Complexity Theory
Circuits and Parallel Computation

Daniel Borchmann, Markus Krötzsch

Computational Logic

2016-01-19

©️ 2015 Daniel Borchmann, Markus Krötzsch

Complexity Theory

©️ 2016-01-19 #1
Review
Modelling Parallelism With Circuits
What is Efficiently Parallelisable?

Experience suggests: some problems can be solved efficiently in parallel, while others can not.

How could this be shown?

Intuitive definition:
A problem has an **efficient parallel algorithm** if it can be solved for inputs of size \( n \)

- in polylogarithmic time, i.e., in time \( O(\log^k n) \) for some \( k \geq 0 \),
- using a computer with a polynomial number of parallel processors, i.e., \( O(n^d) \) processors for some \( d \geq 0 \).
What is Efficiently Parallelisable?

Experience suggests: some problems can be solved efficiently in parallel, while others cannot.

How could this be shown?

Intuitive definition:
A problem has an efficient parallel algorithm if it can be solved for inputs of size $n$

- in polylogarithmic time, i.e., in time $O(\log^k n)$ for some $k \geq 0$,
- using a computer with a polynomial number of parallel processors, i.e., $O(n^d)$ processors for some $d \geq 0$.

Note: Using $O(n^d)$ processors efficiently requires a massively parallel algorithm. However, one could always use fewer processors (each taking on more work), possibly leading to a proportional increase in time.

The hard bit in parallelisation is to utilise many processors effectively – reducing to fewer processors is easy.
Modelling Parallel Computation

What kind of “parallel computer” do we mean here?

(1) How do processors communicate?
(2) What can a processor do in one step?
(3) How are processors synchronized?

Detailed answer: define Parallel Random Access Machine (PRAM)
Modelling Parallel Computation

What kind of “parallel computer” do we mean here?

1. How do processors communicate?
2. What can a processor do in one step?
3. How are processors synchronized?

**Detailed answer:** define Parallel Random Access Machine (PRAM)

**Our answer:**
Details are not critical as long as we can make some general assumptions:

1. Every processor can send a message to any other processor in $O(\log n)$ time
2. In one step, each processors can perform one Boolean operation on “a few” bits, say $O(\log n)$
3. Processor steps are synched with a global clock
Modelling Parallel Computation in Circuits

Simple PRAM computations can be mapped to Boolean circuits (with some extra circuitry for executing more operations or for modelling message passing)

Circuits as models for parallel computation:

- circuit gates can operate in parallel – they only depend on their inputs
- the time needed to evaluate a circuit depends on its depth, not size (depth = longest distance from an input to an output node)
Example: Generalised AND

The function that tests if all inputs are 1 can be encoded by combining binary AND gates:

- size: $2n - 1$
- depth: $\log_2 n$
Small-Depth Circuits

Small depth = short (parallel) time

However: Every Boolean function can be computed by depth $O(\log n)$ circuits using $O(n2^n)$ gates (exercise)

Hence, to capture “efficient parallel computation”, we also restrict the size:

**Definition 18.1**

For $k \geq 0$, we define $\text{NC}^k$ 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 $O(\log^kn)$, and
- there is some $d \geq 0$ so that the size of $C_n$ is bounded by $O(n^d)$

(in other words: $C \in \text{P}/\text{poly}$).

($\text{NC}$ is for “Nick’s class”, named in honour of Nicholas Pippenger, who studied such circuits, by Stephen Cook.)
Alternating Circuits

Different complexity classes are obtained when allowing generalised Boolean gates with many inputs:

Definition 18.2

An AND gate with unbounded fan-in is a gate that computes a generalised AND function over an arbitrary number $n \geq 2$ of inputs. OR gates with unbounded fan-in are defined similarly.

For $k \geq 0$, we define $\text{AC}^k$ exactly like $\text{NC}^k$ but allowing circuits to use gates with unbounded fan-in.

