# COMPSCI 501: Formal Language Theory

Lecture 32: Circuits and Parallelism

Marius Minea
marius@cs.umass.edu

University of Massachusetts Amherst

12 April 2019

## Review: Circuits families and complexity

Circuits are fixed-size $\Longrightarrow$ family of circuits, one per input length

*Def.* A **circuit family** $C$ is an infinite list of circuits, $(C_0, C_1, C_2, \ldots)$, where $C_n$ has $n$ input variables.

$C$ decides a language $A$ over $\{0, 1\}$ if for every string $w$, $w \in A$ iff $C_n(w) = 1$. $(n = |w|)$

Can define:

- *size*, *size-minimal* circuits (no smaller equivalent)
- *size complexity* of a family: $f : \mathbb{N} \to \mathbb{N}$, $f(n) = size(C_n)$
- *depth*, *depth minimal*, *depth complexity* (measure of *parallel time complexity*)

*Circuit complexity of a language* = size complexity of minimal circuit family

## Parallelism: Processor vs. circuit models

*Parallel Random Access Machine* (PRAM):
many (simple) processors simultaneousy access shared memory
with various forms of conflict resolution

Again, PRAM model handles *all input lengths*
For circuits: need to easily obtain entire family

*Def.* A family of circuits $\langle C_0, C_1, \ldots C_n \rangle$ is **uniform**
if some log-space transducer outputs $\langle C_n \rangle$ when input is $1^n$.

**Simultaneous size-depth** circuit complexity $(f(n), g(n))$ if:
size complexity $f(n)$
depth complexity $g(n)$

Why *simultaneous* ?

## Examples: poly size, poly-log depth

Insight: can often group circuits in **binary tree**

**Parity**: $[x_1 \oplus ... \oplus x_{n_2}] \oplus [x_{n/2+1} \oplus \ldots \oplus x_n]$
size-depth: $(O(n), O(\log n))$

**Boolean matrix multiplication**: $c_ik = \bigvee_j (a_{ij} \wedge b_{jk})$
binary tree for the OR
$m^3$ AND gates, $m^3$ OR gates, input size $n = O(m^2)$
size-depth $(O(n^{3/2}), O(\log n))$

**Transitive closure**: $A \vee A^2 \vee \ldots \vee A^m$ for matrix
path of up to $m$ edges $\Longrightarrow$ pairwise connectivity
circuit for $A \vee A^2$: size-depth $(O(n^{3/2}), O(\log n))$
repeated squaring $A \vee \ldots \vee A^4$, etc.
$O(\log n)$ levels of squaring (multiplication with same inputs)
size-depth $(O(n^{3/2} \log n), O(\log^2(n)))$

## The Class NC

*Def.* **NC**$^i$ $(i \geq 1)$ is the class of languages that can be decided by a uniform family of circuits with polynomial size and $O(\log^i n)$ depth.

**NC** is the class of languages that are in NC$^i$ for some $i$.

Functions implemented by such circuits are NC$^i$ computable.

Other circuit models (brief mention):

AC$^i$: like NC, but gates have unlimited fan-in (inputs).
TC$^i$: like AC, and also *majority* gates ("threshold circuits").

Can prove (not here): **NC**$^i \subseteq$ **AC**$^i \subseteq$ **TC**$^i \subseteq$ **NC**$^{i+1}$

## Where is NC in hierarchy?

*Theorem*: **NC** $\subseteq$ **P**

Do in poly-time:
1) generate circuit $C_n$
2) evaluate on $w$ $(|w| = n)$

*Theorem*: **NC**$^1 \subseteq$ **L**

Can we evaluate a NC$^1$ circuit in log space?

1. Construct circuit: doable with log-space transducer (by def.)
2. Evaluate circuit: recursively, from output (DFS)
   need stack (path): ok, since circuit only has depth $O(\log n)$

Next: bound in the other direction: **NL** $\subseteq$ **NC**$^2$

## NL $\subseteq$ NC$^2$

Nondeterminism $\implies$ must evaluate *all* paths
$\implies$ construct (closure of) *transition relation*

From NL machine $M$, construct configuration graph $G$ of $M$:
edge for any $c_1 \to c_2$.

A configuration has log space $\implies$ polynomially many

Condition edge $(c_1, c_2)$ on legal values of cell read by head
0 or 1 (or both)

Can compute path relation (transitive closure of $G$'s edge relation) by poly-size circuit of $O(\log^2 n)$ depth

Construction doable in log space (see proof that *PATH* is NL-hard)

## P-completeness

*Def.* A language $B$ is **P-complete** if

1. $B \in$ P and
2. every language in P is log space reducible to B

If $A \leq_L B$ and $B$ is in NC, then $A$ is in NC.

*CIRCUIT-VALUE* problem = evaluating a circuit on its input
$\{\langle C, x\rangle \mid C$ is a circuit and $C(x) = 1\}$.

*CIRCUIT-VALUE* is P-complete

For a TM taking $t(n)$ steps, we've constructed an $O(t^2(n))$ circuit
Construction is repetitive (encode next symbol for each cell)
and can be done in log space.