• $\mathrm{SIZE}(T) :=$ Lecture 17

Set of languages L
decidable by an $O(T)$-sized
circuit family

* $\forall x$, $x \in L \leftrightarrow C_{|x|}(x) = 1$

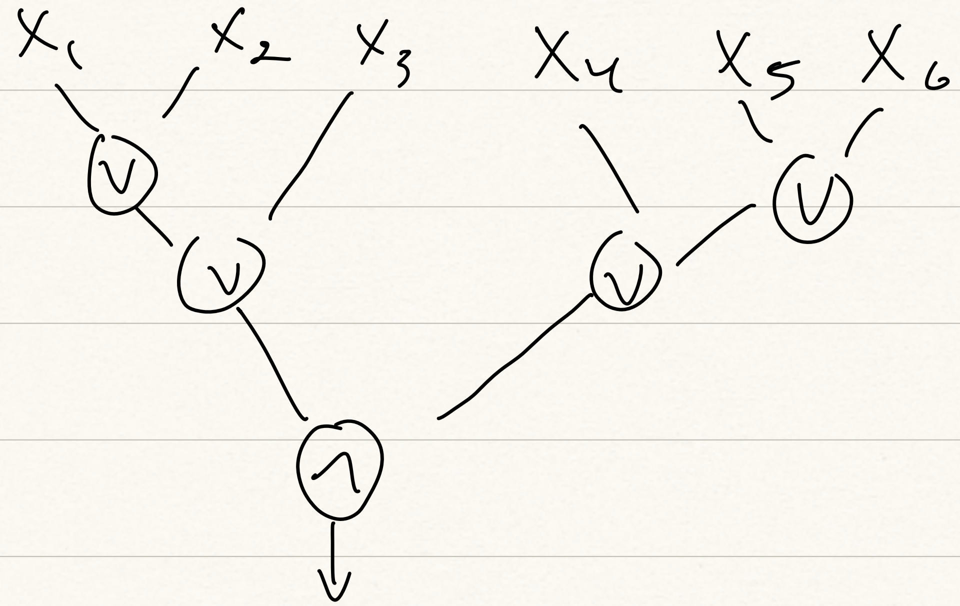
$$\{C_n\}_{n \in \mathbb{N}}$$

Facts:

① 3CNF is a special-case
of circuits

$$\phi = (x_1 \vee x_2 \vee x_3) \wedge$$

$(x_4 \vee x_5 \vee x_6)$



- Every $f: \{0,1\}^n \to \{0,1\}$ has $O(n2^n)$ sized CNF computing it
  $\Rightarrow O(n2^n)$-sized circuit

$\ast$ Shannon: $O(2^n/n)$ $\forall f$

$\ast$ Others: $(2^n/n)(1+o(1))$

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

Properties of P/poly

Thm: $P \subseteq P/poly$

Proof:

① Recall any time-T TM M has an equivalent oblivious TM N running in time $O(T \log T)$ — $O(T^2)$

- $\forall x \quad M(x) = N(x)$

and the positions of N's tape heads are only a function of $|x|$ and the current timestep i.

* For all inputs of length n, $N(x)$ does the exact same thing

* Now, we argue every time-T OTM has an $O(T)$-sized circuit.

- Highlights
  - $N(x)$ runs in time

$$t = T(|x|)$$

- Define transcript of $N(x)$:

