Michael Forbes
mforbes@illinois.edu

2018-01-31.4 → 2018-02-05.1
2018-02-05.2 ← cs579

cs579 Computational Complexity : Lecture 6

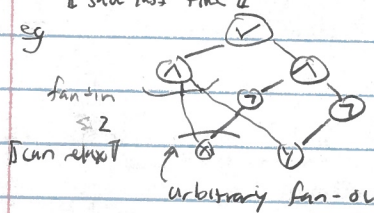
8/11

admin: ps 1 due
ps 2 out

today: circuits

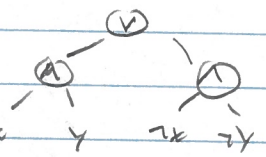
Q: hardware vs software? [GPUs / deep learning, FPGA / bit coin]
↳ changes w/ problem size → indep. of size = uniform
= non uniform

eg [same last time]



≡ EQ(x,y) [computes in natural way]

fan-out 1



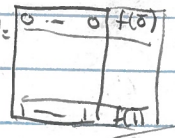
size = # gates

def: $SIZE(s(n)) = \{ L : size(L \cap \{0,1\}^n) \le s(n) \}$

$P/poly = SIZE(poly(n))$ [explain nonuniform later]

Q: P vs P/poly? [today]
NP vs P/poly? [next time]

lem: $f: \{0,1\}^n \to \{0,1\}$. $size(f) \le O(n \cdot 2^n)$

Pf: truth table(f): 

$O(n 2^n)$ size

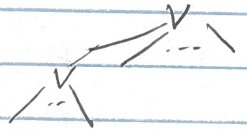
[do lookup]

$$f(\bar{x}) = \bigvee_{\bar{y} \in \{0,1\}^n : f(\bar{y})=1} \mathbb{1}_{\bar{x}=\bar{y}} = \bigvee_{\bar{y}} \bigwedge_{i=1}^{n} (x_i = y_i)$$

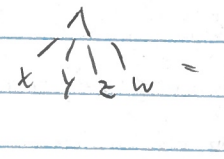
size $O(n 2^n)$

$$(x_i = y_i) = \begin{cases} x_i & y_i = 1 \\ \neg x_i & y_i = 0 \end{cases}$$

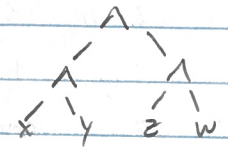
disjunctive normal form (DNF)



but



=

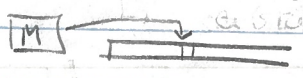


vertices: ≤ doubled
edges: ≤ doubled

[one tape TM]

P.rdp: $TIME(t(n)) \subseteq SIZE(O(t(n)^2))$

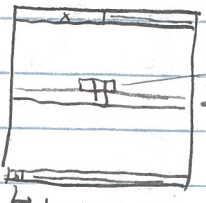
Pf: TM:



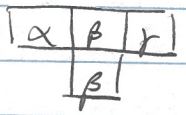
[config of TM]
= - head position
- tape contents
- current state

t(n)

computation tableau

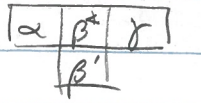


← config at start
[window]
← at time i
← at end

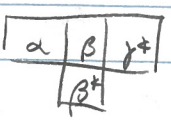


$\alpha, \beta, \gamma \in (\Gamma \cup \Gamma^*) \times Q$

[no head]



[symbol is written]



[head moves]

Clm: each cell determined by local update rule

$$\omega : ((\Gamma \cup \Gamma^*)^3 \times Q) \to (\Gamma \cup \Gamma^*) \times Q$$

↳ $O_n(1)$ - size circuit [multiple outputs]

Michael Forbes
MForbes@illinois.edu
2018-02-05.2 ← 2018-02-05.3
CS 579

$t(n)^2$ cells of $\{0,1\}^{\lceil \lg 2|\Gamma| \cdot Q \rceil}$ bits (constant)
- $O_{\Gamma,Q}(1)$ - size local update

input x = first config
output = last config
$\Rightarrow$ size $O_{\Gamma,Q}(t^2)$

Rmk: $t(n)$ time constructible $n \mapsto C_{M,n}$ computable in $O(\lg t(n))$ space
↳ uniform circuit ↳ counter

Cor: $P \subseteq P/poly$ [L = ? ??]

Thm: $P \not\subseteq P/poly$ [L ∈ TIME(2^{2^n}) \ TIME($2^{2^{2n}}$) yes L ∉ SIZE]

Pf: $L = \{ \underbrace{1^n}_{\text{one input per length}} : n \text{ in binary} = \langle M, x \rangle \text{ st } M \text{ halts on input } x \}$ [weird]
undecidable [weird]

Rmk: time hierarchy: $L \in TIME(2^{2n}) \setminus TIME(2^{o(2^n)})$, yet $L \in SIZE(O(n2^n))$

Q: ==

def: $a(n): \mathbb{N} \to \mathbb{N}$ advice length
$\mathcal{C}$ complexity class
$\mathcal{C}/a = \{ L : L' \in \mathcal{C}$ and $\alpha_1, \alpha_2, \ldots \in \{0,1\}^*$ s.t.
- $|\alpha_n| \le a(n)$
- $x \in L$ iff $\langle x, \alpha_{|x|} \rangle \in L' \}$

(advice ↙, class ↙)
Cor: $P/poly = P/poly$

Pf: $\subseteq$: $x \in L$ iff $\underbrace{\langle x, \alpha_{|x|} \rangle \in L'}_{\text{length } m \le poly(|x|)}$ iff $\underbrace{C_{L',m}(\langle x, \alpha_{|x|} \rangle) = 1}_{=: C_{L,|x|}(x)}$ ($L' \in P$)

$\supseteq$: $x \in L$ iff $C_{|x|}(x) = 1$ iff $\langle C_{|x|}, x \rangle \in CKT\text{-}VAL$ ($|C_{|x|}| \le poly(|x|)$)
$\{ \langle D, y \rangle : D(y) = 1 \} \in P$.

perspective: $P/poly$ = one advice string per input size, trusted advice
NP = one advice string per input, untrusted advice [requires verification]

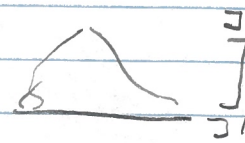
Q: $NP \subseteq P/poly$? [anything outside $P/poly$??]

