CMSC 28100

Introduction to Complexity Theory

Spring 2024
Instructor: William Hoza

Post's Correspondence Problem

- **Given:** a set of "dominos"

$$\boxed{\begin{matrix} t_1 \\ b_1 \end{matrix}} \quad \boxed{\begin{matrix} t_2 \\ b_2 \end{matrix}} \quad \boxed{\begin{matrix} t_3 \\ b_3 \end{matrix}} \quad \cdots \quad \boxed{\begin{matrix} t_k \\ b_k \end{matrix}}$$

- **Goal:** Determine whether it is possible to generate a "match"

$$\boxed{\begin{matrix} t_{i_1} \\ b_{i_1} \end{matrix}}\boxed{\begin{matrix} t_{i_2} \\ b_{i_2} \end{matrix}}\boxed{\begin{matrix} t_{i_3} \\ b_{i_3} \end{matrix}}\boxed{\begin{matrix} t_{i_4} \\ b_{i_4} \end{matrix}}\boxed{\begin{matrix} t_{i_5} \\ b_{i_5} \end{matrix}} \quad \cdots \quad \boxed{\begin{matrix} t_{i_n} \\ b_{i_n} \end{matrix}}$$

in which the sequence of symbols on top equals the sequence of symbols on the bottom

- Using the same domino multiple times is permitted

Post's Correspondence Problem is undecidable

- Define

$$\mathrm{PCP} = \{\langle \Lambda, t_1, \dots, t_k, b_1, \dots, b_k \rangle : \exists i_1, \dots, i_n \text{ such that } t_{i_1} \cdots t_{i_n} = b_{i_1} \cdots b_{i_n}\}$$

Theorem: PCP is undecidable

- Proof outline:
  - Step 1: Show that a modified version ("MPCP") is undecidable by reduction from HALT
  - Step 2: Show that PCP is undecidable by reduction from MPCP

Modified PCP

$$\text{MPCP} = \{\langle \Lambda, t_1, \dots, t_k, b_1, \dots, b_k \rangle : \exists i_1, \dots, i_n \text{ such that } t_1 t_{i_1} \cdots t_{i_n} = b_1 b_{i_1} \cdots b_{i_n}\}$$

- The difference between PCP and MPCP: In MPCP, matches must start with the first domino

Reduction from HALT to MPCP

Reduction is computable ✓

- We produce the following dominos:
- $\left[\frac{\epsilon}{\Diamond q_0 w \sqcup \#}\right]$, $\left[\frac{\#}{\#}\right]$, $\left[\frac{\#}{\sqcup \#}\right]$, $\left[\frac{q_{\text{accept}}\#}{\epsilon}\right]$, and $\left[\frac{q_{\text{reject}}\#}{\epsilon}\right]$
- $\left[\frac{qb}{b'q'}\right]$ for every q, b, q', b' such that $\delta(q,b) = (q', b', \text{R})$ and $q \notin \{q_{\text{accept}}, q_{\text{reject}}\}$
- $\left[\frac{aqb}{q'ab'}\right]$ for every q, b, q', b', a such that $\delta(q,b) = (q', b', \text{L})$ and $q \notin \{q_{\text{accept}}, q_{\text{reject}}\}$
- $\left[\frac{b}{b}\right]$, $\left[\frac{bq}{q}\right]$, and $\left[\frac{qb}{q}\right]$ for every $b \in \Gamma$ and $q \in \{q_{\text{accept}}, q_{\text{reject}}\}$

YES maps to YES

- Suppose M halts on w
- Under this assumption, we showed last time how to construct a match
- The construction was based on the computation history of M on w:

