Circuit Complexity Before the Dawn of the New Millennium

Eric W. Allender
Rutgers University
and Universität Tübingen

Outline

- Survey current state of the field
- Mention obstacles to progress
- Give areas where progress seems likely

Some Misconceptions

- No superlinear lower bound on circuit size is known for any natural problem.

- Complexity Theory provides only asymptotic bounds, and hence it has no importance for practical computing.

Theorem: (Stockmeyer, 1974)
Any circuit that takes as input a formula (in the language of WS1S) with up to 616 symbols and produces as output a correct answer saying whether the formula is valid or not, requires at least 10^{123} gates.

Even if gates were the size of a proton and were connected by infinitely thin wires, the network would densely fill the known universe.

In practice, *any* proof that $A \notin \mathrm{P/poly}$
can be analyzed to obtain *concrete* bounds.

(P/poly is the class of problems
solvable with polynomial-size circuits.)

Open Questions: Spring 1995

Is NP $\subseteq$ P/poly?

Is DTIME(2^{poly}) $\subseteq$ P/poly?

Is $\mathrm{NTIME}(2^{\mathrm{poly}}) \subseteq \mathrm{P/poly}$?

Is $\mathrm{DTIME}(2^{\mathrm{poly}})^{\mathrm{NP}} \subseteq \mathrm{P/poly}$?

Is $\mathrm{MATIME}(2^{\mathrm{poly}}) \subseteq \mathrm{P/poly}$?

Is $\mathrm{PrTIME}(2^{\mathrm{poly}}) \subseteq \mathrm{P/poly}$?

What *is* known??

$\mathrm{NTIME}(n^{\log^* n})^{\mathrm{NP}} \not\subseteq \mathrm{P/poly}$

$\mathrm{ZPTIME}(n^{\log^* n})^{\mathrm{NP}} \not\subseteq \mathrm{P/poly}$

$\mathrm{DTIME}(n^{\log^* n})^{\mathrm{PP}} \not\subseteq \mathrm{P/poly}$

One Obstacle: Oracles

There are oracles relative to which:

$\mathrm{DTIME}(2^{\mathrm{poly}})^{\mathrm{NP}} \subseteq \mathrm{P/poly}$

$\mathrm{MATIME}(2^{\mathrm{poly}}) \subseteq \mathrm{P/poly}$

Crushing an Obstacle!

A new theorem by [Buhrman, Fortnow] and [Thierauf]:

$$\mathrm{MATIME}(2^{\mathrm{poly}}) \not\subseteq \mathrm{P/poly}$$

This does not relativize!

Proof sketch:

$$\begin{aligned} \mathrm{MATIME}(2^{\mathrm{poly}}) \subseteq \mathrm{P/poly} &\Rightarrow \mathrm{DTIME}(2^{\mathrm{poly}}) \subseteq \mathrm{P/poly} \\ &\Rightarrow \mathrm{DTIME}(2^{\mathrm{poly}}) = \mathrm{MA}\ [\mathrm{BFNW93}] \\ &\Rightarrow \mathrm{DTIME}(2^{2^{\mathrm{poly}}}) = \mathrm{MATIME}(2^{\mathrm{poly}}) \\ &\Rightarrow \mathrm{DTIME}(2^{2^{\mathrm{poly}}}) \subseteq \mathrm{P/poly} \end{aligned}$$

Contradiction!

Subclasses of P/poly

NC^1	Regular sets Boolean Formulae Non-solvable algebras
TC^0	$\times, \div$ Sorting Neural Nets
ACC^0	Mod m Solvable algebras
AC^0	$+, -$ First-order Logic
NC^0	not much!!

The Key to Lower Bounds: Depth Reduction

- Let $f \in \mathrm{AC}^0$. Most subfunctions of f are in NC^0.
- Let f in $\mathrm{AC}^0[\mathrm{mod}\ p]$ (for p prime). Then f is computed by a probabilistic depth two circuit of the form

- Let f in ACC^0. Then f is computed by a deterministic depth two circuit of the form

Theorem (Smolensky) Let q not be a power of prime p. Exponential size is required to compute the Mod q function with $\mathrm{AC}^0[\mathrm{mod}\ p]$ circuits.

