Approximate Degree in Classical and Quantum Computing

Other titles in Foundations and Trends® in Theoretical Computer Science

Multi-Valued Reasoning about Reactive Systems
Orna Kupferman
ISBN: 978-1-63828-138-2

Quantified Derandomization: How to Find Water in the Ocean
Roei Tell
ISBN: 978-1-63828-092-7

Complexity Theory, Game Theory, and Economics: The Barbados Lectures
Tim Roughgarden
ISBN: 978-1-68083-654-7

Semialgebraic Proofs and Efficient Algorithm Design
Noah Fleming, Pravesh Kothari and Toniann Pitassi
ISBN: 978-1-68083-636-3

Higher-order Fourier Analysis and Applications
Hamed Hatami, Pooya Hatami and Shachar Lovett
ISBN: 978-1-68083-592-2

Approximate Degree in Classical and Quantum Computing

Mark Bun
Boston University
mbun@bu.edu

Justin Thaler
Georgetown University
justin.thaler@georgetown.edu

the essence of knowledge
Boston — Delft

Foundations and Trends® in Theoretical Computer Science

Published, sold and distributed by:
now Publishers Inc.
PO Box 1024
Hanover, MA 02339
United States
Tel. +1-781-985-4510
www.nowpublishers.com
sales@nowpublishers.com

Outside North America:
now Publishers Inc.
PO Box 179
2600 AD Delft
The Netherlands
Tel. +31-6-51115274

The preferred citation for this publication is

M. Bun and J. Thaler. *Approximate Degree in Classical and Quantum Computing.* Foundations and Trends® in Theoretical Computer Science, vol. 15, no. 3-4, pp. 229–423, 2022.

ISBN: 978-1-63828-141-2

Foundations and Trends® in Theoretical Computer Science

Volume 15, Issue 3-4, 2022

Editorial Scope

Topics

Foundations and Trends® in Theoretical Computer Science publishes survey and tutorial articles in the following topics:

- Algorithmic game theory
- Computational algebra
- Computational aspects of combinatorics and graph theory
- Computational aspects of communication
- Computational biology
- Computational complexity
- Computational geometry
- Computational learning
- Computational Models and Complexity
- Computational Number Theory
- Cryptography and information security
- Data structures
- Database theory
- Design and analysis of algorithms
- Distributed computing
- Information retrieval
- Operations Research
- Parallel algorithms
- Quantum Computation
- Randomness in Computation

Information for Librarians

Foundations and Trends® in Theoretical Computer Science, 2022, Volume 15, 4 issues. ISSN paper version 1551-305X. ISSN online version 1551-3068. Also available as a combined paper and online subscription.

Contents

Approximate Degree in Classical and Quantum Computing

Mark Bun[1] and Justin Thaler[2]

[1] *Boston University, USA; mbun@bu.edu*
[2] *Georgetown University, USA; justin.thaler@georgetown.edu*

ABSTRACT

The approximate degree of a Boolean function f captures how well f can be approximated pointwise by low-degree polynomials. This monograph surveys what is known about approximate degree and illustrates its applications in theoretical computer science.

A particular focus of the survey is a method of proving lower bounds via objects called *dual polynomials*. These represent a reformulation of approximate degree using linear programming duality. We discuss in detail a recent, powerful technique for constructing dual polynomials, called "dual block composition".

Mark Bun and Justin Thaler (2022), "Approximate Degree in Classical and Quantum Computing", Foundations and Trends® in Theoretical Computer Science: Vol. 15, No. 3-4, pp 229–423. DOI: 10.1561/0400000107.

1

Introduction

The ability (or inability) to represent or approximate Boolean functions by polynomials is a central concept in complexity theory, underlying interactive and probabilistically checkable proof systems, circuit lower bounds, quantum complexity theory, and more. In this monograph, we survey what is known about a particularly natural notion of approximation by polynomials, capturing pointwise approximation over the real numbers. The ε-*approximate degree* of a Boolean function $f\colon \{-1,1\}^n \to \{-1,1\}$, denoted $\widetilde{\deg}_\varepsilon(f)$, is the least total degree of a real polynomial $p : \{-1,1\}^n \to \mathbb{R}$ such that

$$|f(x) - p(x)| \leq \varepsilon \text{ for all } x \in \{-1,1\}^n. \tag{1.1}$$

By total degree of p, we refer to the maximum sum of the degrees of all variables appearing in any monomial. For example, $p(x_1, x_2, x_3) = x_1^2 x_2 x_3^2 + x_1 x_2^3$ has total degree 5.

