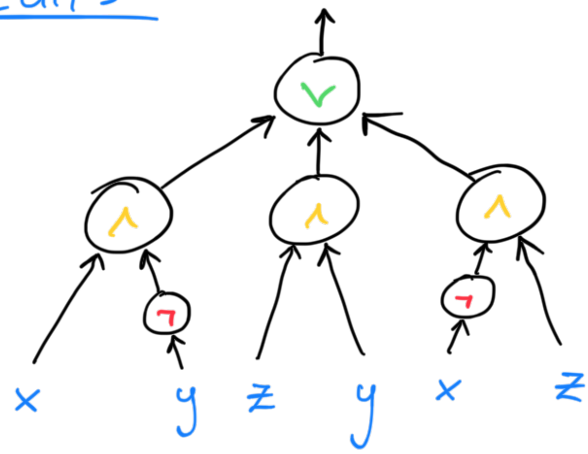
Boolean Circuits

CNFs

(treelike circuit)



Note Every $f:\{0,1\}^n \to \{0,1\}$ is computed by CNF/DNF of size $\le 2^n$

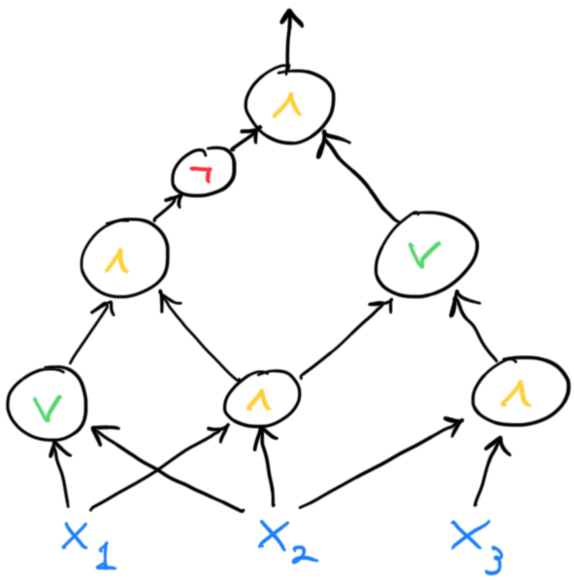
DNF: $f(x) = \bigvee_{\substack{y:f(y)=1 \\ \in \{0,1\}^n}} \underbrace{(x \stackrel{?}{=} y)}_{\bigwedge_{i=1,\dots,n} \begin{cases} x_i & \text{if } y_i = 1 \\ \bar{x}_i & \text{if } y_i = 0 \end{cases}}$ Exp size!

CNF: DNF for $\neg f$, convert to CNF for f

General circuits

- Input vars $x_1 \dots\dots x_n$
- Gates $\wedge, \vee, \neg$
- Directed edges (wires)
  no directed cycles!
- one or more output wires

Size = # wires



Def: $L \in SIZE(t(n))$

$\Updownarrow$

$\exists$ circuit family $\{C_n\}_{n\in\mathbb{N}}$:

$\forall n$: • C_n has size $O(t(n))$

• $\forall x \in \{0,1\}^n$: $C_n(x) = 1$ iff $x \in L$

Note: $\forall L \subseteq \{0,1\}^*$: $L \in SIZE(2^n)$

Def: $P/poly := \bigcup_{k\in\mathbb{N}} SIZE(n^k)$

Note: $P/poly$ contains undec. languages

e.g. $\{1^n : n\text{-th TM halts}\}$

Thm: $P \subseteq P/poly$

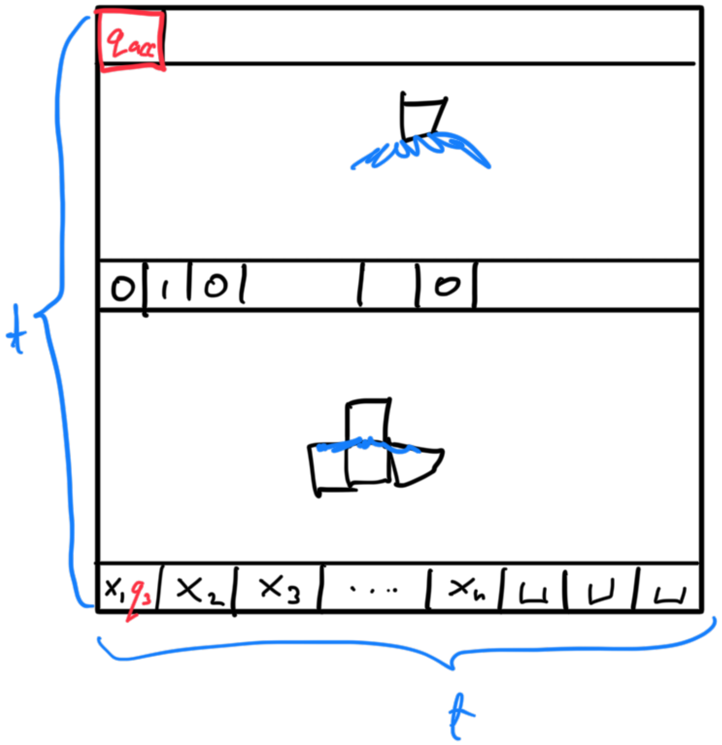
$\Uparrow$

Thm Given TM M, input length n, runtime $t(n)$ we can compute in time $poly(t(n))$ a circuit C_n of size $O(t(n)^2)$ s.t.

