CS121 Lecture 6

Sept 19, 2019

Def: $f: \{0,1\}^n \to \{0,1\}^m$ is in $SIZE(s)$ if there exists a NAND-CIRC program of $\leq s$ lines that computes f.

$$SIZE_{n,m}(s) = \{ f : \{0,1\}^n \to \{0,1\}^m \mid f \in SIZE(s) \}$$

Q: What is the size of $\{f \mid f: \{0,1\}^3 \to \{0,1\}\}$?

$SIZE(f) = 2^8$

Q: What is the size of $\{f \mid f: \{0,1\}^n \to \{0,1\}\}$?

$SIZE(f) = 2^{(2^n)}$

Thm: $\forall$ s-line n-input NAND-CIRC program P, $\exists$ program P' s.t.

- P and P' equivalent: $P(x) = P'(x)$ for every $x \in \{0,1\}^n$
- All working variables in P' are of the form temp_i for $i \leq 3s$

Corollary: $\forall f \in SIZE(s)$ there is a NAND-CIRC program P' computing f whose code has $\leq O(s \log s)$ characters

s lines $\begin{cases} \overbrace{\text{temp\_}}^{5} \overbrace{\text{7254}}^{\log_{10}(85)} = \overbrace{\text{NAND(temp\_3241, temp\_1297)}}^{} \end{cases}$

Corr: $|SIZE(s)| \leq 128^{O(s \log s)} = 2^{O(s \log s)}$

$128^{c s \log s} \geq \left| \begin{array}{c} \text{ASCII strings of length} \\ \leq c s \log s \end{array} \right| \geq \left| \begin{array}{c} \text{programs of at} \\ \text{most } c s \log s \\ \text{characters} \end{array} \right| \geq |SIZE(s)|$

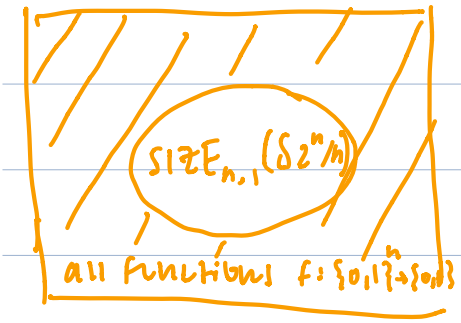
Theorem 2: Some functions $f: \{0,1\}^n \to \{0,1\}$ cannot be computed by circuits of size $o(2^n/n)$

Proof. Enough to prove for small enough $\delta > 0$,

$$|SIZE(\delta 2^n/n)| < |\{f \mid f: \{0,1\}^n \to \{0,1\}\}| = 2^{2^n}$$

$$|SIZE(\delta 2^n/n)| \leq 2^{\frac{c\delta \cdot 2^n \cdot \log(\delta 2^n/n)}{n}} \leq 2^{\frac{c\delta \cdot 2^n \cdot n}{n}} = 2^{c\delta 2^n}$$

which is $< 2^{2^n}$ if $\delta < \frac{1}{c}$ ∎



Define function $EVAL_{s,m,n}: \{0,1\}^{s+n} \to \{0,1\}^m$ s.t.

$EVAL(\text{repres of } P, x) = P(x)$

$EVAL_{s,m,n}$ gets:

- string of length s describing a program/circuit P w/ n inputs, m outputs, s lines
- input $x \in \{0,1\}^n$

returns eval of P on x

Thm 5.3: For every s, n, m there's a NAND-CIRC program $U_{s,m,n}$ to compute $EVAL_{s,m,n}$

NAND-CIRC interpreter in NAND-CIRC, bounded universal program

If P is a NAND-CIRC program, we can represent P as (n, m, L) where L is a list of s triples

"X: representation of

u: NAND(X[0], X[1])
v: NAND(X[0], u)
w: NAND(X[1], u)
Y[0]: NAND(v, w)

→ ((2, 0, 1), (3, 0, 2), (4, 1, 2), (5, 3, 4))