Every Boolean function is approximated to error $\varepsilon = 1$ by the constant 0 function, implying that $\widetilde{\deg}_1(f) = 0$ for all such f. However, whenever ε is strictly less than 1, $\widetilde{\deg}_\varepsilon(f)$ is a fascinating notion with a rich theory and applications throughout theoretical computer science.

Applications of approximate degree lower bounds. The study of approximate degree is itself a "proto-complexity theory" [2], with pointwise approximation by real polynomials serving as a rudimentary model of computation, and degree acting as a measure of complexity. Moreover, when f has large (say, $n^{\Omega(1)}$) approximate degree, it is also hard to compute in a variety of other computational models. Different models correspond to different settings of the error parameter ε with two regimes of particular interest. First, if $\widetilde{\deg}_{1/3}(f)$ is large, then f cannot be efficiently evaluated by *bounded-error* quantum query algorithms [16].[1] This connection is often referred to as the "polynomial method in quantum computing."

Second, if $\widetilde{\deg}_{\varepsilon}(f)$ is large *for every* $\varepsilon < 1$, then f is difficult to compute by *unbounded-error* randomized (or quantum) query algorithms (see, e.g., [56, Lemma 6]). These are randomized algorithms that are only required to do slightly better than random guessing, and correspond to the complexity class **PP** (short for probabilistic polynomial time) defined by Gill [63]. This connection has been used to answer long-standing questions in relativized complexity, e.g., in studying the power of statistical zero-knowledge proofs (Section 7.2), and in communication complexity (Section 10). Approximability of f in this error regime, wherein the error ε is allowed to be arbitrarily close to (but strictly less than) 1,[2] is captured by a notion termed *threshold degree* and denoted $\deg_{\pm}(f)$.

Applications of approximate degree upper bounds. As just discussed, lower bounds on $\widetilde{\deg}_{\varepsilon}(f)$ imply hardness results for computing f. There are also many applications of upper bounds on $\widetilde{\deg}_{\varepsilon}(f)$, typically in the design of fast algorithms in areas such as learning theory [71], [75] (see Section 11.2) and differential privacy [51], [127].

[1]The choice of constant 1/3 is made for aesthetic reasons. Replacing $\varepsilon = 1/3$ with any other constant in $(0, 1)$ changes the ε-approximate degree of f by at most a constant factor.

[2]Approximate degree is a meaningful notion even for error parameters ϵ that are *doubly-exponentially* close to 1. In particular, for any degree bound d, there are known Boolean functions that can be approximated by degree-d polynomials to error $1 - 2^{-n^{\Theta(d)}}$ but not to smaller error [48], [98], [99].

In addition to algorithmic applications, approximate degree upper bounds have also been used to prove complexity *lower bounds*. Here is an illustrative example. Suppose one shows that every circuit over n-bit inputs in a class $\mathcal{C}$ can be approximated to error $\varepsilon < 1$ by a polynomial of degree $o(n)$. We know that simple functions f such as Majority and Parity require approximate degree $\Omega(n)$, and therefore cannot be computed by circuits in $\mathcal{C}$. In fact, if $\varepsilon = 1/3$, then one can even conclude that $\mathcal{C}$ is not powerful enough to compute these functions *on average*, meaning that for every circuit $C \in \mathcal{C}$, we have $\Pr_{x \sim \{-1,1\}^n}[C(x) = f(x)] \leq 1/2 + \frac{1}{n^{\omega(1)}}$ [43], [125]. This principle underlies several state-of-the-art lower bounds for frontier problems in circuit complexity (Section 11.3).

Goals of this survey. This survey covers recent progress on proving approximate degree lower and upper bounds and describes some applications of the new bounds to oracle separations, quantum query and communication complexity, and circuit complexity. On the lower bounds side, progress has followed from an approach called the *method of dual polynomials*, which seeks to prove approximate degree lower bounds by constructing solutions to (the dual of) a certain linear program that captures the approximate degree of any function. This survey explains how several of these advances have been unlocked by a particularly simple and elegant technique—called *dual block composition*—for constructing solutions to this dual linear program. We also provide concise coverage of even more recent lower bound technique based on a new complexity measure called *spectral sensitivity*.

