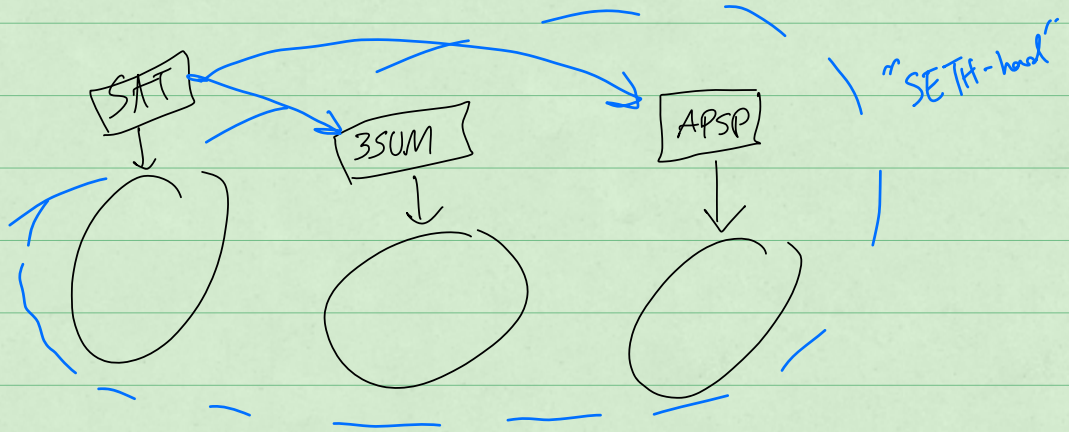
W9: Barriers for Reductions

Big open Questions:

1. SAT → 3SUM? "3SUM in $n^{1.99}$ time then SETH is false"?
2. SAT → APSP? "APSP in $n^{2.99}$ time then SETH is false"?
3. SAT → Max-Flow? "$\tilde{O}(m)$ for Max Flow then SETH is false"?



Max Flow algs:

$m \cdot n$	[Dinitz '70]
$m n^{2/3}$	[Goldberg-Rao 90's]
$m n^{1/2}$	[Lee-Sidford '14]
$m+n^{1.5}$	[vdB et al. '21]

open: $\tilde{O}(m)$

Today: A common barrier for proving these results.

High level idea: Find a measure that separates them.

Is Factoring NP-hard?

Factoring: given N and i, let p be the smallest prime that divides N. Is the i-th bit of p, 1?

Thm: Factoring is in $NP \cap coNP$.

Cor.: $NP \neq coNP \Rightarrow NP \neq NP \cap coNP \Rightarrow$ Factoring is not NP-Complete

Conjecture that gives a barrier for reductions.

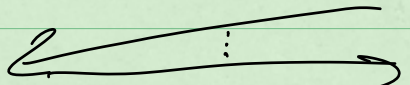
$NP \neq coNP$: "$\overline{k\text{-SAT}}$ is not in $NTIME[poly(n)]$."

"Strong" ↑ Hypothesis"

NSETH: "$\overline{k\text{-SAT}}$ is not in $NTIME[2^{(1-\varepsilon)n}]$" $\forall \varepsilon \exists k \ldots$

Prover — φ — Verifier

"φ is not satisfiable"