Example 18.3

Generalised AND is in $\text{NC}^1$ and in $\text{AC}^0$. 
The **NC Hierarchy**

The classes $\text{NC}^k$ and $\text{AC}^k$ form a hierarchy:

- if $i \leq j$ then $\text{NC}^i \subseteq \text{NC}^j$ (obvious)
- if $i \leq j$ then $\text{AC}^i \subseteq \text{AC}^j$ (obvious)
- $\text{NC}^i \subseteq \text{AC}^i$ (obvious)
- $\text{AC}^i \subseteq \text{NC}^{i+1}$ (since generalised AND and OR can be replaced with $O(\log n)$ bounded fan-in gates as in our example)
The NC Hierarchy

The classes $\text{NC}^k$ and $\text{AC}^k$ form a hierarchy:

- if $i \leq j$ then $\text{NC}^i \subseteq \text{NC}^j$ (obvious)
- if $i \leq j$ then $\text{AC}^i \subseteq \text{AC}^j$ (obvious)
- $\text{NC}^i \subseteq \text{AC}^i$ (obvious)
- $\text{AC}^i \subseteq \text{NC}^{i+1}$ (since generalised AND and OR can be replaced with $O(\log n)$ bounded fan-in gates as in our example)

The limit of this hierarchy is defined as $\text{NC} = \bigcup_{k \geq 0} \text{NC}^k$ so we get:

$$\text{AC}^0 \subseteq \text{NC}^1 \subseteq \text{AC}^1 \subseteq \cdots \subseteq \text{NC}^k \subseteq \text{AC}^k \subseteq \text{NC}^{k+1} \subseteq \cdots \text{NC}$$

Note: $\text{NC}^0$ is not a very useful class, as those circuits cannot process the whole input.
Uniform vs. Non-uniform

Recall: A circuit family is uniform if it can be computed by a (restricted form of) Turing machine.

- Our definitions of $\text{NC}^k$ and $\text{AC}^k$ do not require uniformity.
- It is common to define uniform $\text{NC}^k$ and uniform $\text{AC}^k$ using logspace-uniformity (or even more restricted forms of uniformity).
- Clearly: uniform $\text{NC}^k \subseteq \text{NC}^k$ and uniform $\text{AC}^k \subseteq \text{AC}^k$.

Convention: For the rest of this lecture, we restrict to (logspace) uniform versions of $\text{NC}^k$ and $\text{AC}^k$. 
Example: \textit{Parity} is in $\textbf{NC}1$
Example: \textsc{Parity} is in $\text{NC}^1$

However, we also have the following major result (without proof):

Theorem 18.4 (see Arora/Barak, Chapter 14)

\textsc{Parity} is not in $\text{AC}^0$, and therefore $\text{AC}^0 \subsetneq \text{NC}^1$. 
Example: FOL model checking

**FOL Model Checking**

*Input:* First-order sentence $\varphi$; finite first-order structure $\mathcal{I}$

*Problem:* Is $\varphi$ satisfied by $\mathcal{I}$?

We showed that this problem is $\text{PSPACE}$-complete. It turns out that this complexity is caused by the formula, not by the model:

**FOL Model Checking for $\varphi$**

*Input:* A finite first-order structure $\mathcal{I}$.

*Problem:* Is $\varphi$ satisfied by $\mathcal{I}$?

Theorem 18.5 (see course Database Theory, Summer 2016, TU Dresden)

*For any first-order sentence $\varphi$, FOL Model Checking for $\varphi$ is in $\text{AC}^0$.*
Using the assumption of uniformity, we can solve circuit complexity problems by (1) computing the circuit and (2) evaluating it.

The following are not hard to show:

**Theorem 18.6 (Sipser, Theorem 10.41)**

\[ \text{NC} \subseteq \text{P} \]

**Theorem 18.7 (Sipser, Theorem 10.39)**

\[ \text{NC}^1 \subseteq \text{L} \]
Relationships to Other Complexity Classes (2)

Conversely, some known classes are also subsumed by $\text{NC}$:

**Theorem 18.8**

$\text{NL} \subseteq \text{AC}^1$

**Proof notes.**

General proof idea: (1) construct a “generalised” configuration graph for an $\text{NL}$ machine (a graph that describes all possible configuration graphs using transitions that depend on the actual input that is given); (2) check reachability of the goal state in this graph (basically by repeated matrix multiplication in the reachability matrix).

We do not give a proof here. Sipser (Theorem 10.40) sketches the proof for $\text{NL} \subseteq \text{NC}^2$; the proof for $\text{NL} \subseteq \text{AC}^1$ is the same but also uses that the depth is only logarithmic if we can use unbounded fan-in gates. □
Conversely, some known classes are also subsumed by $\text{NC}$:

**Theorem 18.8**

$\text{NL} \subseteq \text{AC}^1$

**Proof notes.**

General proof idea: (1) construct a “generalised” configuration graph for an $\text{NL}$ machine (a graph that describes all possible configuration graphs using transitions that depend on the actual input that is given); (2) check reachability of the goal state in this graph (basically by repeated matrix multiplication in the reachability matrix).

