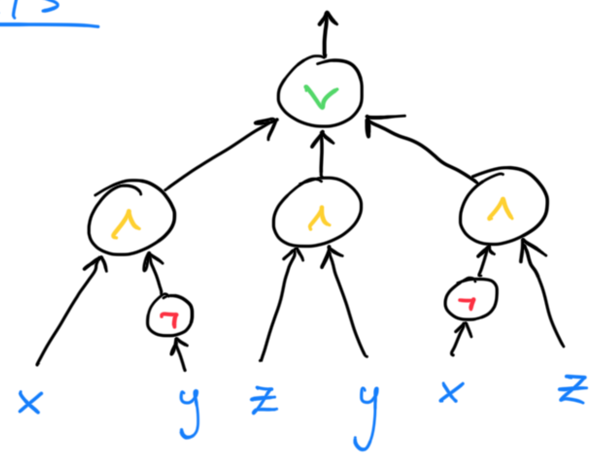
Boolean Circuits

CNFs

(treelike circuit)



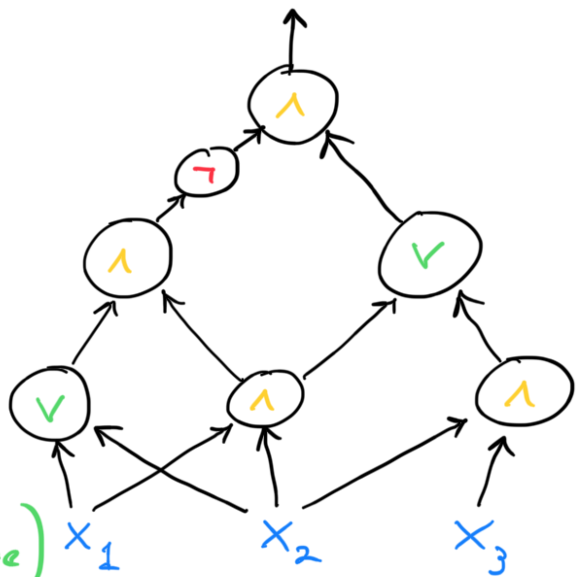
Note: Every $f: \{0,1\}^n \to \{0,1\}$ is computed by CNF/DNF of size $\leq 2^n$

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

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

General circuit

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



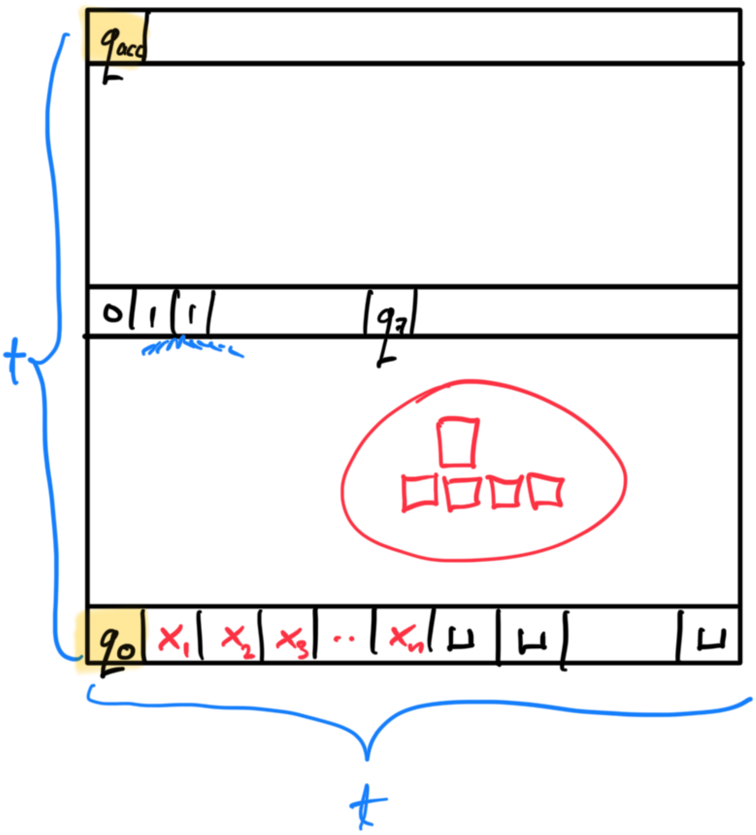
size = #wires (≈ runtime)

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.

