Exercise Sheet 6: Diagonalisation

David Carral

December 11, 2019

Exercise 1

Find the fault in the following proof of $\mathrm{P} \neq \mathrm{NP}$.

1. Suppose for a contradiction that $\mathrm{P} = \mathrm{NP}$.
2. By (1): since **SAT** $\in \mathrm{NP}$, we have that **SAT** $\in \mathrm{P}$.
3. By (2): there is some $k \in \mathbb{N}$ with **SAT** $\in \mathrm{DT{\scriptsize IME}}(n^k)$.
4. Since **SAT** is NP-hard, we have that $\mathbf{L} \leq_p$ **SAT** for every language $\mathbf{L} \in \mathrm{NP}$.
5. By (3) and (4): $\mathrm{NP} \subseteq \mathrm{DT{\scriptsize IME}}(n^k)$.
6. By (1) and (5): $\mathrm{P} \subseteq \mathrm{DT{\scriptsize IME}}(n^k)$.
7. By the Time Hierarchy Theorem, we have that $\mathrm{DT{\scriptsize IME}}(n^k) \subset \mathrm{DT{\scriptsize IME}}(n^{k+1})$.
8. Conclusions (6) and (7) result in a contradiction. Hence, $\mathrm{P} \neq \mathrm{NP}$.

Solution. In the previous argument, we cannot conclude (5) from (3) and (4).

a. By the Time Hierarchy Theorem, there is some $\mathbf{A} \in \mathrm{DT{\scriptsize IME}}(n^{k+1}) \setminus \mathrm{DT{\scriptsize IME}}(n^k)$.

b. By (a): $\mathbf{A} \in \mathrm{P} \subseteq \mathrm{NP}$ and hence, $\mathbf{A} \leq_p$ **SAT**.

Exercise 2

Show the following.

1. $\textsc{Time}(2^n) = \textsc{Time}(2^{n+1})$
2. $\textsc{Time}_*(2^n) \subset \textsc{Time}_*(2^{2n})$
3. $\textsc{NTime}(n) \subset \textsc{PSpace}$

Exercise 2

Definition 5.7: Let $f : \mathbb{N} \to \mathbb{R}^+$ be a function.

(1) DTime($f(n)$) is the class of all languages **L** for which there is an $O(f(n))$-time bounded Turing machine deciding **L**.

(2) DSpace($f(n)$) is the class of all languages **L** for which there is an $O(f(n))$-space bounded Turing machine deciding **L**.

Notation 5.8: Sometimes Time($f(n)$) is used instead of DTime($f(n)$).

Solution 1. We show that $\textsc{Time}(2^n) = \textsc{Time}(2^{n+1})$.

1. Since $2^n \in O(2^{n+1})$, we have that $\mathbf{L} \in O(2^{n+1})$ for all $\mathbf{L} \in O(2^n)$.
2. Since $2^{n+1} \in O(2^n)$, we have that $\mathbf{L} \in O(2^n)$ for all $\mathbf{L} \in O(2^{n+1})$.
    - Definition. $g \in O(f)$ iff there are some $k, x_0 \geq 0$ with $g(x) \leq k \cdot f(x)$ for all $x \leq x_0$.
    - $2^{x+1} \leq k \cdot 2^x$ for all $x \geq x_0$ with (e.g.) $k = 2$ and $x_0 = 0$.

Exercise 2

Example 12.2: We will use, e.g., the following resources:

- DTime time used by a deterministic 1-tape TM
- DTime$_k$ time used by a deterministic k-tape TM
- DTime$_*$ time used by a deterministic TM with any number of tapes

Solution 2. We show that $\mathrm{TIME}_*(2^n) \subset \mathrm{TIME}_*(2^{2n})$.