We do not give a proof here. Sipser (Theorem 10.40) sketches the proof for $\text{NL} \subseteq \text{NC}^2$; the proof for $\text{NL} \subseteq \text{AC}^1$ is the same but also uses that the depth is only logarithmic if we can use unbounded fan-in gates.

We therefore obtain the following picture:

$$\text{AC}^0 \subset \text{NC}^1 \subset L \subset \text{NL} \subset \text{AC}^1 \subset \text{NC}^2 \subset \cdots \quad \text{NC} \subset \text{P}$$
P-Completeness
The Limits of Parallel Computation

\( \text{NC} \) defines a hierarchy of efficiently parallelisable problems in \( \text{P} \)

Are all problems in \( \text{P} \) efficiently parallelisable?
The Limits of Parallel Computation

NC defines a hierarchy of efficiently parallelisable problems in $P$

Are all problems in $P$ efficiently parallelisable?
Nobody knows

State of the art:
- It is not known if $NC \neq P$ or not
- It is not even known if $NC^1 \neq PH$ or not
- It is clear that $AC^0 \neq P$ (since $AC^0 \subset NC^1$)
- It is clear that $NC \neq PSPACE$ (exercise: why?)

“Most experts believe that” $NC \neq P$
$\leadsto$ if this is true, then some problems in $P$ cannot be parallelised efficiently
P-Complete Problems

Recall the definition from Lecture 15:

**Definition 12.9**
A problem $L \in \mathbf{P}$ is complete for $\mathbf{P}$ if every other language in $\mathbf{P}$ is log-space reducible to $L$.

If $\mathbf{NC} \neq \mathbf{P}$ then $\mathbf{P}$-complete problems are tractable but not efficiently parallelisable and therefore inherently serial.
Circuit Evaluation is \( \mathsf{P} \)-complete

**Circuit Value**

*Input:* A Boolean Circuit \( C \) with one output, and an input word \( w \in \{0, 1\}^n \)

*Problem:* Does \( C \) return 1 on this input?

**Theorem 18.9**

*Circuit Value* is \( \mathsf{P} \)-complete.

**Proof.**

Membership is easy. For completeness, we reduce the word problem of polynomially time-bounded Turing machines. A circuit for this problem was constructed in the previous lecture for Theorem 17.7. This circuit family is logspace-uniform (as already remarked in Theorem 17.13), so we get a logspace-reduction.
Propositional Horn Logic

A problem that is closer to artificial intelligence:

- A propositional fact is a formula consisting of a single propositional variable $X$
- A propositional Horn rule is a formula of the form $X_1 \land X_2 \rightarrow X_3$
- A propositional Horn theory is a set of propositional Horn rules and facts

The semantics of propositional Horn theories is defined as usual for propositional logic.

**Prop Horn Entailment**

*Input:* A propositional Horn theory $T$ and a propositional variable $X$

*Problem:* Does $T$ entail $X$ to be true?
**Propositional Horn Logic is \( \mathcal{P} \)-Complete**

**Theorem 18.10**

\( \text{PROP HORN ENTAILMENT is} \ \mathcal{P} \text{-complete.} \)

**Proof sketch.**

One can give a direct Turing machine encoding:

- We use propositional variables to represent configurations as for Cook-Levin
- We encode TM behaviour directly, e.g., for transitions \( \langle q, \sigma \rangle \mapsto \langle q', \sigma', d \rangle \) we can use rules like \( Q_{q,t} \land P_{i,t} \land S_{i,\sigma,t} \rightarrow Q_{q',t+1} \land P_{i+d,t+1} \land S_{i,\sigma',t+1} \) (for all times \( t \) and positions \( i \))
- We do not need rules that forbid inconsistent configurations (two states at once etc.): Horn logic has a least model, and we don’t need to worry about other models when checking entailment
- Disjunctive acceptance conditions (“accepts if there is some time point at which is reaches an accepting state”) can be encoded by many implications (one for each case) without “real” disjunctions

Horn logic is $P$-complete:
- One of the hardest problems in $P$
- Inherently non-parallelisable

However:
- $PROP \text{ HORN ENTAILMENT}$ can be decided in linear time
  [Dowling/Gallier, 1984]
- This does not imply that all problems in $P$ have linear time algorithms