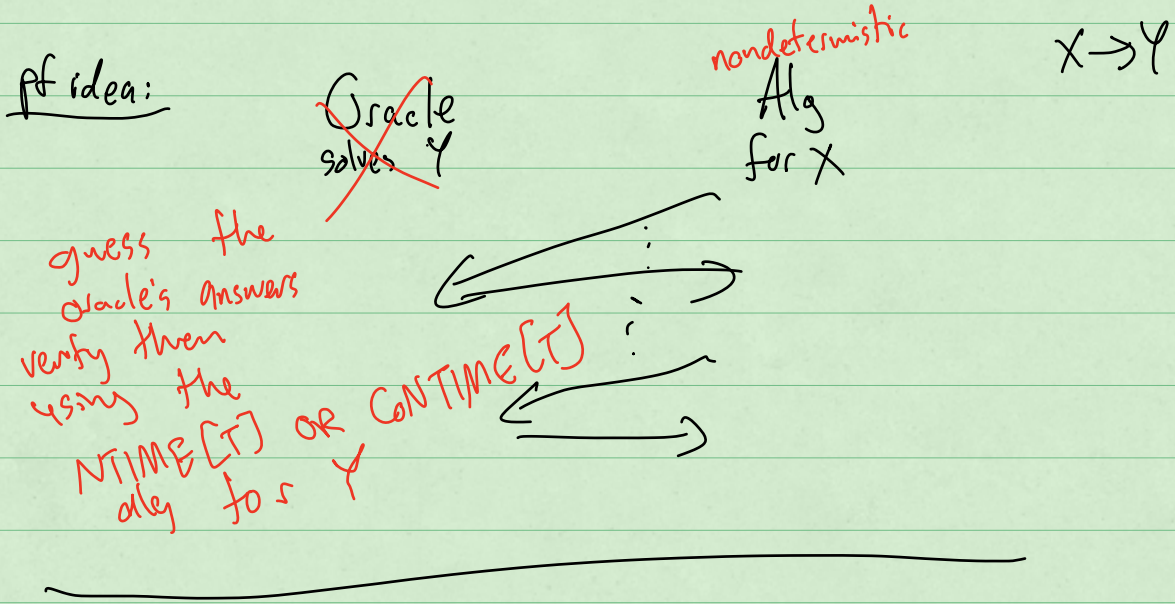
deterministic

only spends $2^{(1-\varepsilon)\cdot n}$ time.

NSETH: this is impossible.

Main Thm: If $X \in \text{NTIME}[T] \cap \text{coNTIME}[T]$ and there is a (deterministic) f.g. reduction proving that $O(T)$ for X refutes SETH then NSETH is fake.

pf idea:



Thm: If $X \in \text{NTIME}[T] \cap \text{coNTIME}[T]$ then, assuming NSETH, we cannot prove any $\Omega(T^{1+\varepsilon})$ l.b. for X under SETH via (det) fine grained reductions from SAT.

	LCS	Max Flow ($m=n$)
det:	n^2	$n^{1.5}$ ← $n^{1.4}$ $m+n^{1.5}$
NTIME∩coNTIME:	n^2	n

Time

Thm: Max Flow is in $NTIME[m] \cap coNTIME[m]$.

Cor. No $m^{1.1}$ l.b. for Max Flow (assuming NSETH and via fig. r)

pf: flow $\geq \tau$: guess the flow (of wt $\geq \tau$)
flow $\leq \tau$: guess the cut (of wt $\leq \tau$)

Thm: 3SUM is in $NTIME[n] \cap coNTIME[n^{1.5}]$.

Cor. no l.b. above $\Omega(n^{1.5})$ for 3SUM under SETH.

pf: (1) "yes": guess a triple and check.

(2) "no"

idea: use nondet. to reduce universe size.

3SUM in $\tilde{O}(U+n)$ via FFT.

Alg:

- guess prime $p \in [n^{1.5}, n^{1.5} \lg n]$

- use FFT to compute:

$$z = |S_p| = \left| \{ a,b,c \in S \text{ s.t. } a+b+c = 0 \bmod p \} \right|$$

- if $z > n^{1.5} \lg n$ - reject

- if $z \leq n^{1.5} \lg n$: guess z triples (a,b,c).
  - accept iff $\forall$ triples:
    $a+b+c = 0 \bmod p$
    but $a+b+c \neq 0$.

Correctness:

Lemma 1: If 3SUM = yes ($\exists\ a,b,c \in S$ s.t. $a+b+c=0$) then we never accept

pf:

$(a,b,c) \in S_p \quad \forall p$.

$\Rightarrow$ we cannot find $|S_p|$ triples with $a+b+c \neq 0$ (but $a+b+c = 0 \bmod p$)

$\exists$ triples s.t. $a+b+c = 0 \bmod p$

& $a+b+c \neq 0$

all are in S_p.