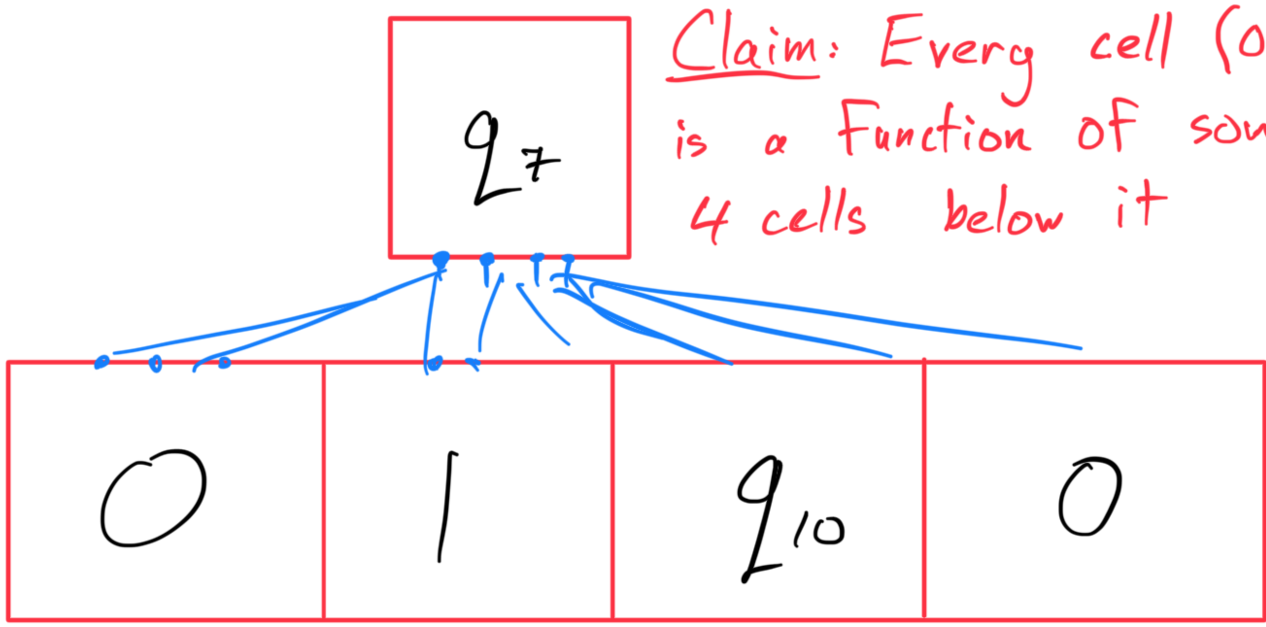
$$C_n(x) = M(x) \quad \forall x \in \{0,1\}^n$$

Proof sketch Consider $t \times t$ tableau for M



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

← i-th row: config after i steps



Claim: Every cell (O(1) bi
is a function of some 4 cells below it

Plan WitnessExistence $\le_p$ Circuit-SAT $\le_p$ SAT

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

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 ($L = \{x : \exists y,\ V(x,y)=1$ in time $n^k\}$)

Reduction $f: L \le_p WE$

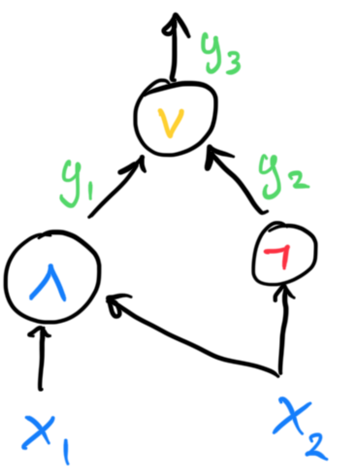
$$f(x) = \langle V, x, 1^{|x|^k} \rangle$$

Ex: HALT and A_{TM} are complete for RE $= \{$recog. languages$\}$

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

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

Key: Introduc new var for each wire



C_n

$$f(C_n) = (y_1 \leftrightarrow x_1 \wedge x_2) \wedge$$

$$(y_2 \leftrightarrow \neg x_2) \wedge$$

$$(y_3 \leftrightarrow y_1 \vee y_2) \wedge y_3$$

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

Lemma $WE \overset{f}{\leq} C\text{-SAT}$

Proof Define $f(\langle V, x, 1^t\rangle) = \langle C_V(x, \overset{\text{Free}}{\underline{\quad}})\rangle$

C_V = circuit compute from V, input length $|x| + |y| \leq t$, runtime t

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