On the upper bounds side, recent explicit constructions of approximating polynomials have been inspired by quantum query algorithms. These constructions also involve new techniques that first express the approximations as sums of exponentially many high-degree terms, and then replace each term with a low-degree approximation that is accurate to exponentially small error.

Roadmap and suggestions for reading the survey. After covering preliminaries (Section 2), we begin in Sections 3 and 4 by covering approximate degree upper bounds, i.e., techniques for constructing low-degree approximations to Boolean functions. We then turn to lower bound techniques, starting with the simpler and older technique of symmetrization (Section 5) before turning to the method of dual polynomials (Section 6). The next two sections provide progressively more sophisticated developments of this technique, with Section 7 introducing dual block composition as a technique for lower bounding the approximate degree of block-composed functions, and Section 8 moving beyond block-composed functions. Section 9 covers approximate degree lower bounds via spectral sensitivity.

The survey then turns to applications of approximate degree upper and lower bounds. Section 10 covers (a variant of) the so-called pattern matrix method for translating approximate degree lower bounds into approximate-rank and communication lower bounds. Section 11 covers assorted additional applications of both upper and lower bounds on approximate degree.

We have primarily organized the survey by technique. For example, all upper bounds that we cover appear in Sections 3 and 4, with the exception of the approximate degree upper bound for a function called Surjectivity that appears in Section 8.1. This organization maximizes technical and conceptual continuity, but does have some downsides. The results are not covered in increasing order of difficulty, e.g., the easiest lower bounds come after the most challenging upper bounds. It also means that for any specific function or class of functions, the tight upper and lower bounds appear in different parts of the survey.

Readers may wish to skip some of the more technical results that we cover on a first reading. Prominent examples include the upper bound for a function called Element Distinctness in Section 4.4, the proof of Theorem 7.7 in Section 7.2 on a state-of-the-art lower bound for block-composed functions, the entirety of Section 8.5 on lower bounds for problems called Collision and Permutation Testing, and the proof of Theorem 10.23 in Section 10.5, which constructs a dual witness for the high threshold-degree of an AC^0 function with certain "smoothness" properties that are important for applications in communication- and circuit-complexity.

References

[1] S. Aaronson, "Quantum lower bound for the collision problem," in *Proceedings on 34th Annual ACM Symposium on Theory of Computing, May 19-21, 2002, Montréal, Québec, Canada*, pp. 635–642, ACM, 2002. DOI: 10.1145/509907.509999.

[2] S. Aaronson, "The polynomial method in quantum and classical computing," in *Foundations of Computer Science*, 2008.

[3] S. Aaronson, "Impossibility of succinct quantum proofs for collision-freeness," *Quantum Information & Computation*, vol. 12, no. 1-2, 2012, pp. 21–28.

[4] S. Aaronson, S. Ben-David, R. Kothari, S. Rao, and A. Tal, "Degree vs. approximate degree and quantum implications of Huang?s sensitivity theorem," in *Proceedings of the 53rd Annual ACM SIGACT Symposium on Theory of Computing*, pp. 1330–1342, 2021.

[5] S. Aaronson, R. Kothari, W. Kretschmer, and J. Thaler, "Quantum lower bounds for approximate counting via laurent polynomials," in *35th Computational Complexity Conference, CCC 2020, July 28-31, 2020, Saarbrücken, Germany (Virtual Conference)*, ser. LIPIcs, vol. 169, 7:1–7:47, Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2020. DOI: 10.4230/LIPIcs.CCC.2020.7.

[6] S. Aaronson and Y. Shi, "Quantum lower bounds for the collision and the element distinctness problems," *Journal of the ACM*, vol. 51, no. 4, 2004, pp. 595–605.

[7] S. Aaronson and A. Wigderson, "Algebrization: A new barrier in complexity theory," *ACM Transactions on Computation Theory (TOCT)*, vol. 1, no. 1, 2009, pp. 1–54.

[8] E. Allender, "A note on the power of threshold circuits," in *Foundations of Computer Science*, pp. 580–584, 1989.

[9] A. Ambainis, "Polynomial degree and lower bounds in quantum complexity: Collision and element distinctness with small range," *Theory of Computing*, vol. 1, no. 1, 2005, pp. 37–46.

[10] A. Ambainis, "Polynomial degree vs. quantum query complexity," *Journal of Computer and System Sciences*, vol. 72, no. 2, 2006, pp. 220–238.

[11] A. Ambainis, "Quantum walk algorithm for element distinctness," *SIAM Journal on Computing*, vol. 37, no. 1, 2007, pp. 210–239.

