CIS 511: Theory of Computation **Apr 18, 2017**

Lecture 24: Circuit Complexity

Professor Sampath Kannan *Zach Schutzman*

NB: *These notes are from CIS511 at Penn. The course followed Michael Sipser's Introduction to the Theory of Computation (3ed) text.*

Parallel Computation

Definition 24.1 *The **Parallel Random Access Model** (PRAM) is a model with synchronous processes with shared memory. Each process can read one cell, perform a computation, and write one cell at each step, synchronously.*

Definition 24.2 *The **Circuit Model** is a model where each gate is considered to be a processor.*

Definition 24.3 *A **bounded fan-in (fan-out)** model is one in which we limit the fan-in (fan-out) of any gate to be at most some constant.*

We can convert unbounded fan-in AND and OR gates into bounded ones by replacing it with a tree of sufficient depth.

Claim 24.4 *Circuits where all gates have fan-out* 1 *can be thought of as equivalent to formulas.*

We can see this by observing that fan-out of 1 *makes the circuit a tree. We can then recursively build the formula by considering left and right subtrees separately.*

The formula for a circuit with fan-out greater than 1 *is exponentially big.*

When considering computation of circuits, there are two parameters we are interested in: the size (number of gates), and the depth (length of the longest path from input to output).

Circuits have a fixed number of inputs. How can they recognize arbitrary languages?

Definition 24.5 *A **(non-uniform) circuit family** C is a collection of circuits $C_1, C_2 \dots$ where we use circuit C_i to compute things on inputs of length i.*

Defined this way, we can define a C which computes the Halting Problem. This is not ideal.

Definition 24.6 *A **uniform circuit family** is a collection of circuits C such that there exists a Turing machine M which runs in log-space which on input 1^n, outputs the circuit C_n.*

Now that we stipulate that it is computable by a log-space transducer, we no longer are able to generate a family of circuits to solve the Halting Problem.

We'll look at simultaneous size-depth bounds (as a function of n) on uniform circuit families. We want $size(n)$ to be at most polynomial and $depth(n)$ to be polylogarithmic ($log^k(n)$).

Definition 24.7 *The class NC^i, for $i \in \mathbb{N}$ is the set of languages recognized by uniform circuit families of size polynomial in n and depth $log^i(n)$.*

Example: *The problem of boolean matrix multiplication is like regular matrix multiplication but the entries are boolean values, we replace elementwise multiplication by AND and addition by OR. This can be done in NC^1, as we can design a circuit with $O(n^3)$ gates and $log(n)$ depth to compute this.*

This problem (using adjacency matrices) can tell us whether two vertices in a graph are connected by a path of length 2.

Example: *The transitive closure of a directed graph, $TC(G)$ is a graph G' such that there is an edge from i to j in G' if and only if there is a path from i to j in G. This captures all of the reachability information of G. We can compute this by taking A to be the adjacency matrix of G and computing $(I + A)^n$, where n is the number of vertices in G. We need size n and depth 1 to do the addition, then $log(n)$ multiplications of size n^3 and depth $log(n)$. In total, we have depth $log^2(n)$ and size $n^3 log(n)$. Therefore, transitive closure is in NC^2.*

Claim 24.8 *$NC^1 \subseteq L \subseteq NL \subseteq NC^2$.*

Proof: *$L \subseteq NL$ is trivial, we've just proven that $NL \subseteq NC^2$ because TC allows us to compute $PATH$, so $PATH \in NC^2$. We also know $NC^1 \subseteq NC^2$. We just need to show that $NC^1 \subseteq L$.*

An NC^1 circuit is a polynomial circuit with depth $log(n)$ and polynomial size which is computed by a log-space transducer.

Let A be a language in NC^1. We will give an algorithm M in L to compute A. On input w first counts the length of w equal to n. It then uses the transducer which generates the circuit family to construct the nth circuit C_n, then recursively evaluates the circuit on input w, starting with the output. Since the circuit is log-depth, the recursion can be computed by a machine which only remembers one bit at each level to remember the path and one bit for the previous result, if it exists for a total of $2log(n)$ bits. Hence $NC^1 \subseteq L$. ■

We also have $NC \subseteq P$.