Complexity Theory

Jan Křetínský

Chair for Foundations of Software Reliability
and Theoretical Computer Science
Technical University of Munich

Summer 2016

July 11, 2016

Lecture 24

$\mathbf{AC^0} \subset \mathbf{NC^1}$

Agenda

- lower bounds for circuits
- **$AC^0 \subset NC^1$**
- tool: random restrictions and switching lemma

Circuit lower bounds

- n is trivial
- $5n - o(n)$ for NP-complete problems
- special cases: bounded depth
- any Boolean formula by circuit of depth 2 and exponential size
- some proven to require exponential size, not valid for depth 3 any more
- do NP-complete problems have polynomial circuits with constant depth, i.e., $\mathbf{AC^0}$?

$AC^0 \subset NC^1$

No!

$\mathbf{AC^0} \subset \mathbf{NC^1}$

No!

Theorem

$\bigoplus \notin \mathbf{AC^0}$

- $\bigoplus \in \mathbf{NC^1}$ by binary "$\oplus$-tree"
- hence $\mathbf{AC^0} \subset \mathbf{NC^1}$

Agenda

- lower bounds for circuits ✓
- $\mathbf{AC}^0 \subset \mathbf{NC}^1$ ✓
- tool: random restrictions and switching lemma

Main idea: random restrictions

- every function with $\mathbf{AC}^0$ satisfies:
- if vast majority of inputs fixed (randomly) to 0's and 1's
- then with positive probability the resulting function is constant
- but $\bigoplus$ is not!

Håstad's switching lemma

Function f under a partial assignment ρ is denoted $f|_\rho$.
Expressibility of f in k-CNF (or k-DNF) is denoted by
$f \in k$-CNF (or $f \in k$-DNF).

Theorem (Håstad's lemma, 1986)

Let $f \in k$-DNF and ρ random partial assignment to t random input bits.
Then $Pr_\rho[f|_\rho \notin s\text{-}CNF] \leq \left(\frac{(n-t)}{n} k^{10}\right)^{s/2}$ for every $s \geq 2$.

Håstad's switching lemma

Function f under a partial assignment ρ is denoted $f|_\rho$.
Expressibility of f in k-CNF (or k-DNF) is denoted by
$f \in k$-CNF (or $f \in k$-DNF).

Theorem (Håstad's lemma, 1986)

Let $f \in k$-DNF and ρ random partial assignment to t random input bits.
Then $Pr_\rho[f|_\rho \notin s\text{-}CNF] \leq \left(\frac{(n-t)}{n}k^{10}\right)^{s/2}$ for every $s \geq 2$.

- similarly for CNF
- restriction allows for switching between DNF and CNF without much blowup
- proof idea: 1-to-1 mapping of "bad" partial assignments (non-constant results) to "good" partial completions (constant results)

Proof sketch of $\bigoplus \notin$ AC^0

- start with any AC^0 circuit (in alternating form)
- in ith round:
- fix $n_i - \sqrt{n_i}$ input bits ($n_0 = n$)
- switch the two bottom layers into the other normal form
- collapse with the layer one above

Proof sketch of $\bigoplus \notin$ AC^0

- start with any AC^0 circuit (in alternating form)
- in ith round:
- fix $n_i - \sqrt{n_i}$ input bits ($n_0 = n$)
- switch the two bottom layers into the other normal form
- collapse with the layer one above
- finally, obtain two-layer DNF
- and make it constant (by fixing $\leq k$ variables in the first clause)

Proof sketch of $\bigoplus \notin$ AC^0

- start with any AC^0 circuit (in alternating form)
- in ith round:
- fix $n_i - \sqrt{n_i}$ input bits ($n_0 = n$)
- switch the two bottom layers into the other normal form
- collapse with the layer one above
- finally, obtain two-layer DNF
- and make it constant (by fixing $\leq k$ variables in the first clause)
- but $\bigoplus$ cannot be made constant for any partial assignment

What have we learnt?

- lower bounds are hard
- in special simple cases possible
- tool: random partial assignments