Exercise Sheet 9: Circuit Complexity

David Carral

January 15, 2020

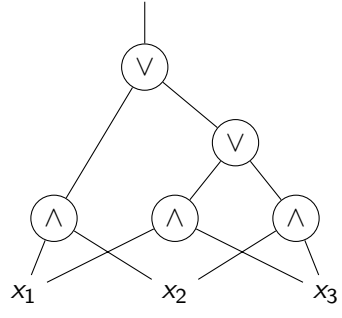
Exercise 1

Exercise. Define the function $\mathrm{maj}_n \colon \{0,1\}^n \to \{0,1\}$ by

$$\mathrm{maj}_n(x_1, \ldots, x_n) := \begin{cases} 0 & \text{if } \sum x_i < n/2 \\ 1 & \text{if } \sum x_i \geq n/2. \end{cases}$$

Devised a circuit to compute maj_3 and test it on the example input 101 and 010.

Solution. Consider the following circuit.



Exercise 2

Exercise. Denote with $\text{add}\colon \{0,1\}^{2n} \to \{0,1\}^{n+1}$ the function that takes two binary n-bit numbers x and y and returns their $n+1$-bit sum z. Show that add can be computed with circuits of size $\mathcal{O}(n)$.

Solution.

- Let $x = x_1, \ldots, x_n$, $y = y_1, \ldots, y_n$, and $z = z_1, \ldots z_n, z_{n+1}$.
- Let $c_0 = 0$; $z_{n+1} = c_n$; and, for all $i \in \{1, \ldots, n\}$, let

$$z_i = \big(x_i \oplus y_i\big) \oplus c_{i-1}, \text{ and}$$
$$c_i = \text{maj}_3(x_i, y_i, c_{i-1}).$$

  Note that $p \oplus q = (p \vee q) \wedge \neg(p \wedge q)$.
- Every full-adder contains a constant number of gates and hence, a chain of n such full-adders yields an $\mathcal{O}(n)$-size circuit.

Exercise 3

Exercise. Show $\mathrm{NC}^1 \subseteq \mathrm{L}$.

Definition 20.1: For $k \geq 0$, we define NC^k to be the class of all problems that can be solved by a circuit family $C = C_1, C_2, C_3, \ldots$ such that

- the depth of C_n is bounded by $O(\log^k n)$, and
- there is some $d \geq 0$ so that the size of C_n is bounded by $O(n^d)$ (in other words: $\mathsf{NC}^k \subseteq \mathsf{P}_{/\mathrm{poly}}$).

Solution.

- Let $\mathbf{L} \in \mathsf{NC}^1$.
- Then, there is some uniform circuit family of polynomial size $(C_n \mid n \in \mathbb{N})$ of polynomial size and $\mathcal{O}(\log n)$ depth that decides $\mathbf{L}$.
- Let $\mathcal{M}$ be the TM which, on input w with $|w|$, computes the circuit and the output of the circuit $C_{|w|}$ on w by doing a depth-first traversal of this circuit.
  - Remark 1: since the circuit can be computed in Łand $C_{|w|}$ is of logarithmic depth, the machine $\mathcal{M}$ only takes logarithmic space.
  - Remark 2: the composition of logspace computable reductions yields a logspace computable reduction.

Exercise 4

Exercise. Show that every Boolean function with n input variables can be computed with a circuit of size $\mathcal{O}(n \cdot 2^n)$.

Solution.

- Let $f : \{0,1\}^n \to \{0,1\}$.
- Let $D = \{(x_1, \ldots, x_n) \in \{0,1\}^n \mid f(x_1, \ldots, x_n) = 1\}$.
- Let C_n be the following circuit:
  - For every $t = (x_1, \ldots, x_n) \in D$, let E_t be a circuit that with n inputs that outputs 1 on input $(x_1, \ldots, x_n)$, and 0 otherwise. Discuss: construction, size, and depth.
  - Then, C_n is the circuit that outputs 1 on input w if and only if some input E_t outputs 1 on w. Discuss: construction, size, and depth.

Exercise 5

Exercise. Show that every language $L \subseteq \{ 1^n \mid n \in \mathbb{N} \}$ is contained in P/poly. Conclude that P/poly contains undecidable languages.

A natural class of problems to consider are those that have polynomial circuit families:

Definition 18.11: $\mathsf{P}_{/\mathrm{poly}} = \bigcup_{d \geq 1} \mathsf{Size}(n^d)$.

Note: A language is in $\mathsf{P}_{/\mathrm{poly}}$ if it is solved by some polynomial-sized circuit family. There may not be a way to compute (or even finitely represent) this family.

