Misc

What's a reduction?
Tapes,
NTIME, NEXP,
Padding,
PH
What is a reduction from A to B? It's the concept that if you can do B, then you can also do A.

For example, buying a house reduces to becoming millionaire;

seeing the Colosseum reduces to flying to Rome.
• **Def1:** (What we gave) A reduces to B as $B \in P \implies A \in P$

• In the proofs we have seen the key of this was exhibiting a polynomial-time map: $R : \forall x, \ x \in A \leftrightarrow R(x) \in B$

• **Def2:** A reduction from A to B is R as above.

• **Claim:** Def2 $\implies$ Def1.

• **Problem with Def2:** only captures very specific way to show that $B \in P \implies A \in P$.

For example, (computing satisfying assignments) reduces to 3SAT? Holds for Def1 but not known for Def 2.
Tapes
• So far, 1-tape TM

• Def.: A $k$-tape TM is a TM with $k$ tapes. We are only concerned with $k = O(1)$. Each tape has its own head moving independently.

$$\delta : Q \times \Gamma^k \rightarrow Q \times \Gamma^k \times \{L,R\}^k$$
• $L := \{x : x \in \{0,1\}^* : x = x^R\}$ Palindromes

• Fact: $L$ not in 1-tape $TIME(o(n^2))$

• Fact: $L \in TIME(O(n))$ on 2-tape.

• Proof:

  ?
• $L := \{ x : x \in \{0,1\}^* : x = x^R \}$ Palindromes

• Fact: $L$ not in 1-tape $\text{TIME}(o(n^2))$

• Fact: $L \in \text{TIME}(O(n))$ on 2-tape.

• Proof:

  Copy input on second tape.
  Bring head on 1st tape at the beginning.
  Bring head on 2nd tape at the end.

  Compare symbol-by-symbol moving 1st head forward and 2nd backward.
• Although P on your laptop and P on TM is the same, for running time n, $n^2$, etc. not even k-tape is an adequate model of your laptop

What's missing?
• Although P on your laptop and P on TM is the same, for running time $n$, $n^2$, etc. not even k-tape is an adequate model of your laptop.

  What's missing?

  The ability to jump quickly to a memory location.

• Def.: A random-access TM (RATM) is a k-tape machine where each tape has an associated indexing tape. In one time step TM may move i-th head to the cell indexed by the indexing tape, in binary.

• This models well your laptop up to polylog factors.
• $L := \{ (i,x) : \text{the i-th bit of } x \text{ is 1} \}$

• $L$ requires 1-tape time?

(Think of an expression in terms of $|i|$)
• \( L := \{ (i,x) : \text{the } i\text{-th bit of } x \text{ is } 1 \} \)

• \( L \) requires 1-tape time \( \Omega(2^{|i|}) \)

• \( L \) can be decided on a RATM in time \( ? \)
• L := \{ (i,x) : the i-th bit of x is 1 \}

• L requires 1-tape time \( \Omega(2^{|i|}) \)

• L can be decided on a RATM in time \( O(|i|) \)
Exercise:

Argue in no more than 10 lines that

polynomial-time on TM
= polynomial-time on k-tape TM
= polynomial-time on RATM
Next: non-determinism
Non-deterministic TM: $\delta$ maps to subset of $Q \times \Gamma \times \{L,R\}$

Accept if there is a computation path that leads to accept.

Def1: $\text{NTIME}(t(n)) = \{ L : L \text{ is decided by a non-deterministic TM that runs in time } \leq t(n) \}$

Def2: $\text{NTIME}(t(n)) = \{ L : \exists M : \forall x \text{ of length } n \ x \in L \iff \exists y, |y| \leq t(n), \ M(x,y) \text{ accepts in } \leq t(n) \}$

● Exercise: Prove the two definitions are equivalent (feel free to use multiple tapes, if that helps)
Def: $\text{NEXP} := \text{NTIME}(2^{\text{poly}(n)})$

Theorem: $P=NP \Rightarrow \text{EXP} = \text{NEXP}$

Proof: Example of padding technique

Let $L \in \text{NTIME}(T(n))$ where $m = 2^{n^c}$.

Let $L' := \{ (x,0^{T(n)}) : x \in L, |x| = n \}$

Note $L' \in \text{NTIME}(\ ?)$
● Def: $\text{NEXP} := \text{NTIME}(2^{\text{poly}(n)})$

● Theorem: $\text{P=NP} \implies \text{EXP} = \text{NEXP}$

● Proof: Example of padding technique

Let $L \in \text{NTIME}(T(n))$ where $m = 2^{/(n^c)}$.

Let $L' := \{(x,0^{T(n)}) : x \in L, |x| = n\}$

Note $L' \in \text{NTIME}(O(n)) \subseteq \text{P}$. So let $M$ solve $L'$ in poly time.

$\text{EXP}$ algorithm for $L$:
$M' := \text{“On input } x; \text{ “}$
Def: \( \text{NEXP} := \text{NTIME}(2^{\text{poly}(n)}) \)

Theorem: \( \text{P} = \text{NP} \implies \text{EXP} = \text{NEXP} \)

Proof: Example of padding technique

Let \( L \in \text{NTIME}(T(n)) \) where \( m = 2^{n^c} \).

