Povzetek

V delu predstavimo pojem naravnega dokaza, podamo dva primera in pokažemo meje naravnih dokazov.

Začnemo s predstavitvijo računskega modela logičnih vezij in nadaljujemo z dvema izrekoma o spodnji meji računske zahtevnosti pri tem modelu. Prvi izrek nam pove, da funkcije, ki računa parnost (t.j. vrne 0, če ima vhodni niz sodo enic in 1 sicer), ne moremo računati z družino vezij tipa $\mathbf{AC}^0$. V dokazu uporabimo slavno Håstadovo lemo, ki je zanimiva že sama po sebi. Drugi izrek je splošnejši in pove, da z družino vezij tipa $\mathbf{ACC}0(p)$ ne moremo računati funkcije MOD_q, ki vrne 0 natanko tedaj, ko je vsota vhodnih bitov deljiva s q, za vsako praštevilo p in njemu tuj $q > 1$. Uporabljena metoda v dokazu je povsem drugačna kot pri dokazu prvega izreka.

Predstavimo tudi pojem naravnega dokaza in pokažemo, da sta oba navedena dokaza spodnje meje naravna po naši definiciji. Glavna omejitev naravnih dokazov je ta, da za poljubno težko funkcijo ne morejo pokazati, da ni v $\mathbf{P}_{\mathbf{poly}}$, če le velja domneva o obstoju dovolj močne enosmerne funkcije.

Abstract

The notion of natural proof is introduced, two examples are given and limits of natural proofs are shown.

We begin by presenting a model of computation called Boolean circuits and continue with two theorems on lower bounds for this model. The first theorem states that the parity function (i.e. a function, which returns 0 if the number of ones in the input string is even and 1 otherwise) cannot be computed by a circuit family of type $\mathbf{AC}^0$. The proof uses the interesting and famous Håstad's Switching Lemma. The second theorem is more general and states that a circuit family of type $\mathbf{ACC}0(p)$ cannot compute functions MOD_q which return 0 iff the sum of the input bits is divisible by q, for each prime p and integer $q > 1$ that are coprime. The method used in the proof is completely different from the method used in the proof of the first theorem.

We also introduce the notion of natural proof and show that both proofs of lower bounds fall within our definition of natural. The main limitation of natural proofs is that, even for a very hard function, they cannot prove that this function is outside $\mathbf{P}_{\mathbf{poly}}$, assuming that a strong enough one-way function exists.

Math. Subj. Class. (2010): 94C10, 68Q15, 68Q17

Ključne besede: naravni dokaz, naravna lastnost, spodnja meja, Håstadova lema, logično vezje, $\mathbf{AC}^0$, $\mathbf{ACC}0$.

Keywords: natural proof, natural property, lower bound, Håstad's Switching Lemma, boolean circuit, $\mathbf{AC}^0$, $\mathbf{ACC}0$.

Literatura

[1] Scott Aaronson in Avi Wigderson. Algebrization: A New Barrier in Complexity Theory. *Electronic Colloquium on Computational Complexity (ECCC)*, 15(005), 2008.

[2] Sanjeev Arora in Boaz Barak. *Computational Complexity: A Modern Approach*. Cambridge University Press, 2009. Več informacij na `www.cambridge.org/9780521424264`.

[3] Theodore P. Baker, John Gill in Robert Solovay. Relativizatons of the P =? NP Question. *SIAM J. Comput.*, 4(4):431–442, 1975.

[4] Manuel Blum in Silvio Micali. How to generate cryptographically strong sequences of pseudo-random bits. *SIAM J. Comput.*, 13:850–864, 1984.

[5] Ravi B. Boppana in Michael Sipser. The Complexity of Finite Functions. Objavljeno v *Handbook of Theoretical Computer Science, Volume A: Algorithms and Complexity (A)*, strani 757–804. The MIT Press, 1990.

[6] Gödel Prize. Dostopno na `http://sigact.org/Prizes/Godel/`. [ogled 4. 8. 2011].

[7] Johan Håstad. Almost optimal lower bounds for small depth circuits. Objavljeno v *STOC*, strani 6–20. ACM, 1986.

[8] Joseph JáJá. *An Introduction to Parallel Algorithms*. Addison-Wesley, 1992.

[9] Riste Škrekovski. Osnove verjetnostne metode. Dostopno na `http://www.fmf.uni-lj.si/~skreko/Gradiva/OVM-skripta.pdf`, 2010. [ogled 22. 7. 2011].

[10] Richard J. Lipton. *The* **P** = **NP** *Question and Gödel's Lost Letter*. Springer, 2010.

[11] Jiří Matoušek in Jan Vondrák. The probabilistic method. Dostopno na `http://www.cs.cmu.edu/afs/cs.cmu.edu/academic/class/15859-f09/www/handouts/matousek-vondrak-prob-ln.pdf`, verzija marec 2008. [ogled 11. 7. 2011].

[12] Millennium Prize Problems. Dostopno na `http://www.claymath.org/millennium/`. [ogled 4. 8. 2011].

[13] Peter Bro Miltersen, Jaikumar Radhakrishnan in Ingo Wegener. On converting CNF to DNF. *Theor. Comput. Sci.*, 347:325–335, 2005.

[14] Rajeev Motwani in Prabhakar Raghavan. *Randomized algorithms*. Cambridge University Press, 1995.

[15] Ketan Mulmuley. A fast parallel algorithm to compute the rank of a matrix over an arbitrary field. *Combinatorica*, 7:101–104, 1987.

[16] Asymptotics of central binomial coefficient. Dostopno na `http://planetmath.org/encyclopedia/AsymptoticsOfCentralBinomialCoefficient.html`. [ogled 9. 7. 2011].

[17] Alexander A. Razborov. Bounded Arithmetic and Lower Bounds in Boolean Complexity. Objavljeno v *Feasible Mathematics II*, strani 344–386. Birkhauser, 1993.

[18] Alexander A. Razborov in Steven Rudich. Natural proofs. *J. Comput. Syst. Sci.*, 55:24–35, 1997.

[19] Michael Sipser. *Introduction to the theory of computation*. PWS Publishing Company, 1997.

[20] Roman Smolensky. Algebraic Methods in the Theory of Lower Bounds for Boolean Circuit Complexity. Objavljeno v *STOC*, strani 77–82. ACM, 1987.

[21] Ivan Vidav. *Algebra*. Mladinska knjiga, Ljubljana, 1972.

[22] Ingo Wegener. The complexity of Boolean functions. Dostopno na `http://ls2-www.cs.uni-dortmund.de/monographs/bluebook/`, 1987. [ogled 28. 7. 2011].

[23] Wallis's Product. Dostopno na `http://www.proofwiki.org/wiki/Wallis's_Product`. [ogled 22. 7. 2011].