$EVAL_{s,m,n}(x) = P(x)$ when (n, m, L) represent P

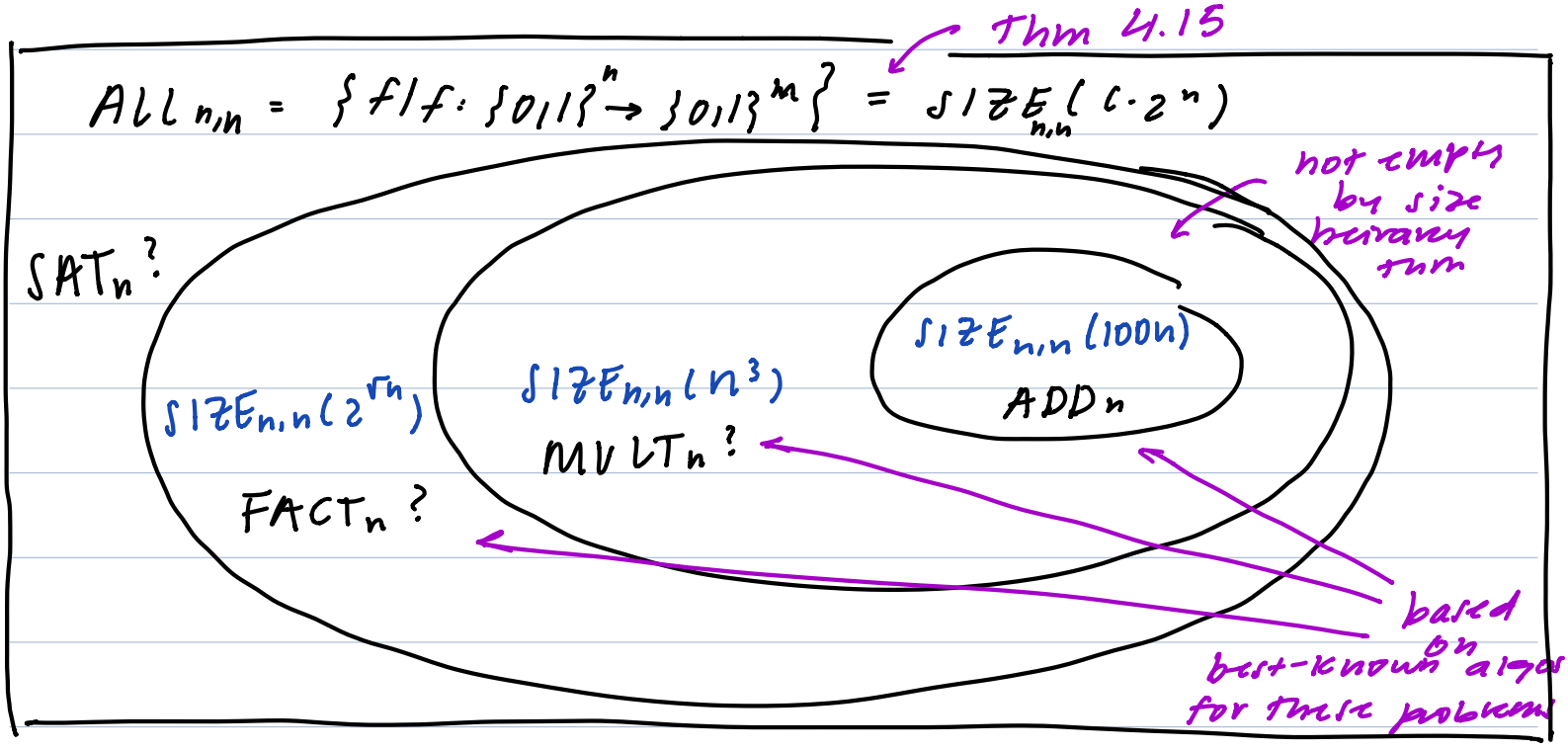
Thm 5.4: can compute $EVAL_{s,n,m}$ in $O(s^2 \log s)$ gates/lines

SIZE HEIRARCHY THRM

Thm 5.11: $\exists C$ (C = 1000 will do) s.t. $\forall \frac{2^n}{Cn}$,

$SIZE_{n,1}(s) \subsetneq SIZE_{n,1}(C \cdot s)$

Special case: $SIZE_{n,1}(n) \subsetneq SIZE_{n,1}(n^2)$



EXTENDED CHURCH TURING HYPOTHESIS (non uniform)

If $f: \{0,1\}^n \to \{0,1\}^m$ can be computed in the physical world using s resources then f can be computed by a circuit of $\approx s$ (eg $O(s^2)$ or $O(s^3)$) gates.

TLDR: so far stands. Only serious challenge is quantum computing