[12] A. Ambainis, "Understanding quantum algorithms via query complexity," in *Proceedings of the International Congress of Mathematicians*, 2018.

[13] S. Arunachalam, J. Briët, and C. Palazuelos, "Quantum query algorithms are completely bounded forms," *SIAM Journal on Computing*, vol. 48, no. 3, 2019, pp. 903–925.

[14] J. Aspnes, R. Beigel, M. Furst, and S. Rudich, "The expressive power of voting polynomials," *Combinatorica*, vol. 14, no. 2, 1994, pp. 135–148.

[15] L. Babai, P. Frankl, and J. Simon, "Complexity classes in communication complexity theory," in *Foundations of Computer Science*, pp. 337–347, 1986.

[16] R. Beals, H. Buhrman, R. Cleve, M. Mosca, and R. De Wolf, "Quantum lower bounds by polynomials," *Journal of the ACM*, vol. 48, no. 4, 2001, pp. 778–797.

[17] P. Beame and W. Machmouchi, "The quantum query complexity of ac^0," *Quantum Inf. Comput.*, vol. 12, no. 7-8, 2012, pp. 670–676. DOI: 10.26421/QIC12.7-8-11.

[18] R. Beigel, "Perceptrons, PP, and the polynomial hierarchy," *Computational complexity*, vol. 4, no. 4, 1994, pp. 339–349.

[19] R. Beigel, N. Reingold, D. Spielman, *et al.*, *The perceptron strikes back*. Yale University, Department of Computer Science, 1990.

[20] R. Beigel, N. Reingold, and D. A. Spielman, "PP is closed under intersection," *Journal of Computer and System Sciences*, vol. 50, no. 2, 1995, pp. 191–202.

[21] A. Belovs, "Learning-graph-based quantum algorithm for k-distinctness," in *Foundations of Computer Science*, pp. 207–216, 2012.

[22] A. Belovs, "Quantum algorithms for learning symmetric juntas via the adversary bound," *Computational Complexity*, vol. 24, no. 2, 2015, pp. 255–293.

[23] S. Ben-David, A. Bouland, A. Garg, and R. Kothari, "Classical lower bounds from quantum upper bounds," in *Foundations of Computer Science*, pp. 339–349, 2018.

[24] G. Beniamini, "The approximate degree of bipartite perfect matching," *arXiv preprint arXiv:2004.14318*, 2020.

[25] G. Beniamini and N. Nisan, "Bipartite perfect matching as a real polynomial," in *STOC '21: 53rd Annual ACM SIGACT Symposium on Theory of Computing, Virtual Event, Italy, June 21-25, 2021*, pp. 1118–1131, ACM, 2021. DOI: 10.1145/3406325.3451002.

[26] C. H. Bennett, E. Bernstein, G. Brassard, and U. Vazirani, "Strengths and weaknesses of quantum computing," *SIAM Journal on Computing*, vol. 26, no. 5, 1997, pp. 1510–1523.

[27] A. Bogdanov, K. Dinesh, Y. Filmus, Y. Ishai, A. Kaplan, and A. Srinivasan, "Bounded indistinguishability for simple sources," in *13th Innovations in Theoretical Computer Science Conference, ITCS 2022*, ser. LIPIcs, vol. 215, 26:1–26:18, Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2022. DOI: 10.4230/LIPIcs.ITCS.2022.26.

[28] A. Bogdanov, Y. Ishai, E. Viola, and C. Williamson, "Bounded indistinguishability and the complexity of recovering secrets," in *International Cryptology Conference*, vol. 9816, pp. 593–618, 2016.

[29] A. Bogdanov, N. S. Mande, J. Thaler, and C. Williamson, "Approximate degree, secret sharing, and concentration phenomena," in *Approximation, Randomization, and Combinatorial Optimization*, ser. LIPIcs, vol. 145, 71:1–71:21, Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2019. DOI: 10.4230/LIPIcs.APPROX-RANDOM.2019.71.

[30] A. Bogdanov and C. Williamson, "Approximate bounded indistinguishability," in *44th International Colloquium on Automata, Languages, and Programming, ICALP 2017*, ser. LIPIcs, vol. 80, 53:1–53:11, Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2017. DOI: 10.4230/LIPIcs.ICALP.2017.53.

