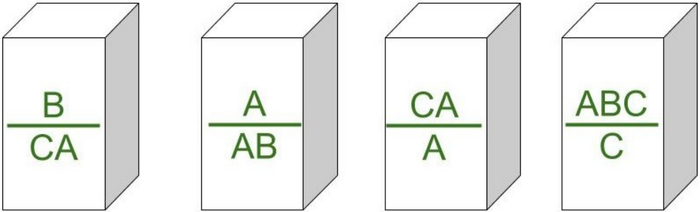
Post's Correspondence Problem (PCP): A reduction by computation history



Textbook: Chapter 5.2

Intro

- Imagine we have some set of dominos, each with a top and bottom section
- We want to arrange them (repetition allowed) so that the top and bottom match when read left to right

$$\left\{ \left[\frac{ab}{a} \right], \left[\frac{c}{bc} \right] \right\}$$

$$\left[\frac{ab}{a} \right] \left[\frac{c}{bc} \right] \rightarrow \frac{abc}{abc}$$

- Some sets of dominos have possible matches, and some don't

For example, this set has no matches:

$$\left\{ \left[\frac{abc}{ab} \right], \left[\frac{ca}{a} \right], \left[\frac{acc}{ba} \right] \right\}$$

Definition

Def. Post's Correspondence Problem. Does a given set of dominos have a possible match?

As a language:

$$PCP = \{w : w \texttt{ encodes a set of dominos which match } \}$$

Undecidability

Thm. *PCP* is undecidable.

Pf. By reduction from the decision problem A_{TM}. We will assume *PCP* is decidable and show that this implies A_{TM} is decidable (a contradiction).

- We can construct an instance of *PCP* which simulates a TM
  - Can design it so it matches iff the TM accepts
- Therefore a *PCP* decider would decide A_{TM}

MPCP

- First let's look at a simpler version: **Modified PCP** (MPCP)
- MPCP is PCP, but matches must begin with the first domino
- Later we will prove MPCP and PCP are equivalent

Def: Modified Post's Correspondence Problem.

$$MPCP = \{w \in PCP : w\texttt{'s match starts w/ the first domino}\}$$

Thm: A_{TM} is reducible to $MPCP$ (a decider for $MPCP$ can be used to decide A_{TM}). Given some TM M and input w, we will construct an instance P' of $MPCP$ which matches iff $M(w)$ accepts by simulating M's accepting computation history.

- Configurations will be delimited by $\#$s

Construction pt. 1

1. The first domino will be the starting configuration

$$\left[\frac{\#}{\# q_0 w_1 w_2 \cdots w_n \#}\right] \in P'$$

Other dominoes will force the next configuration to appear.

2. **Rightward movement:** For every $a, b \in \Gamma$ (the tape alphabet) and $q, r \in Q$ where $q \neq q_{\texttt{reject}}$:
   - **If** $\delta(q, a) = (r, b, R)$ (move from state q on tape cell a to state r, writing b and moving right), **then** add $\left[\frac{qa}{br}\right]$ to P'
3. **Leftward movement:** For every $a, b, c \in \Gamma$ (tape alphabet) and $q, r \in Q$ where $q \neq q_{\texttt{reject}}$:
   - **If** $\delta(q, a) = (r, b, L)$ (move from state q on tape cell a to state r, writing b and moving left) **then** add $\left[\frac{cqa}{rcb}\right]$ to P'

Construction pt. 2

4. **Tape:** For every $a \in \Gamma$, add $\left[\frac{a}{a}\right]$ to P'
5. **Configurations:** Add $\left[\frac{\#}{\#}\right]$ (the configuration deliminator on the top and bottom) and $\left[\frac{\#}{\sqcup\#}\right]$ (where "$\sqcup$" accounts for the infinitely many empty tape cells on the RHS of the configuration) to P'
6. For every $a \in \Gamma$, add to P' the dominoes:

$$\left[\frac{aq_{\mathtt{accept}}}{q_{\mathtt{accept}}}\right], \left[\frac{q_{\mathtt{accept}}\, a}{q_{\mathtt{accept}}}\right]$$

   These allow the acceptance state to "eat" surrounding tape characters until only it remains

7. Finally we add $\left[\frac{q_{\mathtt{accept}}\#\#}{\#}\right]$, allowing the dominoes to finally match

Construction pt. 3

- Clearly A_{TM} is reducible to $MPCP$ P', but can we convert $P' \in MPCP$ to some $P \in PCP$?

"Starring" strings: Let $u = u_1 u_2 \cdots u_n$ be a string of length n. Define $\star u$, $u\star$, and $\star u \star$ as follows.

$$\star u = \star u_1 \star u_2 \cdots \star u_n$$

$$u\star = u_1 \star u_2 \star \cdots u_n \star$$

$$\star u \star = \star u_1 \star u_2 \star \cdots \star u_n \star$$

Construction pt. 4

If P' is the set

$$\left\{ \left[\frac{t_1}{b_1}\right], \left[\frac{t_2}{b_2}\right], \left[\frac{t_3}{b_3}\right], \dots \left[\frac{t_k}{b_k}\right] \right\}$$

Then we let P be the set

$$\left\{ \left[\frac{\star t_1}{\star b_1 \star}\right], \left[\frac{\star t_2}{b_2 \star}\right], \left[\frac{\star t_3}{b_3 \star}\right], \dots \left[\frac{\star t_k}{b_k \star}\right], \left[\frac{\diamond \star}{\diamond}\right] \right\}$$

- $\left[\frac{\diamond \star}{\diamond}\right]$ allows the match to terminate with matching stars
- Thus, *MPCP* can be converted to *PCP*. Since A_{TM} is reducible to *MPCP*, *PCP* is undecidable. End of proof.

Next up: Nondeterministic Turing Machines