Last time:
- resource bounds: time & space complexity, linear speedups / compression
- $P = \bigcup_{k \geq 1} TIME(n^k)$, $PSPACE = \bigcup_{k \geq 1} SPACE(n^k)$
- nondeterminism; $NP = \bigcup_{k \geq 1} NTIME(n^k)$
- Verifiers; $NP = \{L : L \text{ has poly-time verifier}\}$

see web page: ch. 3, 7 Sipser

Today:
- more on NP
- co-classes, e.g. coNP
- Reductions, completeness, NPC, Cook-Levin, favorite NPC problems
- (hopefully) Ladner's Thm: $P \neq NP \Rightarrow \exists$ "NP-intermediate" languages.

Readings: Sipser 7.4, 7.5; AB 2.2–2.4; Pap. 8, 9

Questions?

$P \approx$ decision, given x

$NP \approx$ verific. that $x \in L$, given "help" w
↳ "existential" crit.

Ex:
- $SAT = \{\varphi : \varphi(x_1, \ldots, x_n)$ is a satisfiable Bool. formula $\}$ (0/1)

$\varphi(x) = (x_1 \wedge x_3) \vee (\bar{x}_2 \vee (x_3 \wedge x_7) \wedge \bar{x}_4) \wedge \ldots$

In NP: V takes as input (φ, w)
w an asst in $\{0,1\}^*$

to vars.,

V checks that $\varphi(w) = 1$.

- CLIQUE = $\{(G, k) : G$ is undir. graph cont.^{a} k-clique$\}$

- HAM-PATH = $\{G : G$ has a Ham path$\}$

- GISO = $\{(G_1, G_2) : G_1 \neq G_2$ are isomorphic$\}$

- SHORT-PF = $\{(\varphi, 1^{n}) : \varphi$ is a thm that has a pf of length $\leq n\}$.

(length)

↑ in NP!

P = NP ?	Don't know.

Other nondet. classes:

NL = NLOGSPACE

NPSPACE = Nondet poly space.

$NEXP = \bigcup_{k \geq 1} NTIME(2^{n^k})$

etc.

Co-classes: for $L \subseteq \Sigma^*$, $\overline{L} := \Sigma^* \setminus L$

$\overline{\text{CNF-SAT}} = \{\varphi : \varphi$ is an unsatisfiable CNF formulas$\} \in$ coNP.

For $\mathcal{C}$ a complexity class, $\overline{\mathcal{C}} = \{\overline{L} : L \in \mathcal{C}\}$.

e.g. TAUT $= \{\varphi : \varphi$ is a Boolean tautology, i.e. $\varphi(x) = 1 \ \forall x\}$

TAUT $\in$ coNP.

If $\mathcal{C}$ is a det. class (P, PSPACE, etc): co-$\mathcal{C} = \mathcal{C}$.

NP = co-NP ? Seems no...

Thm: If NP $\neq$ co-NP, P $\neq$ NP.

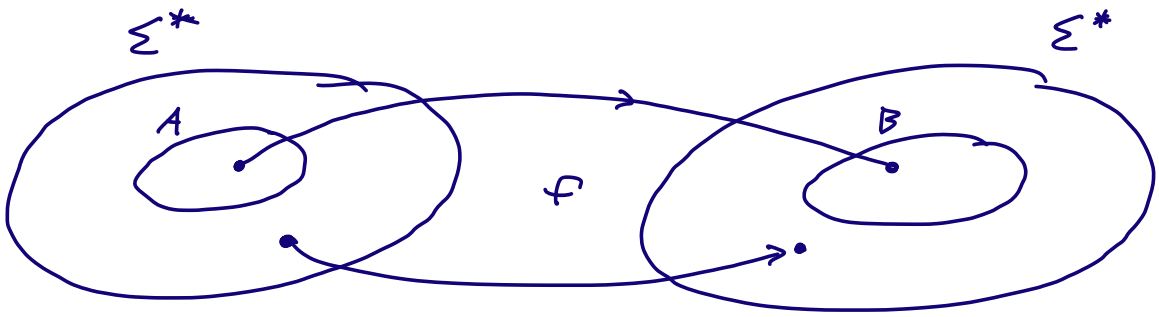
Reductions & Completeness (NP-compl.)

Readings: see above.

"$A \leq_p B$"

p-t mapping red.
p-t many-one red.
Karp red.

Def: Lang. A is poly-time reducible to lang B if $\exists$ poly-time comput. $f : \Sigma^* \to \Sigma^*$ s.t. $\forall w \in \Sigma^*$, $w \in A \iff f(w) \in B$.