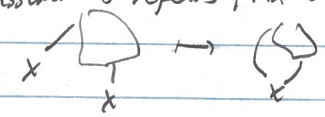
Prop: $\exists f : \{0,1\}^n \to \{0,1\}$ requires size $\Omega(2^n/n)$

Pf: nonconstructive counting argument
functions $f : \{0,1\}^n \to \{0,1\} = 2^{2^n}$
functions f of size $|f| \le s \le$?
$\le$ # ckts of size s

Michael Forbes
miforbes@illinois.edu

2018-02-05.2
2018-02-05.4 → 2018-02-05.3
CS579

Size S circuit = 

S gates, each gate - type: AND, OR, NOT (3 choices) ← wlog assume no repeats, via tensor 

- ≤ 2 children ← discard second child for NOT

$\leq S^2$ choices

output gate - order gates, output = last

choices: - leaves - 0 choices
- non leaves - $(3S^2)^S$

$\leq S^{O(S)}$ many circuits

$\Rightarrow$ if $S^{O(S)} < 2^{2^n}$ then $\exists f$ not of size $\leq S$

$\Rightarrow S = \varepsilon \frac{2^n}{n} \Rightarrow S^{O(S)} = \left(\frac{\varepsilon 2^n}{n}\right)^{O(\varepsilon 2^n/n)} \leq 2^{O(\varepsilon 2^n)} < 2^{2^n}$

$\varepsilon << 1$ ☒

Rmk: can view via probabilistic method $\Rightarrow$ 99% of all functions require $\Omega(2^n/n)$ size
∥ hay in haystack ∥

Cor [Circuit Size Hierarchy]: $S, t : \mathbb{N} \to \mathbb{N}$ $S(n) << t(n)$

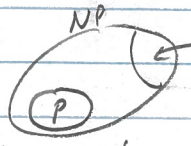
then $SIZE(S(n)) \subsetneq SIZE(t(n))$

Sketch: $\ell = \lg t(n)$

$\Rightarrow$ f function of ℓ bits $\Rightarrow f \in SIZE(\underbrace{O(\ell 2^\ell)}_{\leq t(n)})$

but: # functions ckt size $s(n)$ << # functions on ℓ bits

Question:

Recall: 

L NP-complete if - $L \in NP$
- $\forall A \in NP$ $A \leq L$

Saw: Bounded-Acceptance NP-complete

Thm [Cook-Levin]: 3SAT = $\{\langle \varphi \rangle : \varphi$ is satisfiable 3 CNF formula$\}$ is NP complete

Pf: CKT-SAT = $\{\langle C \rangle : C$ ckt on n bits, $\exists x \in \{0,1\}^n$ $C(x) = 1\}$ (SAT is a special case)

Claim: CKT-SAT NP-complete

Pf: $\in NP$: guess x, eval $C(x)$

NP-complete: $A \in NP$ $A = \{x : \exists y \in \{0,1\}^{p(n)}$ $\langle x, y \rangle \in A'\}$ ($A' \in P$)

$\langle x, y \rangle$ length $m \leq q(|x|)$

construct ckt $C_{A'}$ s.t. (in log space)
- $\langle x, y \rangle \in A'$ iff $C_{A'}(\langle x, y \rangle)$
- $|C_{A'}| \in poly(q(|x|)) \leq poly(|x|)$

Michael Forbes
miforbes@illinois.edu
2018-02-05.3 ⟸ 2018-02-05.4
CS579

now define $C_{A,x}(y) := C_{A'}(\langle x, y\rangle)$

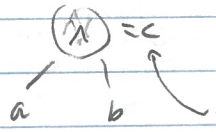
$x \in L$ iff $\exists y\ C_{A'}(\langle x,y\rangle)=1$ iff $\exists y\ C_{A,x}(y)=1$

CKT-SAT.

Claim: CKT-SAT $\leq$ 3SAT

Pf: idea: verify circuit locally

$C(x)=1$ iff - output $=1$
- input $= x$
- each gate is correct



is correct iff $c = a \wedge b$ iff $(a \vee \neg c) \wedge (b \vee \neg c) \wedge (\neg a \vee \neg b \vee c)$

$(a \vee \neg c) \equiv \neg a \Rightarrow \neg c$

$(b \vee \neg c) \equiv \neg b \Rightarrow \neg c$

$(\neg a \vee \neg b \vee c) \equiv a \wedge b \Rightarrow c$

size = gate + (2 children)

3CNF constraints

Circuit $C \mapsto$ 3CNF φ - vars x - inputs x, gates g

an input x ← poly-time computable

- clauses
- output $=1$
- computation checks (g_{out})

$\exists x\ C(x)=1$ iff $\exists x, g$ ← intermediate computations

- output $=1$
- each gate correct

$\varphi(x,g)=1$

Q: why 3SAT? 2SAT $\in P$

admin: ps 1 due

ps 2 out

next time: alternation