1. Time Hierarchy Theorem. If $f, g : \mathbb{N} \to \mathbb{N}$ are such that f is time-constructible and $g \cdot \log g \in o(f)$, then $\mathrm{DTIME}_*(g) \subset \mathrm{DTIME}_*(f)$.
2. Definition. $g \in o(f)$ iff, for all $\varepsilon \geq 0$, there is some $x_0 \geq 0$ such that $g(x) \leq \varepsilon \cdot f(x)$ for all $x \geq x_0$. Note that possibly $\varepsilon < 1$.
3. We have that $2^n \cdot \log(2^n) \in o(2^{2n})$ since, for all $\varepsilon \geq 0$, there is some $x_0 \geq 0$ such that $2^x \cdot x \leq \varepsilon \cdot 2^{2x}$ for all $x \geq x_0$. Note that $\frac{2^x \cdot x}{2^x} = x$ and $\frac{\varepsilon \cdot 2^{2x}}{2^x} = \varepsilon \cdot 2^x$.
4. By (1) and (3), $\mathrm{DTIME}_*(2^n) \subset \mathrm{DTIME}_*(2^{2n})$.

Exercise 2

(1) NTime($f(n)$) is the class of all languages **L** for which there is an $O(f(n))$-time bounded nondeterministic Turing machine deciding **L**.

(2) DSpace($f(n)$) is the class of all languages **L** for which there is an $O(f(n))$-space bounded Turing machine deciding **L**.

Solution 3. We show that $\mathrm{NTime}(n) \subset \mathrm{PSpace}$.

1. $\mathrm{NTime}(n) \subseteq \mathrm{NSpace}(n)$ because any TM that operates in time n on every computation branch can use at most n tape cells on every branch.
2. By Savitch's Theorem: $\mathrm{NSpace}(n) \subseteq \mathrm{Space}(n^2)$.
3. Space Hierarchy Theorem. If $f, g : \mathbb{N} \to \mathbb{N}$ such that f is space-constructible and $g \in o(f)$, then $\mathrm{DSpace}(g) \subset \mathrm{DSpace}(f)$.
4. By (3): $\mathrm{Space}(n^2) \subset \mathrm{Space}(n^3)$. Note that $n^2 \in o(n^3)$.
5. By (1), (2), (4), and $\mathrm{Space}(n^3) \subseteq \mathrm{PSpace}$: $\mathrm{NTime}(n) \subset \mathrm{PSpace}$.

Exercise 3

Show that there exists a function that is not time-constructible.

Definition 12.5: A function $t : \mathbb{N} \to \mathbb{N}$ is time-constructible if $t(n) \geq n$ for all n and there exists a TM that computes $t(n)$ in unary in time $O(t(n))$.

A function $s : \mathbb{N} \to \mathbb{N}$ is space-constructible if $s(n) \geq \log n$ and there exists a TM that computes $s(n)$ in unary in space $O(s(n))$.

Solution. The proof of the Gap Theorem explicitly constructs one.

Gaps in Time

We consider an (effectively computable) enumeration of all Turing machines:

$$\mathcal{M}_0, \mathcal{M}_1, \mathcal{M}_2, \ldots$$

Definition 13.6: For arbitrary numbers $i, a, b \in \mathbb{N}$ with $a \leq b$, we say that $\mathsf{Gap}_i(a, b)$ is true if:

- Given any TM $\mathcal{M}_j$ with $0 \leq j \leq i$,
- and any input string w for $\mathcal{M}_j$ of length $|w| = i$,

$\mathcal{M}_j$ on input w will halt in less than a steps, in more than b steps, or not at all.

Lemma 13.7: Given $i, a, b \geq 0$ with $a \leq b$, it is decidable if $\mathsf{Gap}_i(a, b)$ holds.

Proof: We just need to ensure that none of the finitely many TMs $\mathcal{M}_0, \ldots, \mathcal{M}_i$ will halt after a to b steps on any of the finitely many inputs of length i. This can be checked by simulating TM runs for at most b steps. $\square$

Find the Gap

We can now define the value $f(n)$ of f for some $n \geq 0$:

Let $\text{in}(n)$ denote the number of runs of TMs $\mathcal{M}_0, \ldots, \mathcal{M}_n$ on words of length n, i.e.,

$$\text{in}(n) = |\Sigma_0|^n + \cdots + |\Sigma_n|^n \qquad \text{where } \Sigma_i \text{ is the input alphabet of } \mathcal{M}_i$$