Lemma 2: If 3SUM = no ($a+b+c=0$)

then there is a guess that makes the alg accept.

pf:

Claim: $\exists\ p \in [n^{1.5}, n^{1.5}\log n]$ s.t. $|S_p| \leq n^{1.5}\log n$

$U = n^{3.1} \Rightarrow \forall a,b,c:\ a+b+c = C(n^{3.1})$

$\Rightarrow$ only $\log n$ primes ~~in $[n^{1.5}, \ldots]$~~ divide $a+b+c$

$\Rightarrow (a,b,c) \in S_p$ for only $O(\log n)$ primes.

$n^{3.1} = \tilde{p_1}^2 \tilde{p_2}^2 \cdots p_k$

$k \leq \log_2 n^{3.1}$

$\Rightarrow \sum_{p \in [n^{1.5}, n^{1.5}\log n]} |S_p| \leq n^3 \log n$

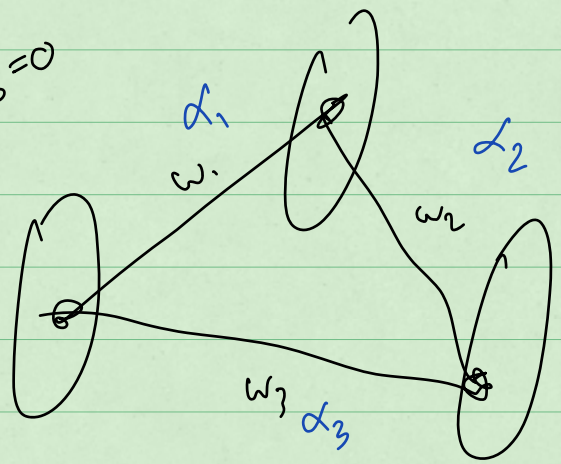
$\exists$ $n^{1.5}$ primes in $[n^{1.5}, n^{1.5}\log]$ $\Rightarrow$ $\exists p$ s.t. $|S_p| \leq n^{1.5}\log n$

Thm: APSP is in $\mathrm{NTIME}[n^{2.96}] \cap \mathrm{coNTIME}[n^{2.96}]$

Zero-$\triangle$ in

APSP
↓
Neg-$\triangle$
↓
Zero-$\triangle$

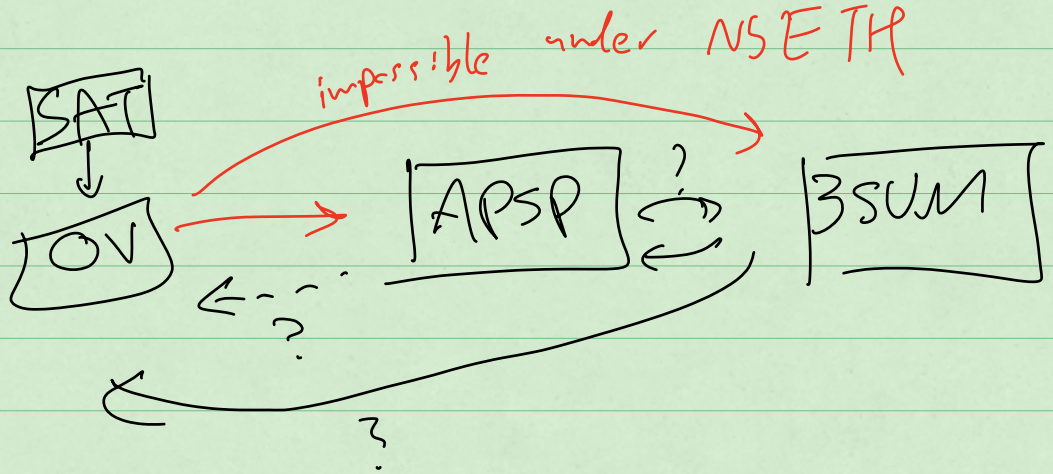
$\alpha_1, \alpha_2, \alpha_3$
$\alpha_1 + \alpha_2 + \alpha_3 = 0$



p^3

$p^3 \cdot n^\omega$ - counting # $\triangle$'s of wt 0 mod p.

$+ \frac{n^3}{p}$


impossible under NSETH
SAT
OV
APSP
3SUM
?
?
?