[31] A. Bouland, L. Chen, D. Holden, J. Thaler, and P. N. Vasudevan, "On the power of statistical zero knowledge," *SIAM Journal on Computing*, vol. 49, no. 4, 2019, pp. 1–58.

[32] G. Brassard, P. Høyer, M. Mosca, and A. Tapp, "Quantum amplitude amplification and estimation," in *Quantum computation and information (Washington, DC, 2000)*, ser. Contemp. Math. Vol. 305, 2002, pp. 53–74. DOI: 10.1090/conm/305/05215.

[33] G. Brassard, P. Hoyer, and A. Tapp, "Quantum algorithm for the collision problem," *ACM SIGACT News (Cryptology Column)*, vol. 28, 1997, pp. 14–19.

[34] G. Brassard, P. Høyer, and A. Tapp, "Quantum counting," in *Automata, Languages and Programming, 25th International Colloquium, ICALP'98, Aalborg, Denmark, July 13-17, 1998, Proceedings*, vol. 1443, pp. 820–831, Springer, 1998. DOI: 10.1007/BFb0055105.

[35] J. Briët and F. E. Gutiérrez, "On converses to the polynomial method," *arXiv preprint arXiv:2204.12303*, 2022.

[36] J. Bruck and R. Smolensky, "Polynomial threshold functions, acˆ0 functions, and spectral norms," *SIAM Journal on Computing*, vol. 21, no. 1, 1992, pp. 33–42.

[37] H. Buhrman, R. Cleve, R. De Wolf, and C. Zalka, "Bounds for small-error and zero-error quantum algorithms," in *Foundations of Computer Science*, pp. 358–368, 1999.

[38] H. Buhrman, R. Cleve, and A. Wigderson, "Quantum vs. classical communication and computation," in *Proceedings of the thirtieth annual ACM symposium on Theory of computing*, pp. 63–68, 1998.

[39] H. Buhrman, I. Newman, H. Rohrig, and R. de Wolf, "Robust polynomials and quantum algorithms," *Theory of Computing Systems*, vol. 40, no. 4, 2007, pp. 379–395.

[40] H. Buhrman, N. Vereshchagin, and R. de Wolf, "On computation and communication with small bias," in *Twenty-Second Annual IEEE Conference on Computational Complexity (CCC'07)*, IEEE, pp. 24–32, 2007.

[41] H. Buhrman and R. de Wolf, "Communication complexity lower bounds by polynomials," in *Proceedings 16th Annual IEEE Conference on Computational Complexity*, IEEE, pp. 120–130, 2001.

[42] M. Bun, R. Kothari, and J. Thaler, "The polynomial method strikes back: Tight quantum query bounds via dual polynomials," in *Symposium on Theory of Computing*, pp. 297–310, 2018.

[43] M. Bun, R. Kothari, and J. Thaler, "Quantum algorithms and approximating polynomials for composed functions with shared inputs," *Quantum*, vol. 5, 2021. DOI: 10.22331/q-2021-09-16-543.

[44] M. Bun, N. S. Mande, and J. Thaler, "Sign-rank can increase under intersection," *ACM Transactions on Computation Theory (TOCT)*, vol. 13, no. 4, 2021, pp. 1–17.

[45] M. Bun and J. Thaler, "Dual lower bounds for approximate degree and Markov–Bernstein inequalities," *Information and Computation*, vol. 243, 2015, pp. 2–25.

[46] M. Bun and J. Thaler, "Hardness amplification and the approximate degree of constant-depth circuits," in *International Colloquium on Automata, Languages, and Programming*, pp. 268–280, 2015.

[47] M. Bun and J. Thaler, "Approximate Degree and the Complexity of Depth Three Circuits," in *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques (APPROX/RANDOM 2018)*, ser. Leibniz International Proceedings in Informatics (LIPIcs), vol. 116, 35:1–35:18, Dagstuhl, Germany: Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, 2018. DOI: 10.4230/LIPIcs.APPROX-RANDOM.2018.35.

[48] M. Bun and J. Thaler, "Approximate degree and the complexity of depth three circuits," in *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques (APPROX/RANDOM 2018)*, Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik, 2018.

[49] M. Bun and J. Thaler, "A nearly optimal lower bound on the approximate degree of AC^0," *SIAM Journal on Computing*, vol. 49, no. 4, 2019, pp. 59–96.

[50] M. Bun and J. Thaler, "The large-error approximate degree of AC^0," in *International Conference on Randomization and Computation*, ser. LIPIcs, vol. 145, 55:1–55:16, Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2019.

