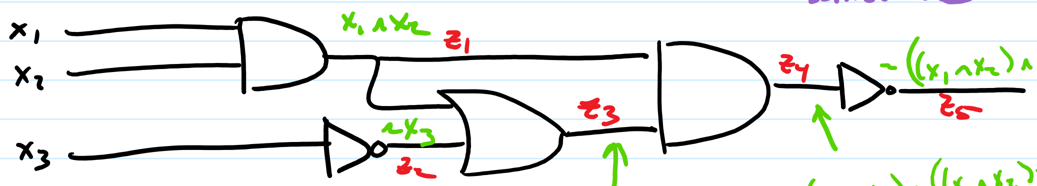
CIRCUIT-SAT and SAT

CIRCUIT-SAT $\le_p$ SAT [given circuit C, need to create φ s.t. C is satisfiable $\leftrightarrow$ φ is satisfiable]



$\sim((x_1 \wedge x_2) \wedge ((x_1 \wedge x_2) \vee \sim x_3))$

exponential :(

$(x_1 \wedge x_2) \wedge ((x_1 \wedge x_2) \vee \sim x_3)$

$(x_1 \wedge x_2) \vee \sim x_3$

$$
\begin{aligned}
&(z_1 \leftrightarrow (x_1 \wedge x_2))\\
\wedge\ &(z_2 \leftrightarrow \sim x_3)\\
\wedge\ &(z_3 \leftrightarrow (z_1 \vee z_2))\\
\wedge\ &(z_4 \leftrightarrow (z_1 \wedge z_3))\\
\wedge\ &(z_5 \leftrightarrow \sim z_4)\\
\wedge\ &z_5
\end{aligned}
$$

polynomial

SAT and 3-SAT

SAT $\leq_p$ 3-SAT [Goal: given φ, create 3-CNF φ' in poly-time s.t. $\varphi \equiv \varphi'$]

$$(x \underset{z_1}{\wedge} y) \underset{z_4}{\wedge} \underset{z_3}{\sim}(x \underset{z_2}{\vee} y)$$

$$\begin{aligned} & z_4 \\ \wedge\ & (z_4 \leftrightarrow z_1 \wedge z_3) \\ \wedge\ & (z_3 \leftrightarrow \sim z_2) \\ \wedge\ & (z_2 \leftrightarrow x \vee y) \\ \wedge\ & (z_1 \leftrightarrow x \wedge y) \end{aligned}$$

x	y	z_1	$z_1 \leftrightarrow x \wedge y$
T	T	T	T
T	T	F	F
T	F	T	F
T	F	F	T
F	T	T	F
F	T	F	T
F	F	T	F
F	F	F	T

$$\sim(z_1 \leftrightarrow x \wedge y) \equiv \sim\big((x \wedge y \wedge z_1) \vee (x \wedge \sim y \wedge \sim z_1) \vee (\sim x \wedge y \wedge \sim z_1) \vee (\sim x \wedge \sim y \wedge \sim z_1)\big)$$

$$\equiv (x \wedge y \wedge \sim z_1) \vee (x \wedge \sim y \wedge z_1) \vee (\sim x \wedge y \wedge z_1) \vee (\sim x \wedge \sim y \wedge z_1)$$

$$z_1 \leftrightarrow x \wedge y \equiv \sim\ \sim(z_1 \leftrightarrow x \wedge y) \equiv \sim\big((x \wedge y \wedge \sim z_1) \vee (x \wedge \sim y \wedge z_1) \vee (\sim x \wedge y \wedge z_1) \vee (\sim x \wedge \sim y \wedge z_1)\big)$$

co-NP

Decision Problem P is in NP means there is a poly-time algorithm A s.t. the set of instances x of P for which answer is YES is exactly the set of instances of x s.t. there exists y (poly-size) s.t. $A(x,y)=$ OK

Problem X is in ~~NP~~ co-NP means there is a poly-time algorithm A s.t. the set of instances x of X for which answer is ~~YES~~ NO is exactly the set of instances of x s.t. there exists y (poly-size) s.t. $A(x,y)=$ OK

Ex: $\overline{SAT}$ = given φ, determine if φ has <u>no</u> satisfying assignment

$\overline{SAT} \in$ co-NP using verifier for SAT

$(x \vee y) \wedge (\neg x \vee y)$

$(x \vee y) \wedge (\neg x \vee y) \wedge \neg y$

THM: If $X \in P$ then $\overline{X} \in P$

Proof: Suppose $X \in P$. Then $\dfrac{X\text{-comp}(x)}{\text{return } \neg X(x)}$ is a poly-time alg for $\overline{X}$, so $\overline{X} \in P$

THM: If $P = NP$ then $NP =$ co-NP

Proof: Suppose $P = NP$ [need $NP =$ co-NP]

$NP \subseteq$ co-NP: if $X \in NP$ then $X \in P$ and $\overline{X} \in P$ and $\overline{X} \in NP$ and $X \in$ co-NP

co-NP $\subseteq NP$:

COR: If $NP \neq$ co-NP then $P \neq NP$

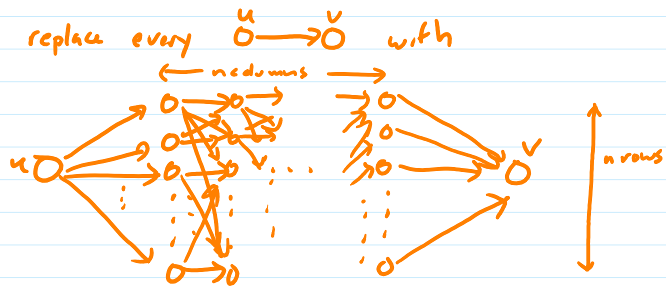
PSPACE

QSAT: Given φ, determine whether $\exists x_1 \forall x_2 \exists x_3 \ldots \varphi(x_1, \ldots, x_n)$ is true.

AVG-PATH-LEN: Given directed G, vertices s,t, integer k, determine if avg path length $s \rightsquigarrow t > k$

s-t HAM-PATH $\leq_p$ AVG-PATH-LEN

replace every $u \to v$ with



AVG-PATH-LEN $\in$ NP?
dunno, seems like not
same w/ QSAT

one $s \rightsquigarrow t$ HP becomes $(n^n)^{n-1}$ paths of length $(n+1)(n-1)$
all other paths become $\leq (n^n)^{n-2}$ paths of length $\leq (n+1)(n-2)$
if one HP in G, then so many long paths in G' that avg is $> (n+1)(n-2)$

PSPACE: set of problems solvable in poly space

QSAT $\in$ PSPACE

```
eval(φ)
  write Q x_i φ'
  let φ_T = φ' with x_i set to T
      φ_F = φ' with x_i set to F
  r_T = eval(φ_T)
  r_F = eval(φ_F)
  if Q = ∀ and r_T and r_F both T
      return T
  else if Q = ∃ and (r_T or r_F) is T
      return T
  else
      return F
```

AVG-PATH-LEN $\in$ PSPACE : try every permutation of vertices
if it is a path
compute len, add to sum,
incr count
avg $\leftarrow$ sum/count
return avg $\leq k$

P $\subseteq$ PSPACE

NP $\subseteq$ PSPACE
co-NP $\subseteq$ PSPACE

SAT $\in$ PSPACE $\quad \forall X \in NP,\ X \leq_p SAT$

$P \stackrel{?}{=} PSPACE$ don't know
$NP \stackrel{?}{=} PSPACE$