Let \( L' := \{ (x,0^{T(n)}) : x \in L, |x| = n \} \)

Note \( L' \in \text{NTIME}(O(n)) \subseteq \text{P} \). So let \( M \) solve \( L' \) in poly time.

\text{EXP} \ algorithm for \( L \):
\[ M' := \text{"On input } x; \text{ Replace } x \text{ with } (x,0^{T(n)}); \text{ Run } M." \]

\( M'(x) = M(x,0^{T(n)}) = \text{accept } \iff x \in L \)

\( M' \) runs in time \( O(T(n)) + \text{poly}(T(n)) \).
• Padding:

Equivalences propagate “upward”

Intuition: if you have an equivalence between resources, then when you have even more of those resources the equivalence will continue to hold

Contrapositive of padding

Differences propagate “downward”

EXP $\neq$ NEXP $\Rightarrow$ P $\neq$ NP
Given formula $\varphi$:

- $\text{NP} = \sum_1 P = \exists y : M(x,y) = 1$
- $\text{co-NP} = \prod_1 P = \forall y : M(x,y) = 1$
- $\sum_2 P = \exists y \forall z : M(x,y,z) = 1$
- $\prod_2 P = \forall y \exists z : M(x,y,z) = 1$
- $\sum_3 P = \exists y \forall z \exists w : M(x,y,z,w) = 1$
- etc.

**Def:**

$\sum_i P = \{ L : \exists \text{ poly-time } M, \text{ polynomial } q(n) :$

- $x \in L \iff \exists y_1 \in \{0,1\}^{q(n)} \forall y_2 \in \{0,1\}^{q(n)} \ldots \forall y_{i+1} \in \{0,1\}^{q(n)}$

- $M(x,y_1,y_2,\ldots,y_{i+1}) = 1\}$

Polynomial-time hierarchy $\text{PH} := U_c \sum_c P = U_c \prod_c P$
Theorem: $P = NP \implies P = PH$

Proof:
Theorem: $P = NP \implies P = PH$

Proof: We prove by induction on $i$ that $\sum_i P \cup \prod_i P \subseteq P$

W.l.o.g. let $L \in \sum_{i+1} P$, so $\exists$ poly-time $M$, polynomial $q(n)$:

$x \in L \iff \exists y_1 \in \{0,1\}^{q(n)} \forall y_2 \in \{0,1\}^{q(n)} \ldots Q y_{i+1} \in \{0,1\}^{q(n)}$

$M(x, y_1, y_2, \ldots, y_{i+1}) = 1$

Consider $L' := \{ (x, y_1) : \forall y_2 \in \{0,1\}^{q(n)} \ldots Q y_{i+1} \in \{0,1\}^{q(n)}$

$M(x, y_1, y_2, \ldots, y_{i+1}) = 1 \}$

$L' \in \ ?$
Theorem: \( P = NP \implies P = PH \)

Proof: We prove by induction on \( i \) that \( \sum_i P \cup \prod_i P \subseteq P \)

W.l.o.g. let \( L \in \sum_{i+1} P \), so \( \exists \) poly-time \( M \), polynomial \( q(n) \):
\[ x \in L \iff \exists y_1 \in \{0,1\}^{q(n)} \forall y_2 \in \{0,1\}^{q(n)} \ldots Q y_{i+1} \in \{0,1\}^{q(n)} \]
\[ M(x, y_1, y_2, \ldots, y_{i+1}) = 1 \]

Consider \( L' := \{(x, y_1) : \forall y_2 \in \{0,1\}^{q(n)} \ldots Q y_{i+1} \in \{0,1\}^{q(n)} \]
\[ M(x, y_1, y_2, \ldots, y_{i+1}) = 1 \} \)

\( L' \in \prod_i P \subseteq P \). Let poly-time machine \( M' \) solve \( L' \).

So \( x \in L \iff \exists y_1 \in \{0,1\}^{q(n)} : M'(x, y_1) = 1 \)

And so \( L \in ? \)
Theorem: $P = NP \rightarrow P = PH$

Proof: We prove by induction on $i$ that $\sum_i P \cup \prod_i P \subseteq P$

W.l.o.g. let $L \in \sum_{i+1} P$, so $\exists$ poly-time $M$, polynomial $q(n)$:

$$x \in L \iff \exists y_1 \in \{0,1\}^{q(n)} \forall y_2 \in \{0,1\}^{q(n)} ... Q y_{i+1} \in \{0,1\}^{q(n)} M(x, y_1, y_2, ..., y_{i+1}) = 1$$

Consider $L' := \{(x, y_1) : \forall y_2 \in \{0,1\}^{q(n)} ... Q y_{i+1} \in \{0,1\}^{q(n)} M(x, y_1, y_2, ..., y_{i+1}) = 1 \}$

$L' \in \prod_i P \subseteq P$. Let poly-time machine $M'$ solve $L'$.

So $x \in L \iff \exists y_1 \in \{0,1\}^{q(n)} : M'(x, y_1) = 1$

And so $L \in NP \rightarrow L \in P$
Exercise:

$\prod_2 P \subseteq \sum_2 P \rightarrow PH = \sum_2 P$

Terminology: “The polynomial-time hierarchy collapses” means $\exists c : PH = \sum_c P$. 