CS538, Spring 1998
Script for Lecture on 2/25/98
by Ali Shokoufandeh

We start with introducing three complexity classes of languages which are of particular importance in circuit complexity;

- $\mathbf{TC}^k$
  The class of languages recognizable by a Dlogtime-uniform circuit family of Size($n^{O(1)}$), with Depth($O(\log^k n)$), using **Majority** and $\neg$ gates[1].
- $\mathbf{AC}^k$
  The class of languages recognizable by a Dlogtime-uniform circuit family of Size($n^{O(1)}$), with Depth($O(\log^k n)$), using unbounded fan-in $\wedge$, $\vee$, and $\neg$ gates.
- $\mathbf{NC}^k$
  The class of languages recognizable by a Dlogtime-uniform circuit family of Size($n^{O(1)}$), with Depth($O(\log^k n)$), using bounded fan-in $\wedge$, $\vee$, and $\neg$ gates.

Among these, the class NC^0 (polynomial size, constant depth, with bounded fan-in gates) have the least importance, since the output gate can only depend on a constant number of inputs, and having constant depth, the output gate is not able to check all the inputs (even a simple function like $\mathbf{AND}(x_1, ..., x_n)$ can not be implemented in this model). The general hierarchy among the rest of the complexity classes is shown in figure 1 (The class **NC** is defined as $\cup_k \mathrm{NC}^k$). In what follows, inclusions of the classes TC^k in NC^{k+1}

Figure 1: The hierarchy of complexity classes involving circuits.

will be justified, the rest of the inclusions in this hierarchy are left to the reader:

Theorem 1 *For all* k, $\mathrm{TC}^k \subseteq \mathrm{NC}^{k+1}$.

[1] **Majority** is an unbounded fan-in gate, and for the input $x_1, ..., x_n$

$$\mathbf{Majority}(x_1, ..., x_n) = \begin{cases} 1 & \text{if } \sum_i x_i \geq n/2, \\ 0 & \text{Otherwise.} \end{cases}$$

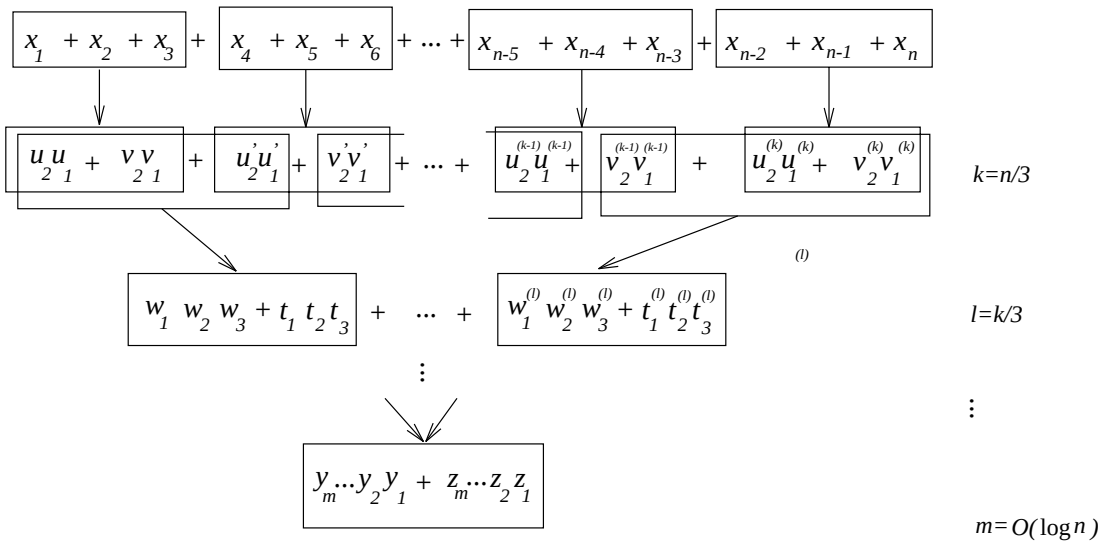

Figure 2: Reduction of **Majority** to an NC^1 circuit.

