Computational Complexity — tutorial 7

Boolean circuits 2

Quick reminder: We define the following complexity classes for $k \in \{0, 1, 2, \dots\}$:

- AC^k: problems which can be solved by circuits with polynomial size and depth at most $O(\log^k n)$ where n is the number of inputs.
- NC^k: same as AC^k, but all gates have **at most** 2 **inputs** (have fan-in $\leqslant 2$).

$$\mathsf{AC} = \mathsf{AC}^0 \cup \mathsf{AC}^1 \cup \mathsf{AC}^2 \cup \mathsf{AC}^3 \cup \dots, \qquad \mathsf{NC} = \mathsf{NC}^0 \cup \mathsf{NC}^1 \cup \mathsf{NC}^2 \cup \mathsf{NC}^3 \cup \dots$$

Uniform classes (u-AC^k, u-AC, u-NC^k, u-NC): problems solved by circuits which can be generated in logarithmic space.

[Furst, Saxe, Sipser 1984] The Parity problem (given n inputs, decide if an odd number of them is true) is **not** in AC^0. *It's obviously in NC^1 (and in u-NC^1).*

Consider the Multiplication problem: given two n-bit numbers, compute their product.

1. Prove that Multiplication is in AC^1.

2. Prove that Multiplication is in NC^1.
Hint: define a function add3to2 *mapping triples of integers (x, y, z) into pairs of integers (x', y') such that $x + y + z = x' + y'$. Can it be implemented in constant depth using only unary and binary gates?*

3. Prove that Multiplication is not in AC^0.
Hint: solve Parity *using* Multiplication *as a black-box.*

We consider the relations between the regular languages and circuit complexity classes.

4. Prove that there exists a regular language not in AC^0.

5. Prove that there exists a language in AC^0 which is not regular.

6. Prove that all regular languages are in NC^1 (even in u-NC^1).

Consider the Majority problem: given n bits (n odd), which bit (0/1) occurs more frequently?

7. Construct a circuit solving Majority of size $O(n)$ and depth $O(\log n)$, using only unary and binary gates. Note that this implies that Majority $\in \mathsf{NC}^1$.

8. Prove that Majority is not in AC^0. *Hint: solve* Parity *using* Majority *as a black-box.*

We consider the relations between the uniform circuit complexity classes and log-space classes.

9. Prove that u-$\mathsf{NC}^1 \subseteq$ LogSpace.

10. Prove that NLogSpace $\subseteq$ u-AC^1.