L30 2022-11-30

Space Complexity.

def like time complexity, but instead of #steps we count max size of tape during computation.

$sp(x) = \max |s_i|$ where $s_0 \dots s_t$ are states

$sp(n) = \max\limits_{|x|=n} |sp(x)|$

$DSPACE(g) = \{L : \exists TM \text{ deciding } L \text{ in space } O(g)\}$.

$PSPACE = \{L : \exists TM \text{ deciding } L \text{ in space } O(n^c)\}$.

obs $DTIME(g) \subseteq DSPACE(g)$, hence $P \subseteq PSPACE$.

in fact, $\Sigma^i P \subseteq PSPACE \ \forall i$.

(sketch: can try all combinations of quantifiers using space $\lesssim$ length of quantified strings $\lesssim$ poly + space needed for verifier $\lesssim$ poly).

e.g. $SAT \in PSPACE$.

M: for each $\alpha \in \{0,1\}^n$:
  if $F(\alpha)$ is SAT:
    accept
  reject

If space is small, then time is also small.

prop $DSPACE(g) \subseteq DTIME(2^g)$.

(sketch: there are 2^s states of size s).

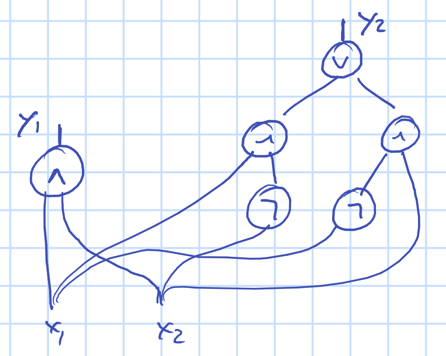
hence $PSPACE \subseteq EXP$, and $\underset{\text{space } \log(n).}{L} \subseteq P$

Circuit Complexity.

A circuit is a collection of $\wedge, \vee, \neg$ gates (with 2/2/1 inputs and 1 output) connected by wires.

Each input is connected to either a variable x_i or to the output of another gate. Note one output can have multiple inputs.

e.g. $y_1 y_2 = x_1 + x_2$.



A circuit computes a function $\{0,1\}^n \to \{0,1\}^m$, where m is the number of (global) output gates not connected to any input. Usually $m = 1$.

A family of circuits can be used to decide a language:

$L(C_0, C_1, \dots C_n, \dots) = \{x : C_{|x|}(x) = 1\}$.

def size of a family of circuits $sz(n) = |C_n|$.

th poly-time TMs can be computed by poly-size ckts.

We can look at depth as a measure of parallelization.

def depth of a circuit $d(C)$ = longest path input-output.

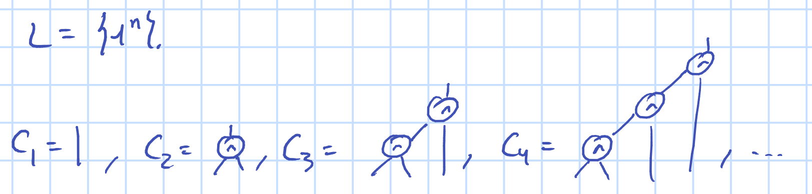
def $NC^i = \{L : \exists^u \text{ circuits of depth } (\log(n))^i \text{ and poly size deciding } L\}$

NC^i is easy to parallelize.

$NC^i \subseteq P$; P-hard problems are hard to parallelize.

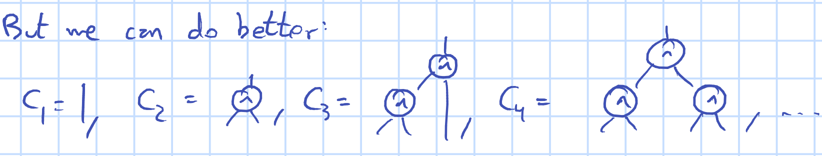
* $\exists^u$ stands for "there exists a uniform family of circuits". Uniform means that there is a TM $M : n \mapsto C_n$. It is important to have this condition, otherwise we could have undedidable languages in NC^1. (e.g. 1^n, where $n = \langle M, x\rangle$).

e.g. $L = \{1^n\}$.



Family of poly-size, but linear depth circuits.

But we can do better:



Family of poly-size and log-depth circuits.

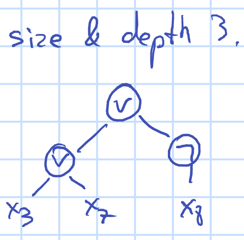
Hence $\{1^n\} \in NC^1$.

e.g. $L = 3CNF\text{-}Eval = \{F, \alpha \text{ st } F(\alpha) = 1\}$

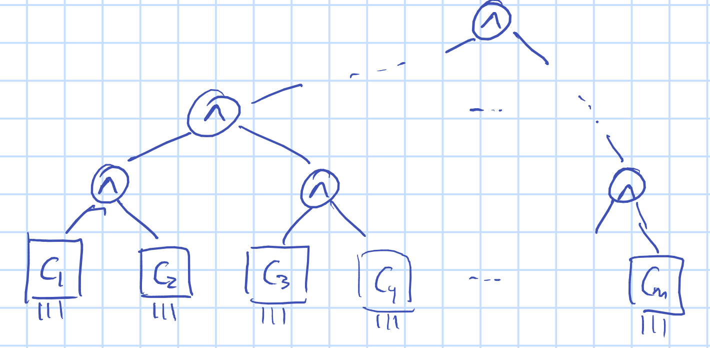
Let $F = D_1 \wedge D_2 \wedge \dots \wedge D_m$.

Can evaluate D_i with a circuit of size & depth 3.

e.g. $D_i = x_3 \vee x_7 \vee \overline{x_8}$

$C_i =$ 

Can evaluate all D_i in parallel, and check AND of all of them with previous construction:



Hence $3CNF\text{-}Eval \in NC^1$.