$$C_n(x) = M(x) \quad \forall x \in \{0,1\}^n$$

Proof sketch

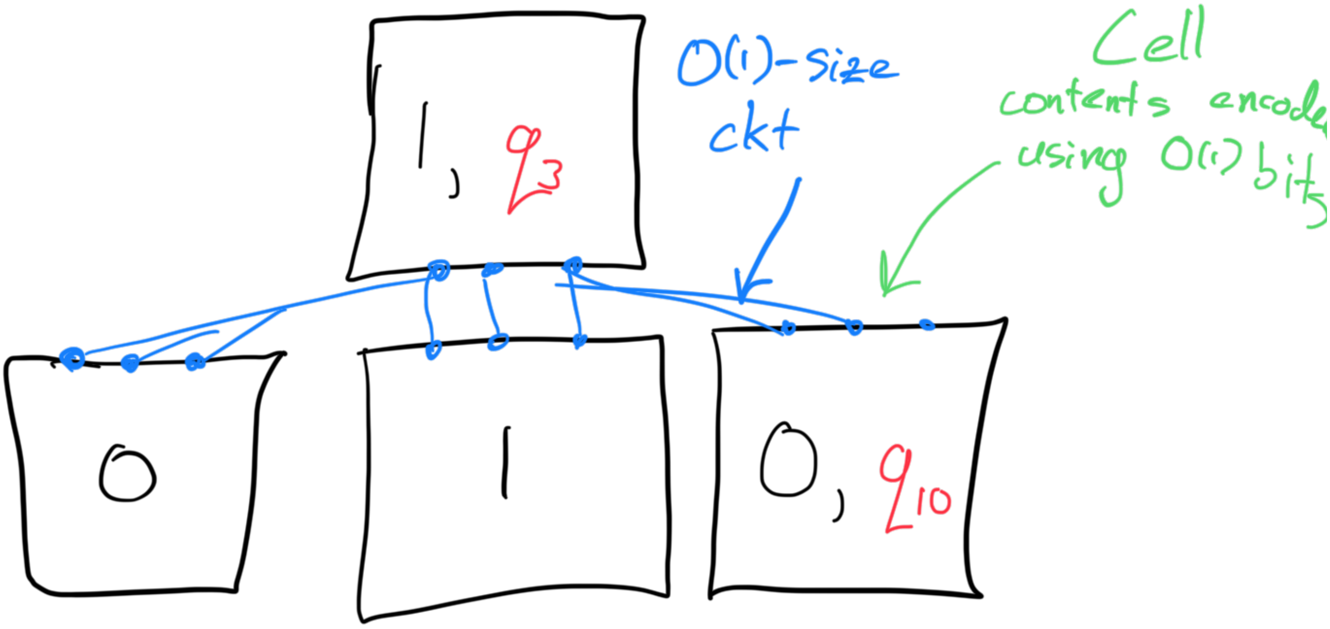
Consider $t \times t$ tableau for M



Size
$t^2 \cdot O(1)$

← i-th row: config after i steps

<u>Claim:</u> Every cell ($O(1)$ bits) is function of some 3 cells below it



<u>Plan</u>

WitnessExistence $\leq_p$ Circuit-SAT $\leq_p$ SAT

Def: $WE = \{\langle \overset{\text{TM}}{V}, x, \underbrace{1^t}_{\text{unary}}\rangle : \exists y,\ V(x,y)=1 \text{ in time } t\}$

Claim: $WE \in NP$

Lemma: WE is NP-hard $(\forall L \in NP,\ L \le_p WE)$

Proof. Let $L \in NP$. Say V is an n^k-time verifier for L. $(L = \{x : \exists y.\ V(x,y)=1 \text{ in time } n^k\})$

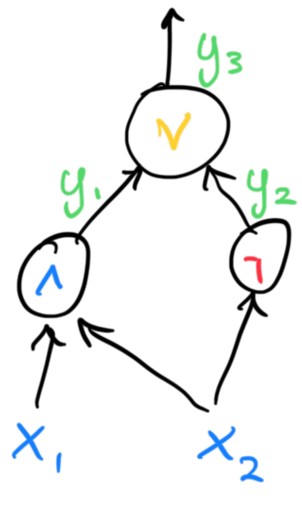
Reduction $f: L \le_p WE$

$$f(x) = \langle V, x, 1^{|x|^k}\rangle \quad (\text{Runtime } O(n^k))$$

Def: $\text{CircuitSAT} = \{\langle C_n\rangle : \exists x \in \{0,1\}^n,\ C_n(x) = 1\}$

Lemma $\text{C-SAT} \overset{f}{\le_p} \text{SAT}$

Key: Introduce new var for each wire



C_n

$$\begin{aligned} f(C_n) = {} & (y_1 \leftrightarrow x_1 \wedge x_2) \wedge \\ & (y_2 \leftrightarrow \neg x_2) \wedge \\ & (y_3 \leftrightarrow y_1 \vee y_2) \wedge y_3 \end{aligned}$$

Def: $WE = \{\langle V, x, \underbrace{1^t}_{\text{unary}} \rangle : \exists y,\ V(x,y)=1 \text{ in time } t\}$

Lemma $WE \leq_p C\text{-}SAT$

Proof Define $f(\langle V, x, 1^t \rangle) = \langle C_V(\overset{\text{hardcode}}{x}, \overset{\text{free}}{\_\_}) \rangle$

C_V = circuit computed from $V, |x|, t$

$[C_V(x,y) = V(x,y)]$