$$z_1, z_2, \dots, z_t$$

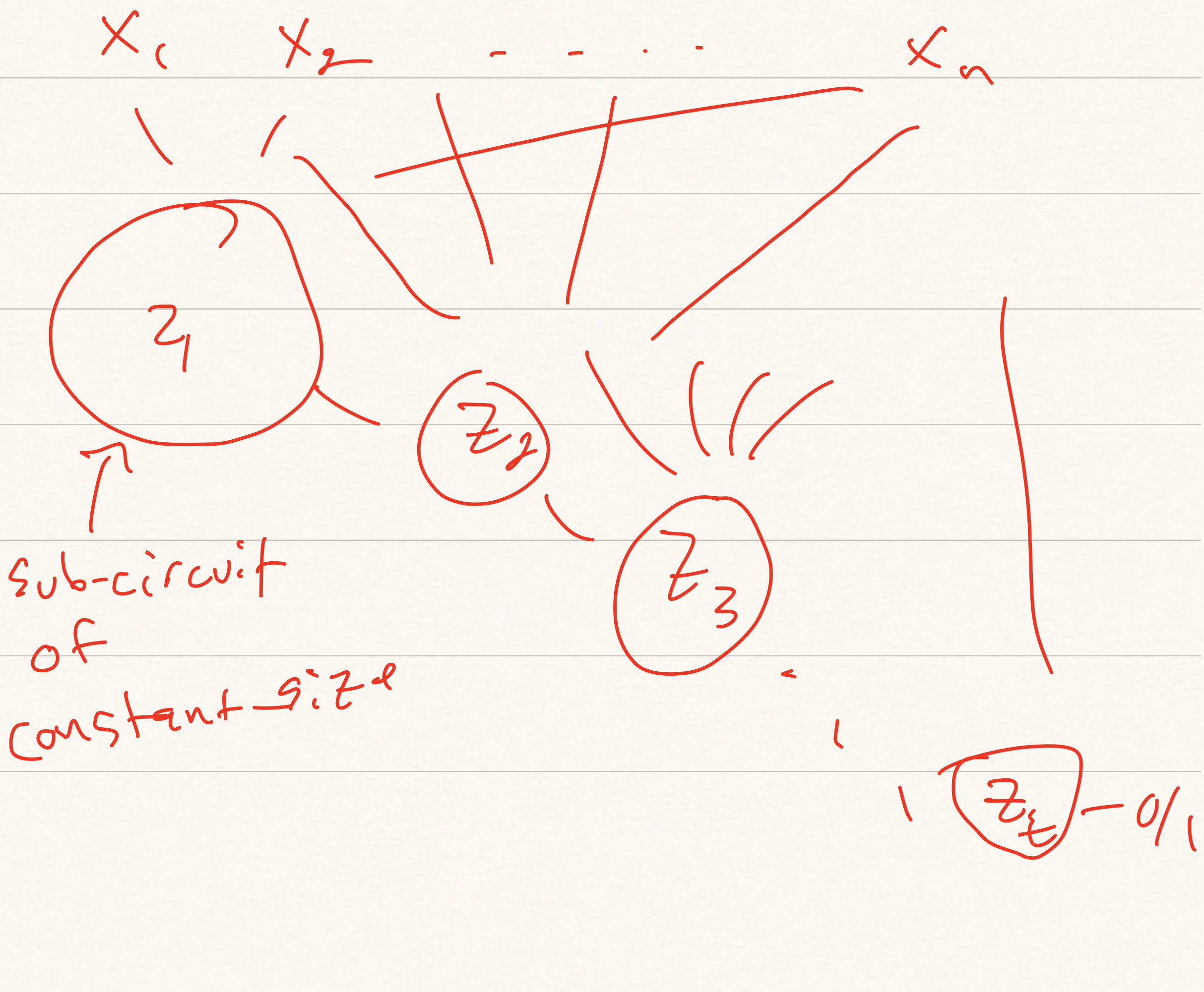
$$\delta(z_1) = z_2 \dots \delta(z_i) = z_{i+1}$$

Each z_i is a snapshot
- N's current state
- All k-symbols read by N's tape heads

$\Rightarrow |z_i| = O(1)$

* can compute each z_i using a constant-size circuit.

* compose all these circuits together, you get $O(t)$-size circuit



* In the above proof, we can do the transformation in

  - poly-time
  - log-space *

---

* $P \subsetneq P/poly$
  - Because $\exists\, L \subset \{1\}^* \subset \{1^n : n \in \mathbb{N}\}$ s.t. $L \in EXP$ or L is undecidable