We recursively define a series of numbers $k_0, k_1, k_2, \ldots$ by setting $k_0 = 2n$ and $k_{i+1} = 2^{k_i}$ for $i \geq 0$, and we consider the following list of intervals:

$$\begin{array}{cccc}
[k_0 + 1, k_1], & [k_1 + 1, k_2], & \cdots, & [k_{\text{in}(n)} + 1, k_{\text{in}(n)+1}] \\
\parallel & \parallel & & \parallel \\
[2n + 1, 2^{2n}], & [2^{2n} + 1, 2^{2^{2n}}], & \cdots, & [2^{\cdot^{\cdot^{2n}}} + 1, 2^{2^{\cdot^{\cdot^{2n}}}}]
\end{array}$$

Let $f(n)$ be the least number k_i with $0 \leq i \leq \text{in}(n)$ such that $\text{Gap}_n(k_i + 1, k_{i+1})$ is true.

Exercise 4

Consider the function $\text{pad}\colon \Sigma^* \times \mathbb{N} \to \Sigma^*\#^*$ defined as $\text{pad}(s, \ell) = s\#^j$, where $j = \max(0, \ell - |s|)$. In other words, $\text{pad}(s, \ell)$ adds enough copies of a fresh symbol $\#$ to the end of s so that the length is at least ℓ.

Examples.

- $\text{pad}(01011, 8) = 01011\#\#\#$
- $\text{pad}(01011, 12) = 01011\#\#\#\#\#\#\#$
- $\text{pad}(01011, 3) = 01011$

For a language $\mathbf{A} \subseteq \Sigma^*$ and a function $f\colon \mathbb{N} \to \mathbb{N}$, let

$$\text{pad}(\mathbf{A}, f) = \{\, \text{pad}(s, f(|s|)) \mid s \in \mathbf{A} \,\}.$$

Exercise 4

Let pad: $\Sigma^* \times \mathbb{N} \to \Sigma^* \#^*$ be defined as $\text{pad}(s, \ell) = s\#^j$, where $j = \max(0, \ell - |s|)$.
For $\mathbf{A} \subseteq \Sigma^*$ and $f : \mathbb{N} \to \mathbb{N}$, let $\text{pad}(\mathbf{A}, f) = \{ \text{pad}(s, f(|s|)) \mid s \in \mathbf{A} \}$.

Solution 1. We show that, if $\mathbf{A} \in \text{DTIME}(n^6)$, then $\text{pad}(\mathbf{A}, n^2) \in \text{DTIME}(n^3)$.

1. Let $\mathcal{M}$ be a DTM deciding $\mathbf{A}$ in $O(n^6)$ time.
2. Let $\mathcal{M}'$ be the TM that, on input w, performs the following computation:
   2.1 *Reject* if w is not of the form $w = s\#^\ell$ with $|w| = |s|^2$.
   2.2 Simulate $\mathcal{M}$ on input s and return the result of the simulation.
3. The check in (2.1) can be done in linear time using a 3-tape TM (discuss). Hence, it can be done in $O(n^2)$ with a single tape TM.
4. Simulating $\mathcal{M}$ on s is $O(|s|^6) = O(|w|^3) = O(n^3)$.
5. $\mathcal{M}'$ runs in $O(n^3)$.
6. $\mathcal{M}'$ accepts $s\#^\ell$ iff $|s| = \sqrt{|s\#^\ell|}$ and $s \in \mathbf{A}$. That is, $\mathcal{L}(\mathcal{M}') = \text{pad}(\mathbf{A}, n^2)$.

Remarks:

- The choice of the particular numbers 2, 3, and 6 is arbitrary.
- We could make an analogous argument for space instead of time.
- The converse is also true.

Exercise 4

Let $\mathrm{pad}\colon \Sigma^* \times \mathbb{N} \to \Sigma^*\#^*$ be defined as $\mathrm{pad}(s, \ell) = s\#^j$, where $j = \max(0, \ell - |s|)$.
For $\mathbf{A} \subseteq \Sigma^*$ and $f\colon \mathbb{N} \to \mathbb{N}$, let $\mathrm{pad}(\mathbf{A}, f) = \{\, \mathrm{pad}(s, f(|s|)) \mid s \in \mathbf{A} \,\}$.