Want solve problem A.

Optimist: if can solve B, red. from A to B lets you solve A.

Pessimist: if can't solve C, having a red. from C to A means you can't solve A either.

Facts:

- Transitive:
  If $L_1 \leq_p L_2$ + $L_2 \leq_p L_3$,
  then $L_1 \leq_p L_3$.

- If $L_1 \leq L_2$ + $L_2 \in P$, then $L_1 \in P$.

Let $\mathcal{C}$ be a cx class s.t. $P \subseteq \mathcal{C}$.
(think of $\mathcal{C}$ as NP, PSPACE, etc.)

Def we say L is **hard for $\mathcal{C}$** ($\mathcal{C}$-hard)
if $\forall L' \in \mathcal{C}$, have $L' \leq_p L$.

If furthermore $L \in \mathcal{C}$, we say L is **$\mathcal{C}$-complete.**

So, if $P \subseteq \mathcal{C}$ & L is $\mathcal{C}$-complete & $L \in P$, then $\mathcal{C} \subseteq P$.

? Do NPC (NP-complete) langs exist?

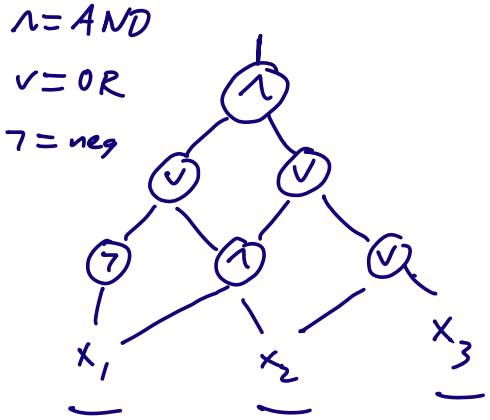
Y: $L = \{w = (M, x, 1^t) : M$ is an NTM that accepts x within t time steps$\}$.

is NPC.

There are other, cleaner, NPC langs...

Consider CIRCUIT-SAT $= \{C : C$ is a satisfiable Bool ckt$\}$.

$\wedge$ = AND
$\vee$ = OR
$\neg$ = neg



Cook-Levin thm: CIRCUIT-SAT is NPC.

- C-S is in NP: easy to guess s.a. sat. asst, check it indeed is s.a.

- Hardness: Let $L \in$ NP (any lang in NP), M be NTM, poly-time, dec. L.

To show: $L \leq_p$ C-S. $\qquad x \stackrel{?}{\in} L$

i.e. give poly-time red R: maps any $x \in \Sigma^*$ to a ckt C, st

$x \in L \Rightarrow C$ is sat.

$x \notin L \Rightarrow C$ <u>not</u> sat.

$T(n)$-time TM comput $\Rightarrow T(n) \times T(n)$ "computation tableau":

A Bool. ckt eval. to 1 on its given

$\Updownarrow$

a tableau being a legit descrip. of a det TM's exec. on x.

What about nondet of M?

vars of C?

Binary nondet choices of TM M $\Updownarrow$ Bool vars of C ;

partic. seq of nondet. choices causing M to accept

$\Updownarrow$

asst. to vars causing C to eval. to 1.

See Sipser thm 7.37 for details.

Recall: a CNF is AND of (clauses) ORs of lits x_i $\bar{x}_i$

A 3CNF: each clause has ≤ 3 lits.

DEF: 3CNF-SAT = $\{\varphi : \varphi$ is a satisfiable 3CNF$\}$

Thm: 3CNFSAT is NPC.

Pf sketch: Show CKT-SAT $\leq_p$ 3CNFSAT.

$C \longrightarrow f(C) = \varphi$ a 3CNF with a new var y_i for each gate in C. (+ C's old vars)

Struc. of clauses ensures that • clause i is sat iff value of new var $y_i \equiv$ value of gate i of ckt, given any asst to orig. input vars.

• clause for output gate (so that clause sat iff ckt is sat.) Sipser 7.42

Thm: CLIQUE is NPC.

Red. 3CNFSAT $\leq_p$ CLIQUE:

k-clause CNF $\rightsquigarrow$ G st G has k-clique iff C is satisfiable.

IND-SET = $\{(G,k)$: G has ind. set of size $k\}$

CLIQUE $\leq_p$ IND-SET: take complem. of G

VERTEX-COVER
SUBSET-SUM
COLORABILITY
⋮

} all NP-complete

Next time: Ladner's thm.

PS 1 up, due in 2 weeks.