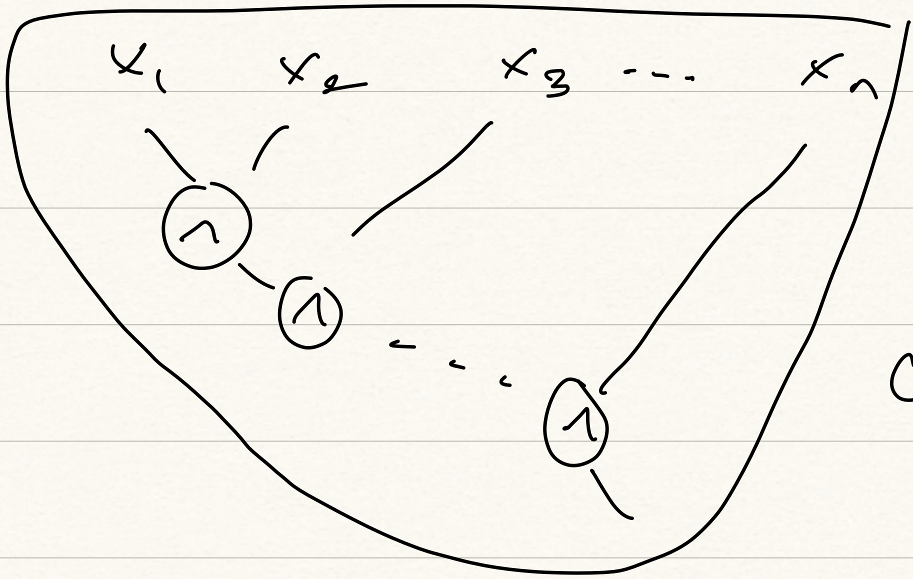
<u>Lemma</u>: $\forall L \subset \{1^n : n \in \mathbb{N}\}$

$L \in P/poly$

<u>Proof</u>:

If $1^n \in L$,

C_n is the big AND circuit

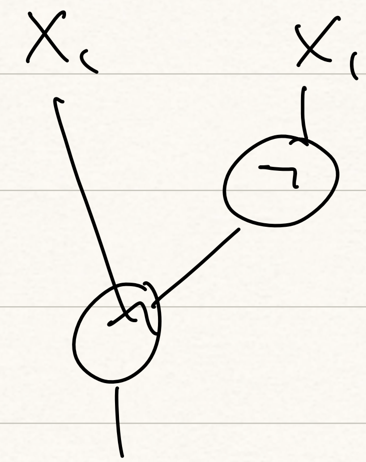


C_n

$C_n(x) = 1 \iff x = 1^n$

If $1^n \notin L$, define

$C_n =$



$\square$

<u>Ex</u>:

$$\mathrm{UHALT} := \{ 1^n \mid \langle n \rangle_2 = (M, x) \text{ and } \underset{\substack{\uparrow \\ \mathrm{TM}}}{M}(x) \text{ halts} \}$$

* $P/poly \not\subseteq EXP$

$\not\subseteq NP$

$\mathrm{UHALT} \in P/poly$

but <u>not</u> Turing Decidable.

Alternate Cook-Levin Thm/Proof

Def. CKT-SAT

$\doteq \{ C \mid C$ encodes a circuit with 1-bit output and $\exists\, w$ s.t. $C(w) = 1 \}$

Thm: CKT-SAT is NP-complete.

① CKT-SAT $\in$ NP.

- Certificate is w

s.t. $C(w) = 1$

② CKT-SAT is NP-Hard

$\forall L \in NP$

$L \le_p$ CKT-SAT

$\Rightarrow$ Proof we did before transforming det. verifier M_L to circuit of size $O(T^2)$ if M_L runs in time T

