SS23 Advanced Complexity Theory

Circuit Complexity

Main references: [3, 6]

1 Upper bounds

1.1 Basic definitions

Circuits over arbitrary bases as straightline programs and as labeled acyclic digraphs.

Interpretation as models of parallel computation with depth modeling parallel time.

1.2 Examples

Addition, iterated addition (2-for-3 trick), logarithmically iterated addition, multiplication, iterated multiplication via chinese remaindering, Beame, Cook and Hoover's algorithm for division [1].

Majority, parity, digraph reachability.

Two tractability notions emerge: logarithmic depth binary circuits NC_1, constant depth unbounded circuits AC_0.

1.3 Constant depth reductions

Equivalence of iterated addition, multiplication and majority.

1.4 Symmetric functions

Constant depth reducibility to majority.

Denenberg, Gurevich and Shelah's coding lemma ([2, Lem 1]).

Håstad, Wegener, Wurm and Yi's very small constant depth circuits for polylogarithmic threshold functions, and generalizations thereof [2].

Symmetric polynomials, Minsky-Papert theorem ([3, Thm 2.2])

1.5 NC- and AC-hierarchies

$\mathsf{NC}_0 \subseteq \mathsf{AC}_0 \subseteq \mathsf{NC}_1 \subseteq \mathsf{AC}_1 \subseteq \cdots \subseteq \mathsf{AC} = \mathsf{NC}$.

Logspace-uniform versions: $\mathsf{uNC}_1 \subseteq \mathsf{L} \subseteq \mathsf{NL} \subseteq \mathsf{uAC}_1$.

P vs. NC as the question whether all feasible algorithms are parallelizable. P-completeness of the monotone circuit value problem.

Spira's characterization of NC_1 by propositional formulas.

Characterization of AC_0 by first-order logic ([4, Lem 1.4.4]).

Derandomization of RNC_1.

1.6 Parallel random access machines

PRAMS as a very generous model of parallel computation.

Simulation of PRAMS by logspace uniform circuits (and vice-versa), with parallel time closely related to depth [5, Sec 15.2].

2 Lower bounds

2.1 Formula lower bounds

2.1.1 Nechiporuk's method

Non-explicit $(1-\epsilon)\cdot 2^n/\log n$ formula lower bound.

Nechiporuk's $n^{2-o(1)}$ lower bound.

2.1.2 Subbotovskaya's method

The shrinking exponent for formulas is at least 1.5.

Andreev's $n^{2.5-o(1)}$ lower bound.

2.2 Bounded depth lower bounds

2.2.1 Decision trees

Decision trees and certificate complexity.

2.2.2 Håstad's switching lemma

Razborov's proof of Håstad's switching lemma.

Robustness bound for constant depth circuits.

Depth $d+1$ circuits computing parity have size $2^{\Omega(n^{1/d})}$.

Exponential lower bound for majority.

Polynomial upper bound for approximate majority and derandomization of RAC_0.

2.2.3 Razborov-Smolensky lower bound

Low degree approximation of $\mathsf{AC}_0[p]$-circuits by poynomials over $\mathbb{F}_p$.

$\mathsf{AC}_0[p]$-circuits of depth d that count mod q have size $2^{\Omega(n^{1/2d})}$.

2.2.4 Razborov's lower bound

Monotone circuits computing k-CLIQUE have size $n^{\Omega(\sqrt{k})}$.

References

[1] Paul Beame, Stephen A. Cook, H. James Hoover: Log Depth Circuits for Division and Related Problems. SIAM J. Comput. 15(4): 994-1003 (1986)

[2] Johan Håstad, Ingo Wegener, Norbert Wurm, Sang-Zin Yi: Optimal Depth, Very Small Size Circuits for Symmetric Functions in AC0. Inf. Comput. 108(2): 200-211 (1994)

[3] Stasys Jukna: Boolean Function Complexity - Advances and Frontiers. Algorithms and combinatorics 27, Springer 2012, ISBN 978-3-642-24507-7, pp. I-XV, 1-617

[4] Jan Krajíček: Proof complexity, Encyclopedia of Mathematics and Its Appplications, Vol.170, Cambridge University Press, Cambridge - New York - Melbourne, (March 2019), 530pp. ISBN: 9781108416849.

[5] Christos H. Papadimitriou: Computational complexity. Academic Internet Publ. 2007, ISBN 978-1-4288-1409-7, pp. 1-49

[6] Heribert Vollmer: Introduction to Circuit Complexity, A Uniform Approach, XI, 272 pages, Springer Berlin, Heidelberg