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 $B \in P \Rightarrow A \in P$

- 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 $\Rightarrow$ Def1.

- Problem with Def2: only captures very specific way to show that $B \in P \Rightarrow A \in P$.

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

  $\delta : Q \times \Gamma^k \to Q \times \Gamma^k \times \{L,R\}^k$

- $L := \{x : x \in \{0,1\}^* : x = x^R \}$ 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 TIME($o(n^2)$)

- Fact: $L \in$ 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. $\blacksquare$

- 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.

- $L := \{ (i,x) : \text{the } i\text{-th bit of } x \text{ is } 1 \}$

- L requires 1-tape time ?

(Think of an expression in terms of $|i|$)

- 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 ?

- 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: δ maps to subset of $Q \times \Gamma \times \{L,R\}$

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

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

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

- Exercise: Prove the two definitions are equivalent

(feel free to use multiple tapes, if that helps)

- Def: NEXP := $\mathrm{NTIME}(2^{\mathrm{poly}(n)})$

- Theorem: P=NP ➔ EXP = NEXP

- Proof: Example of padding technique

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

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

Note $L' \in \mathrm{NTIME}(?$

- Def: NEXP := NTIME($2^{poly(n)}$)

- Theorem: P=NP ➔ EXP = NEXP

- Proof: Example of padding technique

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

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

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

EXP algorithm for L:
M' := “On input x; ?

- Def: NEXP := NTIME($2^{poly(n)}$)
- Theorem: P=NP ➔ EXP = NEXP
- Proof: Example of padding technique

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

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

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

EXP algorithm for L:

M' := "On input x; Replace x with $(x,0^{T(n)})$; Run M."

M'(x) = M$(x,0^{T(n)})$ = accept ←→ x $\in$ L

M' runs in time O(T(n)) + 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 ≠ NEXP ➔ P ≠ NP

Complete problem
Given formula φ:

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

- Def:

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

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

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

Polynomial-time hierarchy PH := $U_c \sum_c P = U_c \prod_c P$

Theorem: $P = NP \Rightarrow P = PH$

Proof:

Theorem: P = NP $\Rightarrow$ P = PH

Proof: We prove by induction on i that Σ_i P U Π_i P $\subseteq$ P

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

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

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

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: $P = NP \Rightarrow P = PH$

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) :

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

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

And so $L \in$?

Theorem: P = NP $\Rightarrow$ P = PH

Proof: We prove by induction on i that $\Sigma_i P \cup \Pi_i P \subseteq P$

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

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

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

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

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

And so $L \in NP \Rightarrow L \in P$ ■

Exercise:

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

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