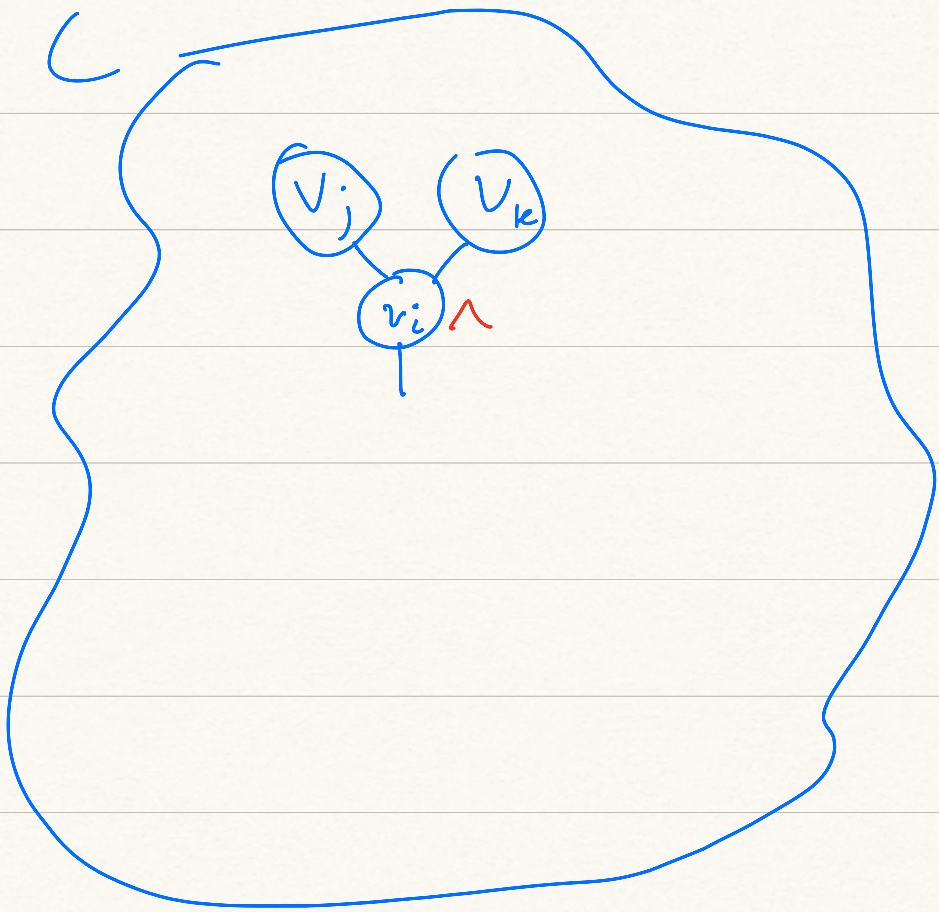
$x \in L \iff \exists w$ s.t. $M_L(x,w) = 1$

transform into C_x s.t.

$C_x(w) = 1$.

③ CKT-SAT $\leq_p$ 3SAT

C



$(\underline{v_j} \wedge v_k) = v_i$ nodes in C

$\downarrow$

$\underbrace{(z_j \wedge z_k) = z_i}_{\text{Boolean equality}} \mapsto$ 4 clauses in 3CNF

$x = y \mapsto \underline{(x \vee \bar{y}) \wedge (\bar{x} \vee y)}$

$(\underline{v_j \vee v_k}) = v_i$

$(z_j \vee z_k) = z_i$

$\hookrightarrow (\bar{z}_i \vee z_j \vee z_k)$

$\wedge (z_i \vee \bar{z}_j) \wedge (z_i \vee \bar{z}_k)$

$$v_j \xmapsto{} v_i$$

NOT

$\bar{z}_j = z_i \leftrightarrow (z_i \vee \bar{z}_j) \wedge (\bar{z}_i \vee z_j)$

Corollary: If $A \in DTIME(T)$ then $A \in SIZE(T^2)$

Uniformly Generated Circuits

- If $L \in P/poly$, its enough that $\{C_n\}$ exists.

Def: $\{C_n\}$ is P-uniform if there exists a poly-time TM M s.t. $\forall n$

$$M(1^n) = C_n$$

Thm: L has a P-uniform circuit family iff $L \in P$.

Proof: $\forall x$: $n = |x|$

P-uniform $\left\{ \begin{array}{l} x \in L \iff C_n(x) = 1 \\ \text{where } \underbrace{M(1^n) = C_n}_{\text{poly}(n)} \end{array} \right.$

Define: $N(x)$:

- Run $M(1^{|x|}) = C_{|x|}$
- Output $C_{|x|}(x)$

clearly poly-time.

- Other direction

$$A \in DTIME(T)$$

$$\Rightarrow A \in SIZE(T^2) \qquad \square$$

Logspace Uniform Circuits

↳ P-uniform circuits that are (implicitly) logspace

$M(1^n) = C_n$ using

$O(\log(n))$ space on
non-output tape

* $M(1^n)$ outputs ith
bit of $\langle C_n \rangle_2$ in
logspace for all i.

<u>Thm</u>: L is decidable by a
logspace uniform circuit
family iff $L \in P$.

P/poly vs. NP

Thm. If $NP \subseteq P/poly$, then $PH = \Sigma_2^P$.

Proof next time

* Show $\Pi_2^P \subseteq \Sigma_2^P$ if $NP \subseteq P/poly$ *

P/poly vs. EXP?

Thm: If $EXP \subseteq P/poly$ then $EXP = \Sigma_2^P$

BPP vs. P/poly?

* $P \subseteq BPP$

- Thm: $BPP \subseteq P/\text{poly}$.

Lecture 17