ϵ	$C_0' \sqcup$	$\#$	$C_1' \sqcup$	$\#$	…	$\#$	$C_{T-1}' \sqcup$	$\#$	H_0	$\#$	H_1	$\#$	…	$\#$	H_{n-1}	$\#$	$H_n\#$
$\Diamond q_0 w \sqcup \#$	C_1'	$\sqcup \#$	C_2'	$\sqcup \#$		$\sqcup \#$	C_T'	$\#$	H_1	$\#$	H_2	$\#$		$\#$	H_n	$\#$	ϵ

NO maps to NO

- Suppose M loops on w. Let $C_0, C_1, C_2, \ldots$ be the computation history of M on w (an infinite sequence of configurations)
- Assume, for the sake of contradiction, that there is a match
- We will show by induction that for every $i \in \mathbb{N}$, there exist $k, r \in \mathbb{N}$ and $x \in \Lambda^*$ such that $k \geq i$, there are at least k dominos in the match, and the first k dominos form the following super-domino: $\left[\frac{x}{xC_i \sqcup^r \#}\right]$
- Base case $i = 0$: By definition of MPCP, the match must start with $\left[\frac{\epsilon}{\Diamond q_0 w \sqcup \#}\right]$

NO maps to NO

- Inductive step: Assume that
- Subsequent dominos must s
- Exercise: There are only two possible ways to do this, namely

$\frac{C_i \sqcup^r}{C_{i+1} \sqcup^r}$	followed by either	$\frac{\#}{\#}$	or	$\frac{\#}{\sqcup \#}$

- Either way, the inductive step is complete
- Consequence: The match is infinitely long, a contradiction

When we are computing $f(\langle M, w\rangle)$, how do we know whether there is a match?

A: We simulate M on w and observe what happens

B: We inspect the transition function of M

C: We do not know whether there is a match, and that's okay

D: We do not know whether there is a match, and that's an issue

Respond at PollEv.com/whoza or text "whoza" to 22333

NO maps to NO

- This completes the proof that MPCP is undecidable
  - We designed a mapping reduction from HALT to MPCP
  - If MPCP were decidable, then HALT would be decidable too

Post’s Correspondence Problem is undecidable

- Define

$$\mathrm{PCP} = \{\langle \Sigma, t_1, \ldots, t_k, b_1, \ldots, b_k \rangle : \exists i_1, \ldots, i_n \text{ such that } t_{i_1} \cdots t_{i_n} = b_{i_1} \cdots b_{i_n}\}$$

Theorem: PCP is undecidable

- Proof outline:
  - Step 1: Show that a modified version, “MPCP,” is undecidable by reduction from HALT
  - Step 2: Show that PCP is undecidable by reduction from MPCP

Reduction from MPCP to PCP

- For each string $u = u_1 u_2 \ldots u_n$, define $\overline{u} = u_1 \star u_2 \star \cdots \star u_n$
- Reduction:

$$f\left(\left[\frac{t_1}{b_1}\right] \left[\frac{t_2}{b_2}\right] \left[\frac{t_3}{b_3}\right] \cdots \left[\frac{t_k}{b_k}\right] \right) = \left[\frac{\star\,\overline{t_1}}{\star\,\overline{b_1}\,\star}\right] \left[\frac{\star\,\overline{t_1}}{\overline{b_1}\,\star}\right] \left[\frac{\star\,\overline{t_2}}{\overline{b_2}\,\star}\right] \left[\frac{\star\,\overline{t_3}}{\overline{b_3}\,\star}\right] \cdots \left[\frac{\star\,\overline{t_k}}{\overline{b_k}\,\star}\right] \left[\frac{\star}{\epsilon}\right]$$

- Computable ✓

YES maps to YES

- Suppose the MPCP instance has a match

t_1	t_{i_1}	t_{i_2}	t_{i_3}	t_{i_4}	$\cdots$	t_{i_n}
b_1	b_{i_1}	b_{i_2}	b_{i_3}	b_{i_4}		b_{i_n}

- Then the constructed PCP instance also has a match:

$\star\,\overline{t_1}$	$\star\,\overline{t_{i_1}}$	$\star\,\overline{t_{i_2}}$	$\cdots$	$\star\,\overline{t_{i_n}}$	$\star$
$\star\,\overline{b_1}\,\star$	$\overline{b_{i_1}}\,\star$	$\overline{b_{i_2}}\,\star$		$\overline{b_{i_n}}\,\star$	ϵ

NO maps to NO

- We prove the contrapositive. Suppose the constructed PCP instance has a match
- Must start with $\left[\dfrac{\star\,\overline{t_1}}{\star\,\overline{b_1}\,\star}\right]$ because that's the only domino with the same first symbol on top and on bottom
- Delete all the $\star$ symbols from the match, and we get a match for the original MPCP instance

Using reductions to prove undecidability

- **OBJECTION:** "I don't like mapping reductions. I preferred our first few undecidability proofs, where we did proofs by contradiction and the concept of a reduction was implicit."
- **RESPONSE 1:** Mapping reductions help us to reason clearly about undecidability
- **RESPONSE 2:** You should get comfortable with the concept of a mapping reduction now in preparation for what will come later
- The concept might feel "optional" now, but later it will be essential

The “emptiness p

Given $\langle M, w\rangle$, how would we compute $f(\langle M, w\rangle)$?

A: Simulate M on w, and if it ever halts, accept

B: Simulate M on w and construct $\langle M'\rangle$ based on simulation results

C: Modify the transition function of M to construct $\langle M'\rangle$

D: There does not exist an algorithm that computes f

Respond at PollEv.com/whoza or text “whoza” to 22333

- Let $\mathrm{E_{TM}} = \{\langle M\rangle :$ there do

- **Claim:** $\mathrm{E_{TM}}$ is undecidable

- **Proof:** We will design a mapping reduction from $\overline{\mathrm{HALT}}$ to $\mathrm{E_{TM}}$

- Let $f(\langle M, w\rangle) = \langle M'\rangle$, where M' is a TM that does the following on input x:

  1. Simulate M on w
  2. If M ever halts, accept

- YES maps to YES ✓ NO maps to NO ✓ Computable ✓

Which languages are undecidable?

Some more undecidable problems

- We have seen several interesting examples of undecidable problems
- To wrap up our discussion of undecidability, I’ll mention a few more examples of undecidable problems – but we won’t do the proofs
- (This material will not be on problem sets or exams)

Hilbert's 10$^{\text{th}}$ problem

- Problem: Given a polynomial equation with integer coefficients such as

$$x^2 + 3xz + y^3 + z^2x^2 = 4xy^2 + 6yz + 2,$$

determine whether there is an integer solution

- Let $\mathrm{HILBERT10} = \{\langle p, q \rangle : \exists \vec{x} \ \text{ such that } \ p(\vec{x}) = q(\vec{x})\}$

Theorem: $\mathrm{HILBERT10}$ is undecidable

Derivatives vs. Integrals

- Recall: Calculus
- Computing derivatives is mechanistic
  - Sum rule $(f+g)' = f' + g'$, product rule $(fg)' = f'g + fg'$, chain rule $(f \circ g)' = (f' \circ g) \cdot g'$, etc.
- In contrast, computing integrals seems to involve creativity
  - u-substitutions, integration by parts, etc.

Elementary functions

- Definition: A function $f : \mathbb{R} \to \mathbb{R}$ is elementary if it can be defined by a formula using addition, multiplication, rational constants, powers, exponentials, logarithms, trigonometric functions, and π
- E.g. $f(x) = x \cdot \sin(x^4) - 3\pi \cdot e^{e^{\sqrt{x}}}$

Integration is undecidable

- Fact: There exist elementary functions that do not have elementary antiderivatives, such as $f(x) = e^{-x^2}$
- Let $\text{INTEGRABLE} = \{\langle f \rangle : f \text{ is an elementary function with an elementary antiderivative}\}$

Theorem: INTEGRABLE is undecidable