Solution.

1. Let $\mathbf{L} \subseteq \{1^n \mid n \in \mathbb{N}\}$. Then, for all $i \geq 1$, let $C_n(x_1, \ldots, x_n) = x_1 \wedge \ldots \wedge x_n$ if $1^n \in \mathbf{L}$, and $C_n(x_1, \ldots, x_n) = x_1 \wedge \neg x_1$ otherwise.
2. *Discuss*: The circuit family defined in (1) is of polynomial size and decides $\mathbf{L}$.
3. By (2): every language $\mathbf{A} \subseteq \{1^n \mid n \in \mathbb{N}\}$ is in P/poly.
4. *Discuss:* Some of the languages that are subsets of $\{1^n \mid n \in \mathbb{N}\}$ are undecidable.
5. By (3) and (4): the class P/poly contains undecidable languages.

Exercise 6

Exercise. Find a decidable language in P/POLY that is not contained in P.
Hint: take a $2\mathrm{EXPTIME}$-hard language over $\{0,1\}$ and consider its unary encoding.

From $\mathrm{DTime}(f) \subseteq \mathrm{Size}(f^2)$ we get:

Corollary 18.13: $\mathsf{P} \subseteq \mathsf{P}_{/\mathrm{poly}}$.

Solution.

- Let $\mathbf{L}$ be some $2\mathrm{EXPTIME}$-hard problem (e.g., the word problem of an exponential space TM) defined over the alphabet $\{0,1\}$.
- Let $\mathbf{L}'$ be the unary encoding of $\mathbf{L}$; that is, $\mathbf{L}' = \{1^n \mid n \in L\}$.
- Suppose for a contradiction that $\mathbf{L}' \in \mathsf{P}$.
- Then, $\mathbf{L} \in \mathrm{EXPTIME}$: to decide if a word $w \in \{0,1\}^*$ is in $\mathbf{L}$, we first encode w in unary and check whether this encoding is in $\mathbf{L}'$. This yields an $\mathrm{EXPTIME}$-procedure and hence, $\mathbf{L} \in \mathrm{EXPTIME}$.
- Since $\mathbf{L}$ is $2\mathrm{EXPTIME}$-hard we conclude that $2\mathrm{EXPTIME} \subseteq \mathrm{EXPTIME}$, contradicting the Time Hierarchy Theorem.

Exercise 7

Exercise. Show how to compute maj_n with circuits of size $\mathcal{O}(n \log n)$.

Solution.

- The first stage consists of an adder-tree of depth $\mathcal{O}(\log n)$ that adds together the n input bits. The size of this tree is $\mathcal{O}(n \log n)$.
- The $1 + \log n$ output bits of this tree are then fed into circuits for the functions

$$E_{n/2+1}^{\log n+1}(x_1, \ldots, x_{\log n+1}), \ldots, E_n^{\log n+1}(x_1, \ldots, x_{\log n+1}) \tag{1}$$

  where, for $i \in \{1, \ldots, 2n-1\}$, the circuit $E_i^{\log n+1}(x_1, \ldots, x_{\log n+1})$ outputs 1 if and only if the number represented by its input is equal to i. This can be done using NOT and AND-gates with a circuit of size $\mathcal{O}(\log n)$.
- Finally, the results of the circuits for the functions in (1) are combined with an OR-tree of size $\mathcal{O}(n)$ and depth $\mathcal{O}(\log n)$.
- Therefore, the whole circuit has size $\mathcal{O}(n \log n + n \log n + n) = \mathcal{O}(n \log n)$.

Exercise 8

Exercise. Show that $\mathrm{NC} \neq \mathrm{PSPACE}$.

Solution.

- If $\mathbf{L} \in \mathrm{NC}$, then $\mathbf{L} \in \mathrm{NC}^k$ for some k.
- That is $\mathbf{L}$ can be solved using a circuit family $C = C_1, C_2, \ldots$ such that, for all $i \geq 1$, the depth of C_i is bounded by $\mathcal{O}(\log^k n)$.
- Hence, $\mathbf{L}$ can be solved using a $\mathcal{O}(\log^k n)$-space bounded Turing machine.

Space Hierarchy Theorem 13.1: If $f, g : \mathbb{N} \to \mathbb{N}$ are such that f is space-constructible, and $g \in o(f)$, then

$$\mathrm{DSpace}(g) \subsetneq \mathrm{DSpace}(f)$$

- Indeed, $\log^k n \in o(n)$.
- `https://math.stackexchange.com/questions/1625701/how-do-i-use-lhopitals-rule-to-determine-if-logkn-is-on-for-any-consta`