[51] K. Chandrasekaran, J. Thaler, J. Ullman, and A. Wan, "Faster private release of marginals on small databases," in *Innovations in Theoretical Computer Science*, pp. 387–402, 2014.

[52] A. Chattopadhyay and N. Mande, "A short list of equalities induces large sign rank," in *2018 IEEE 59th Annual Symposium on Foundations of Computer Science (FOCS)*, IEEE, pp. 47–58, 2018.

[53] K. Cheng, Y. Ishai, and X. Li, "Near-optimal secret sharing and error correcting codes in AC^0," in *Theory of Cryptography Conference*, Springer, pp. 424–458, 2017.

[54] M. Cheraghchi, E. Grigorescu, B. Juba, K. Wimmer, and N. Xie, "$AC^0 \circ MOD_2$ lower bounds for the Boolean inner product," *J. Comput. Syst. Sci.*, vol. 97, 2018, pp. 45–59. DOI: 10.1016/j.jcss.2018.04.006.

[55] D. Coppersmith and T. J. Rivlin, "The growth of polynomials bounded at equally spaced points," *SIAM Journal on Mathematical Analysis*, vol. 23, no. 4, 1992, pp. 970–983.

[56] M. Dall'Agnol, T. Gur, S. Roy Moulik, and J. Thaler, "Quantum Proofs of Proximity," *Quantum*, vol. 6, 2022. DOI: 10.22331/q-2022-10-13-834.

[57] I. Diakonikolas, P. Gopalan, R. Jaiswal, R. A. Servedio, and E. Viola, "Bounded independence fools halfspaces," *SIAM Journal on Computing*, vol. 39, no. 8, 2010, pp. 3441–3462.

[58] M. Ezra and R. D. Rothblum, "Small circuits imply efficient Arthur-Merlin protocols," in *ECCCTR: Electronic Colloquium on Computational Complexity, technical reports*, 2021.

[59] J. Forster, "A linear lower bound on the unbounded error probabilistic communication complexity," *Journal of Computer and System Sciences*, vol. 65, no. 4, 2002, pp. 612–625.

[60] M. Furst, J. B. Saxe, and M. Sipser, "Parity, circuits, and the polynomial-time hierarchy," *Mathematical systems theory*, vol. 17, no. 1, 1984, pp. 13–27.

[61] M. L. Furst, J. B. Saxe, and M. Sipser, "Parity, circuits, and the polynomial-time hierarchy," *Math. Syst. Theory*, vol. 17, no. 1, 1984, pp. 13–27. DOI: 10.1007/BF01744431.

[62] D. Gavinsky and A. A. Sherstov, "A separation of NP and coNP in multiparty communication complexity," *Theory of Computing*, vol. 6, no. 1, 2010, pp. 227–245.

[63] J. Gill, "Computational complexity of probabilistic Turing machines," *SIAM Journal on Computing*, vol. 6, no. 4, 1977, pp. 675–695.

[64] V. Guruswami and P. Raghavendra, "Hardness of learning halfspaces with noise," *SIAM Journal on Computing*, vol. 39, no. 2, 2009, pp. 742–765. DOI: 10.1137/070685798. eprint: https://doi.org/10.1137/070685798.

[65] P. Harsha and S. Srinivasan, "On polynomial approximations to AC," *Random Struct. Algorithms*, vol. 54, no. 2, 2019, pp. 289–303. DOI: 10.1002/rsa.20786.

[66] D. Haussler, "Decision theoretic generalizations of the PAC model for neural net and other learning applications," *Inf. Comput.*, vol. 100, no. 1, 1992, pp. 78–150. DOI: 10.1016/0890-5401(92)90010-D.

[67] H. Huang, "Induced subgraphs of hypercubes and a proof of the sensitivity conjecture," *Annals of Mathematics*, vol. 190, no. 3, 2019, pp. 949–955.

[68] S. Jukna, *Boolean Function Complexity - Advances and Frontiers*, vol. 27, ser. Algorithms and combinatorics. Springer, 2012. DOI: 10.1007/978-3-642-24508-4.

[69] V. Kabanets, S. Koroth, Z. Lu, D. Myrisiotis, and I. C. Oliveira, "Algorithms and lower bounds for De Morgan formulas of low-communication leaf gates," in *35th Computational Complexity Conference, CCC 2020*, ser. LIPIcs, vol. 169, 15:1–15:41, Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2020. DOI: 10.4230/LIPIcs.CCC.2020.15.