Open:

Is $\mathrm{DTIME}(2^{\mathrm{poly}})^{\mathrm{NP}} \subseteq \mathrm{AC}^0[\mathrm{mod}\ 6]$?

Status for last ten years:

Incremental progress on small subclasses of TC^0 and ACC^0.

Another Obstacle: Natural Proofs

Razborov and Rudich formalized a class of arguments called "Natural Proofs". Current lower bound proofs are "natural".

If popular cryptographic assumptions are true, then no natural proof can show $\mathrm{NP} \not\subseteq \mathrm{TC}^0$.

Avoiding an Obstacle: Uniformity

$\{C_n\}$ is *uniform* if $n \mapsto C_n$ is "easy" to compute.

Open: Is $\mathrm{DTIME}(2^{\mathrm{poly}})^{\mathrm{NP}} \subseteq \mathrm{ACC}^0$?

Theorem (Allender, Gore)
$\mathrm{PP} \not\subseteq$ uniform ACC^0.

Theorem (Allender)
$\mathrm{PP} \not\subseteq$ uniform TC^0.

Proofs use diagonalization.
Diagonalization is not "natural".

Lower bounds on #P complete problems (such as the Permanent).

Circuit Class	Necessary condition on size $T(n)$
ACC^0	$T(n) > 2^{n^\epsilon}$
TC^0	$T(T(\ldots T(n)\ldots)) > 2^n$

Lower bounds on PP complete problems (such as MajSAT).

Circuit Class	Necessary condition on size $T(n)$
ACC^0	$T(T(n)) > 2^n$
TC^0	$T(T(\ldots T(n)\ldots)) > 2^n$

A report card
for complexity theory.

Subject	Performance
Lower Bounds for Natural Problems	*Disappointing*
Classification of Natural Problems (Completeness)	*Outstanding!*

Almost every natural computational problem is complete for some complexity class under AC^0 reducibility.

Nature presents us with computational problems corresponding in deep ways to notions of nondeterminism, counting, and circuits.

Empirically, problems complete for NP (or some other class) are p-isomorphic.

Hence, the Berman-Hartmanis conjecture:

The NP-complete sets are p-isomorphic.

Complexity classes give us a vocabulary to understand the computational problems nature provides us.

Complete problems are an artifact of natures invention, not of our own.

Should we not expect that the complete problems really <u>are</u> all p-isomorphic???

Why nobody believes the isomorphism conjecture: One-Way Functions

Let f be one-way. $f(\mathrm{SAT})$ is NP-complete, but is it isomorphic to SAT?

We do know that there are $f \in \mathrm{AC}^0$ such that $f^{-1} \notin \mathrm{AC}^0$ (and in fact, for all k, there are such f that are *pseudorandom* to depth k).

Is it possible to *disprove* the AC^0-isomorphism conjecture??

Isomorphism Theorem:

(Agrawal, Allender, Rudich)

All sets complete under AC^0 reductions are AC^0-isomorphic.

Gap Theorem:

(Agrawal, Allender, Rudich)

All sets complete under AC^0 reductions are complete under NC^0 reductions.

That is, there is a "gap" between NC^0 and AC^0, in terms of the complete sets.

Stop-Gap Theorem:

(Agrawal, Allender, Impagliazzo, Pitassi, Rudich)

There is a set that is complete under $\mathrm{AC}^0[\mathrm{mod}\ 2]$ reductions, but not under AC^0 reductions.

Summary

- The problems circuit complexity addresses are important.
- There appear to be some obstacles to progress on some of these problems
  - Relativizations
  - Natural proofs
- progress is being made by
  - Destroying the obstacles
  - Avoiding the obstacles