Solution 2. We show that if $\mathrm{NE}\textsc{xp}\mathrm{T}\textsc{ime} \neq \mathrm{E}\textsc{xp}\mathrm{T}\textsc{ime}$, then $\mathrm{P} \neq \mathrm{NP}$.

$$
\begin{aligned}
\mathbf{A} \in \mathrm{DT}\textsc{ime}(2^{n^d}) &\implies \mathrm{pad}(\mathbf{A}, 2^{n^d}) \in \mathrm{P}, \\
\mathrm{pad}(\mathbf{A}, 2^{n^d}) \in \mathrm{DT}\textsc{ime}(n^k) &\implies \mathbf{A} \in \mathrm{E}\textsc{xp}\mathrm{T}\textsc{ime}
\end{aligned}
$$

for all $k, d \in \mathbb{N}$. This also holds true for $\mathrm{NT}\textsc{ime}$ instead of $\mathrm{DT}\textsc{ime}$.

Then, assuming $\mathrm{P} = \mathrm{NP}$, we can infer

$$
\begin{aligned}
\mathbf{A} \in \mathrm{NE}\textsc{xp}\mathrm{T}\textsc{ime} &\implies \mathbf{A} \in \mathrm{NT}\textsc{ime}(2^{n^d}) \text{ for some } d \in \mathbb{N} \\
&\implies \mathrm{pad}(\mathbf{A}, 2^{n^d}) \in \mathrm{NP} \text{ for some } d \in \mathbb{N} \\
&\implies \mathrm{pad}(\mathbf{A}, 2^{n^d}) \in \mathrm{P} \text{ for some } d \in \mathbb{N} \\
&\implies \mathrm{pad}(\mathbf{A}, 2^{n^d}) \in \mathrm{DT}\textsc{ime}(n^k) \text{ for some } d, k \in \mathbb{N} \\
&\implies \mathbf{A} \in \mathrm{E}\textsc{xp}\mathrm{T}\textsc{ime}
\end{aligned}
$$

Exercise 4

Let $\text{pad}\colon \Sigma^* \times \mathbb{N} \to \Sigma^*\#^*$ be defined as $\text{pad}(s, \ell) = s\#^j$, where $j = \max(0, \ell - |s|)$.
For $\mathbf{A} \subseteq \Sigma^*$ and $f\colon \mathbb{N} \to \mathbb{N}$, let $\text{pad}(\mathbf{A}, f) = \{\, \text{pad}(s, f(|s|)) \mid s \in \mathbf{A} \,\}$.

Solution 3. We show that, for every $\mathbf{A} \subseteq \Sigma^*$ and $k \in \mathbb{N}$, $\mathbf{A} \in \mathrm{P}$ iff $\text{pad}(\mathbf{A}, n^k) \in \mathrm{P}$.

- $\mathbf{A} \in \mathrm{P}$ implies $\text{pad}(\mathbf{A}, n^k) \in \mathrm{P}$.
  1. Let $\mathbf{A} \subseteq \Sigma^*$ and $k \in \mathbb{N}$.
  2. If $\mathbf{A} \in \mathrm{P}$, then $\mathbf{A} \in \mathrm{DTIME}(n^\ell)$ for some $\ell \in \mathbb{N}$.
  3. $\text{pad}(\mathbf{A}, n^k) \in \mathrm{DTIME}(n^{\lceil \ell/k \rceil}) \subseteq \mathrm{P}$ (analogous argument to the one from part 1).
- $\text{pad}(\mathbf{A}, n^k) \in \mathrm{P}$ implies $\mathbf{A} \in \mathrm{P}$.
  1. If $\text{pad}(\mathbf{A}, n^k) \in \mathrm{P}$, then $\text{pad}(\mathbf{A}, n^k) \in \mathrm{DTIME}(n^\ell)$ for some $\ell \in \mathbb{N}$.
  2. Therefore, $\mathbf{A} \in \mathrm{DTIME}(n^{\ell \cdot k}) \subseteq \mathrm{P}$.