[70] J. Kahn, N. Linial, and A. Samorodnitsky, "Inclusion-exclusion: Exact and approximate," *Combinatorica*, vol. 16, no. 4, 1996, pp. 465–477.

[71] A. T. Kalai, A. R. Klivans, Y. Mansour, and R. A. Servedio, "Agnostically learning halfspaces," *SIAM Journal on Computing*, vol. 37, no. 6, 2008, pp. 1777–1805.

[72] M. J. Kearns, R. E. Schapire, and L. M. Sellie, "Toward efficient agnostic learning," *Machine Learning*, vol. 17, no. 2, 1994, pp. 115–141.

[73] H. Klauck, "Rectangle size bounds and threshold covers in communication complexity," in *18th Annual IEEE Conference on Computational Complexity (Complexity 2003), 7-10 July 2003, Aarhus, Denmark*, pp. 118–134, IEEE Computer Society, 2003. DOI: 10.1109/CCC.2003.1214415.

[74] H. Klauck, "On arthur merlin games in communication complexity," in *2011 IEEE 26th Annual Conference on Computational Complexity*, IEEE, pp. 189–199, 2011.

[75] A. R. Klivans and R. A. Servedio, "Learning DNF in time $2^{\tilde{O}(n^{1/3})}$," *Journal of Computer and System Sciences*, vol. 68, no. 2, 2004, pp. 303–318.

[76] A. R. Klivans and A. A. Sherstov, "A lower bound for agnostically learning disjunctions," in *International Conference on Computational Learning Theory*, Springer, pp. 409–423, 2007.

[77] K.-I. Ko, *Constructing oracles by lower bound techniques for circuits*, 1989.

[78] I. Kremer, *Quantum communication*. Citeseer, 1995.

[79] T. Lee, "A note on the sign degree of formulas," *arXiv preprint arXiv:0909.4607*, 2009.

[80] T. Lee and A. Shraibman, "An approximation algorithm for approximation rank," in *2009 24th Annual IEEE Conference on Computational Complexity*, IEEE, pp. 351–357, 2009.

[81] T. Lee and A. Shraibman, "Lower bounds in communication complexity," *Foundations and Trends in Theoretical Computer Science*, vol. 3, no. 4, 2009, pp. 263–399. DOI: 10.1561/0400000040.

[82] T. Lee and S. Zhang, "Composition theorems in communication complexity," in *Automata, Languages and Programming, 37th International Colloquium, ICALP 2010*, ser. Lecture Notes in Computer Science, vol. 6198, pp. 475–489, Springer, 2010. DOI: 10.1007/978-3-642-14165-2_41.

[83] N. Linial and A. Shraibman, "Learning complexity vs communication complexity," *Comb. Probab. Comput.*, vol. 18, no. 1-2, 2009, pp. 227–245. DOI: 10.1017/S0963548308009656.

[84] N. Linial and A. Shraibman, "Lower bounds in communication complexity based on factorization norms," *Random Struct. Algorithms*, vol. 34, no. 3, 2009, pp. 368–394. DOI: 10.1002/rsa.20232.

[85] N. Littlestone, "Learning quickly when irrelevant attributes abound: A new linear-threshold algorithm," *Machine learning*, vol. 2, no. 4, 1988, pp. 285–318.

[86] S. V. Lokam, "Complexity lower bounds using linear algebra," *Foundations and Trends in Theoretical Computer Science*, vol. 4, no. 1-2, 2009, pp. 1–155. DOI: 10.1561/0400000011.

[87] N. S. Mande, J. Thaler, and S. Zhu, "Improved approximate degree bounds for k-distinctness," in *Theory of Quantum Computation, Communication and Cryptography*, vol. 158, 2:1–2:22, 2020.

[88] N. S. Mande, "Communication complexity of xor functions," Ph.D. dissertation, Tata Institute of Fundamental Research Mumbai, 2018.

[89] A. A. Markov, "On a question by DI Mendeleev," *Zapiski Imperatorskoi Akademii Nauk*, vol. 62, no. 1-24, 1890.

[90] C. Marriott and J. Watrous, "Quantum Arthur–Merlin games," *Computational Complexity*, vol. 14, no. 2, 2005, pp. 122–152.

[91] M. Minsky and S. Papert, *Perceptrons: An introduction to computational geometry.* MIT Press, 1969.