Proof. It is sufficient to show that the **Majority** gate is in NC^1, since if in a TC^k circuit, each **Majority** gate is replaced by an NC^1 circuit, the resulting circuit will be a Dlogtime-uniform circuit of Size($n^{O(1)}$), which is built using bounded fan-in $\wedge$, $\vee$, and $\neg$ gates, and has depth $O(\log^{k+1} n)$.
In order to show **Majority**$(x_1, ..., x_n) \in \mathrm{NC}^1$, we need to compute the sum of the bits $x_1, ..., x_n$. (Using the usual divide and conquer method to carry out this addition will not result in a Depth($O(\log n)$) circuit.)
Observe that adding three b-bit numbers $< x_b, ..., x_1 >$, $< y_b, ..., y_1 >$, and $< z_b, ..., z_1 >$ can be reduced to adding two $b+1$-bit numbers, $< u_{b+1}, ..., u_1 >$ and $< v_{b+1}, ..., v_1 >$, defined as follows:

$$\begin{cases} u_i = \text{Parity}(x_i, y_i, z_i), & 1 \le i \le b, \\ u_{b+1} = 0, & \\ v_1 = 0, & \\ v_{i+1} = \text{Majority}(x_i, y_i, z_i), & 1 \le i \le b. \end{cases}$$

It is easy to see that Parity(x_i, y_i, z_i) and Majority(x_i, y_i, z_i) can be implemented with constant depth circuits.
Getting back to the original problem of computing the summation of the bits $x_1, x_2, ..., x_n$, we can start grouping the bits into sets of size 3, $\{x_1, x_2, x_3\}, ..., \{x_{n-2}, x_{n-1}, x_n\}$ (W.L.O.G assume $n = 3k$). By the previous observation the summation of the bits in each group $\{x, y, z\}$ can be replaced by the sum of two, two bit numbers $\{< v_2 v_1, u_2 u_1 >\}$. As a result of this reduction, the total number of additions required to compute the original sum will be reduced by a factor of $\frac{2}{3}$. Repeating the same procedure for $O(\log n)$ steps will reduce the original problem to the problem of adding two $O(\log n)$-bits numbers (see Figure 2). Up to this point we have only used $O(\log n)$ gates to compute the **Majority**. It remains to show that the final two numbers $< y_m ... y_2 y_1 >$ and $< z_m ... z_2 z_1 >$ can be added using a circuit in NC^1. To this ends, we will show that using an AC^0 circuit, this last sum can be easily computed. Let $< \sigma_{m+1} ... \sigma_2 \sigma_1 >$ denote the summand of $< y_m ... y_2 y_1 >$ and $< z_m ... z_2 z_1 >$ and c_i denote the i^{th} carry bit, then the following relations hold

$$\begin{cases} c_0 = 0 & \\ c_i = \bigvee_{j \le i} \left[(y_j \wedge z_j) \bigwedge_{j \le k \le i} (y_k \vee z_k) \right], & 1 \le i \le m, \\ \sigma_i = c_{i-1} \oplus y_i \oplus z_i, & 1 \le i \le m, \\ \sigma_{m+1} = c_m. & \end{cases}$$

Observe that, using bounded fan-in gates to compute c_i's and σ_i's will increase the depth of the circuit by

a multiplicative factor of $O(\log n)$. Define$\sigma =< \sigma_{m+1}...\sigma_2\sigma_1 >$, $p = 2^{\lceil \log n \rceil - 1} - \frac{n}{2}$ and form $s = \overbrace{11...1}^{p}$ (the string of p padded 1's). It can be shown that; **Majority**$(x_1, x_2, ..., x_n) = 1$ if and only if $\sigma + s \geq 2^{\lceil \log n \rceil - 1}$. Finally, by using an AC^0 circuit which verifies the last bit of the summand $\sigma + s$, the value of **Majority** can be determined.□