$\text{CIRCUIT-SAT} = \{\langle C\rangle : \exists x \in \{0,1\}^n\ C(x)=1\}$

n input gates, m total gates } brute force $O(2^n \text{poly}(m))$

CNF = AND of ORs = $\wedge\vee$

$\text{CNF-SAT} = \{\langle F\rangle : \exists x \in \{0,1\}^n\ F(x)=1,\ F \text{ CNF}\}$

n input gates

m OR gates

k-SAT = CNF-SAT but each clause has at most k literals

Randomized k-SAT solver

RW($\langle F,x\rangle$): // random walk

for u in 1 to $100n^2$:

pick uniformly random clause $C \in F$ violated by x

pick uniformly random literal $x_j \in C$

flip x_j to $1-x_j$

WALK-SAT($\langle F\rangle$):

for t in 1 to $(2-\frac{2}{k})^n$:

pick uniformly random $x \in \{0,1\}^n$

$x \leftarrow$ RW($\langle F,x\rangle$)

if $F(x)=1$: accept

reject

Proof. (2-SAT)

$R(i,i+1) = N(i+1) - N(i)$

$R = \sum_0^{n-1} R(i,i+1)$

linearity, Markov

} R: # times RW loop runs

$N(i)$ = num steps taken by RW until agree(j) = i

ETH (exponential time hypothesis)

$\exists \delta>0,\ \text{3-SAT} \notin \text{TIME}(2^{\delta n})$

SETH (strong exponential time hypothesis)

$\forall \delta>0, \exists k \in \mathbb{N},\ k\text{-SAT} \notin \text{TIME}(2^{(1-\delta)n})$

$\text{SETH} \Rightarrow \forall \varepsilon>0\ \ \text{LCS} \notin \text{TIME}(n^{2-\varepsilon})$

TM $V(\langle x,y\rangle)$ verifier if

$x \in L \Rightarrow \exists y\ V(\langle x,y\rangle)$ accepts

$\exists y\ V(\langle x,y\rangle)$ accepts $\Rightarrow x \in L$

V polytime if $V(\langle x,y\rangle)$ halts in $O(|x|^c)$ time

$\text{NP} = \{L : \exists \text{ polytime } V \text{ for } L\}$

$\text{NP} \subseteq \text{EXP}$ try all $c|x|^c$ strings

$\text{P} \subseteq \text{NP}$ ignore verifier

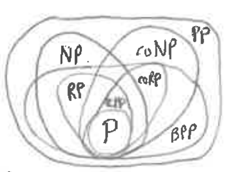
$\text{NP} = \{L : \exists$ polytime PTM M,

$x \in L \Rightarrow \mathbb{P}[M(x)=1] > 0$

$x \notin L \Rightarrow \mathbb{P}[M(x)=1] = 0\}$

$\text{RP} \subseteq \text{NP}$

$\text{coRP} \subseteq \text{coNP}$



RECAP For M polytime PTM, if

$x \in L$	$x \notin L$	class
$\mathbb{P}[M(x)=1]=1$	$\mathbb{P}[M(x)=1]=0$	P
$\mathbb{P}[M(x)=1]\geq \frac{2}{3}$	$\mathbb{P}[M(x)=1]=0$	RP
$\mathbb{P}[M(x)=1]=1$	$\mathbb{P}[M(x)=1]\leq \frac{1}{3}$	coRP
$\mathbb{P}[M(x)=1]>0$	$\mathbb{P}[M(x)=1]=0$	NP
$\mathbb{P}[M(x)=1]\geq \frac{2}{3}$	$\mathbb{P}[M(x)=1]< \frac{1}{3}$	BPP

$A \leq_m^P B$ if $\exists$ polytime $R: A \to B$

$A \leq_T^P B$ if given oracle deciding B in polytime, $\exists$ polytime TM deciding A

all's Thm. $G(U,V,E)$ bipartite, $|U|=|V|$ has perfect matching iff $\forall S \subseteq U, |N(S)| \geq |S|$

S NP-hard if $\forall L \in \text{NP}, L \leq_m^P S$

S NP-complete if ① $S \in \text{NP}$
② S NP-hard

END DIDEROT CHAPTERS 9-15

Review

THT: $f(n)$ clockable, $n \log n \leq O(f(n)) \Rightarrow \exists L,\ L \in \text{TIME}(f(n) \cdot \log f(n)),\ L \notin \text{TIME}\left(\frac{f(n)}{\log f(n)}\right)$

Usefully, $f(n) = n^{c+0.5} \Rightarrow \text{TIME}(n^c) \subsetneq \text{TIME}(n^{c+1})$

ECFT: M decides $L \subseteq \{0,1\}^*$, $T_M(n) \geq n \Rightarrow \forall n \exists C_n$ of size $O(T_M(n)^2)$ deciding L on length-n inputs

If $T_M(n) \leq n^k$, $\exists F_M$ such that $F_M(n) = \langle C_n\rangle$ in polytime