on the bottom not the top, and I use the stronger statement that the top and bottom strings are the same, not just of the same length. The first drawing with  $\wedge$ s should be viewed as a "detail" of the second one.

For the end of the good housekeeping routine, we have erasure "dominoes" where the instruction is  $(q, d/D, L, r)$  (wlog needed only in the end stage before going to  $q_{acc}$ ).

Finally, we have "monominoes"  $\begin{bmatrix} c \\ c \end{bmatrix}$  for all  $c \in \Gamma$ , and initially just nothing for  $c \in \Sigma$ .

Plus  $\begin{bmatrix} \# \\ \# \end{bmatrix}$

**Post Correspondence Problem:** Given a set of "ominoes" and an initial configuration can it be completed so that the bottom is the same [length] as the top?

The more careful defn of PCP emulates the action of our two-tape DFA that checks computations.

Initial "domino"  $I_0(x)$  on bottom

end.

The 2-tape DFA has a valid completion of  $I_0(x) \iff M$  accepts  $x$ , so (this form of) PCP is undecidable.

Emil Post actually had in mind — in 1929! — a machine that acts as a queue and writes the bottom half of an "omino" to the queue and re-runs on the output until the queue empties.

The bottom starts out longer, but the end of the "good housekeeping" routine shortens it one-by-one until they align when the final "q\_acc 1" is reached. The other technical difference from Debray's notes (and almost every other version of the PCP) is that I stacked the state above the scanned char rather than before it. This will come in handy when we simulate computations by Boolean circuits next.

Defn (implicit, not so explicit, in text and Watrous's notes). The Kleene T-predicate  $T(\langle M \rangle, x, \bar{c})$  holds when  $\bar{c}$  is a valid accepting halting computation of  $M$  on input  $x$ .

For any fixed  $M$ , we can build a 2-tape DFA  $M'$  that decides  $T(\langle M \rangle, x, \bar{c})$  in linear time. When  $M$  varies, the time is  $\approx O(|Q_M| \cdot |\bar{c}|)$  but this still counts as time that is polynomial in  $|\langle M \rangle| + |x| + |\bar{c}|$ .

Defn: A language  $A$  belongs to  $\mathcal{P}$  ("polynomial time") if there is a DTM  $M$  such that  $L(M) = A$  and for all  $x$ ,  $M(x)$  halts within  $|x|^{O(1)}$  time. And a number  $k \geq 1$  s.t.  $L(M) = A$  and  $\forall x$ ,  $M(x)$  halts within  $|x|^k + k$  steps.

And  $A$  is in NP (nondet<sup>c</sup> poly time) if  $A = L(N)$  for some NTM  $N$  that runs in  $n^{O(1)}$  time — i.e.  $\exists k \forall x$  all possible  $\bar{c}$  halt within  $|x|^k + k$  steps.

Theorem (often used as the defn of NP): A language  $A$  is in NP  $\Leftrightarrow$  there is a DTM  $V$  such that  $V(x, y)$  runs in  $|x|^{O(1)}$  time and for all  $x$ ,  $x \in A \Leftrightarrow (\exists y) V(x, y)$ .

Proof: Take  $N$  to be an NTM that runs in  $|x|^k + k$  time for some  $k$  and accepts  $A$ . Consider the T-predicate  $T(\langle N \rangle, x, \bar{c})$ . By the defn of running time for  $N$ , all possible accepting computations  $\bar{c}$  have at most  $|x|^k + k$  IDs, and since IDs can grow by at most one char at each step, the total length of  $\bar{c}$  is at most  $(|x|^k + k)^2$ . Hence our poly (linear)-time decider for  $T$  is the required verifier  $V$ .

The 2-tape DFA has a valid completion of  $I_0(x) \Leftrightarrow M$  accepts  $x$ , so (this form of) PCP is undecidable.

Emil Post actually had in mind — in 1929! — a machine that acts as a queue and writes the bottom half of an "omino" to the queue and re-runs on the output until the queue empties.

Theorem (often used as the defn of NP): A language  $A$  is in NP  $\Leftrightarrow$  there is a DTM  $V$  such that  $V(x, y)$  runs in  $|x|^{O(1)}$  time and for all  $x$ ,  $x \in A \Leftrightarrow (\exists y) V(x, y)$ .

Proof: Take  $N$  to be an NTM that runs in  $|x|^k + k$  time for some  $k$  and accepts  $A$ . Consider the T-predicate  $T(\langle N \rangle, x, \bar{c})$ . By the defn of running time for  $N$ , all possible accepting computations  $\bar{c}$  have at most  $|x|^k + k$  IDs, and since IDs can grow by at most one char at each step, the total length of  $\bar{c}$  is at most  $(|x|^k + k)^2$ . Hence our poly (linear)-time decider for  $T$  is the required verifier  $V$ .

The 2-tape DFA has a valid completion of  $I_0(x) \Leftrightarrow M$  accepts  $x$ , so (this form of) PCP is undecidable.

Emil Post actually had in mind — in 1929! — a machine that acts as a queue and writes the bottom half of an "omino" to the queue and re-runs on the output until the queue empties.