Exercise 4

Let $\text{pad}\colon \Sigma^* \times \mathbb{N} \to \Sigma^*\#^*$ be defined as $\text{pad}(s, \ell) = s\#^j$, where $j = \max(0, \ell - |s|)$.
For $\mathbf{A} \subseteq \Sigma^*$ and $f\colon \mathbb{N} \to \mathbb{N}$, let $\text{pad}(\mathbf{A}, f) = \{\, \text{pad}(s, f(|s|)) \mid s \in \mathbf{A} \,\}$.

Solution 4. We show that $\mathrm{P} \neq \mathrm{DS{\scriptsize PACE}}(n)$.

1. Assume $\mathrm{P} = \mathrm{DS{\scriptsize PACE}}(n)$.
2. By the space hierarchy theorem: There is some language $\mathbf{A} \in \mathrm{DS{\scriptsize PACE}}(n^2) \setminus \mathrm{DS{\scriptsize PACE}}(n)$.
3. $\text{pad}(\mathbf{A}, n^2) \in \mathrm{DS{\scriptsize PACE}}(n)$.
4. $\text{pad}(\mathbf{A}, n^2) \in \mathrm{P}$.
5. $\mathbf{A} \in \mathrm{P}$.
6. $\mathbf{A} \in \mathrm{DS{\scriptsize PACE}}(n)$.

Exercise 4

Let $\mathrm{pad}\colon \Sigma^* \times \mathbb{N} \to \Sigma^*\#^*$ be defined as $\mathrm{pad}(s, \ell) = s\#^j$, where $j = \max(0, \ell - |s|)$. For $\mathbf{A} \subseteq \Sigma^*$ and $f\colon \mathbb{N} \to \mathbb{N}$, let $\mathrm{pad}(\mathbf{A}, f) = \{\, \mathrm{pad}(s, f(|s|)) \mid s \in \mathbf{A} \,\}$.

Solution 5. We show that $\mathrm{NP} \neq \mathrm{DS}\textsc{pace}(n)$.

1. We can make a similar argument to the one from (3) to show the following: for every $\mathbf{A} \subseteq \Sigma^*$ and $k \in \mathbb{N}$, we have that $\mathbf{A} \in \mathrm{NP}$ iff $\mathrm{pad}(\mathbf{A}, n^k) \in \mathrm{NP}$.
2. Then, make a similar argument to the one from (4) to show $\mathrm{NP} \neq \mathrm{DS}\textsc{pace}(n)$.

Exercise 5

You are given two oracles and one of them is the set **TQBF**, but you do not know which one. Design a polynomial algorithm that decides **TQBF** using these oracles.

- Given a QBF formula $\phi = \exists y_1 \forall y_2 \ldots \exists y_{m-1} \forall y_m . \psi(y_1, \ldots, y_m)$
- Query ϕ with both oracles. *Accept* ϕ if both answer "true", *reject* ϕ if both answer "false", and otherwise play a game with two players: the $\exists$-player, that uses the accepting oracle, and the $\forall$-player, that uses the rejecting oracle.
- The $\exists$-player plays in turns $i \in \{1, 3, \ldots, m-1\}$ of the game. This player asks his oracle both for $b = 0$ and $b = 1$ whether the formula $\exists y_i \forall y_{i+1} \ldots Q_m y_m . \psi(x_1, \ldots, x_{i-1}, b, y_{i+1}, \ldots, y_m)$ is true or false. If both values are "false" then *reject* ϕ (the oracle is acting inconsistently). Otherwise, let $x_i = b$ for a value b for which the answer was "true".
- The $\forall$-player plays in turns $i \in \{2, 4, \ldots, m\}$ of the game. This player asks his oracle both for $b = 0$ and $b = 1$ whether the formula $\forall y_i \exists y_{i+1} \ldots Q_m y_m . \psi(x_1, \ldots, x_{i-1}, b, y_{i+1}, \ldots, y_m)$ is true or false. If both values are "true" then *accept* ϕ (the oracle is acting inconsistently). Otherwise, let $x_i = b$ for a value b for which the answer was "false".
- *Accept* ϕ iff $\psi(x_1, \ldots, x_m)$ evaluates to true (no need to use any oracles here!).