[92] S. Muroga, I. Toda, and S. Takasu, "Theory of majority switching elements," *J. Franklin Institute*, vol. 271, no. 5, 1961, pp. 376–418.

[93] N. Nisan, "The communication complexity of threshold gates," *Combinatorics, Paul Erdos is Eighty*, vol. 1, 1993, pp. 301–315.

[94] N. Nisan and M. Szegedy, "On the degree of Boolean functions as real polynomials," *Computational Complexity*, vol. 4, no. 4, 1994, pp. 301–313.

[95] R. O'Donnell, *Linear and semidefinite programming (advanced algorithms) fall 2011 lecture notes*, 2011.

[96] R. Paturi, "On the degree of polynomials that approximate symmetric boolean functions (preliminary version)," in *Symposium on Theory of Computing*, pp. 468–474, 1992.

[97] R. Paturi and J. Simon, "Probabilistic communication complexity," *Journal of Computer and System Sciences*, vol. 33, no. 1, 1986, pp. 106–123.

[98] V. V. Podolskii, "A uniform lower bound on weights of perceptrons," in *International Computer Science Symposium in Russia*, Springer, pp. 261–272, 2008.

[99] V. V. Podolskii, "Perceptrons of large weight," *Problems of Information Transmission*, vol. 45, no. 1, 2009, pp. 46–53.

[100] A. A. Razborov, "Lower bounds on the size of bounded depth circuits over a complete basis with logical addition," *Mathematical Notes of the Academy of Sciences of the USSR*, vol. 41, no. 4, 1987, pp. 333–338.

[101] A. A. Razborov, "Quantum communication complexity of symmetric predicates," *Izvestiya: Mathematics*, vol. 67, no. 1, 2003.

[102] A. A. Razborov and A. A. Sherstov, "The sign-rank of AC^0," *SIAM Journal on Computing*, vol. 39, no. 5, 2010, pp. 1833–1855.

[103] B. Reichardt, "Reflections for quantum query algorithms," in *Proceedings of the Twenty-Second Annual ACM-SIAM Symposium on Discrete Algorithms, SODA 2011, San Francisco, California, USA, January 23-25, 2011*, pp. 560–569, SIAM, 2011. DOI: 10.1137/1.9781611973082.44.

[104] F. Rosenblatt, "Principles of neurodynamics. perceptrons and the theory of brain mechanisms," Cornell Aeronautical Lab Inc Buffalo NY, Tech. Rep., 1961.

[105] B. Rossman, R. A. Servedio, and L. Tan, "Complexity theory column 89: The polynomial hierarchy, random oracles, and boolean circuits," *SIGACT News*, vol. 46, no. 4, 2015, pp. 50–68. DOI: 10.1145/2852040.2852052.

[106] A. A. Sherstov, "Halfspace matrices," *Computational Complexity*, vol. 17, no. 2, 2008, pp. 149–178.

[107] A. A. Sherstov, "The pattern matrix method," *SIAM Journal on Computing*, vol. 40, no. 6, 2011, pp. 1969–2000.

[108] A. A. Sherstov, "Making polynomials robust to noise," in *Symposium on Theory of Computing*, pp. 747–758, 2012.

[109] A. A. Sherstov, "Strong direct product theorems for quantum communication and query complexity," *SIAM Journal on Computing*, vol. 41, no. 5, 2012, pp. 1122–1165.

[110] A. A. Sherstov, "Approximating the AND-OR tree," *Theory of Computing*, vol. 9, no. 1, 2013, pp. 653–663.

[111] A. A. Sherstov, "Optimal bounds for sign-representing the intersection of two halfspaces by polynomials," *Combinatorica*, vol. 33, no. 1, 2013, pp. 73–96.

[112] A. A. Sherstov, "The intersection of two halfspaces has high threshold degree," *SIAM Journal on Computing*, vol. 42, no. 6, 2013, pp. 2329–2374.

[113] A. A. Sherstov, "Communication lower bounds using directional derivatives," *Journal of the ACM (JACM)*, vol. 61, no. 6, 2014, pp. 1–71.

[114] A. A. Sherstov, "Algorithmic polynomials," in *Symposium on Theory of Computing*, pp. 311–324, 2018.

[115] A. A. Sherstov, "Breaking the Minsky–Papert barrier for constant-depth circuits," *SIAM Journal on Computing*, vol. 47, no. 5, 2018, pp. 1809–1857.

[116] A. A. Sherstov, "On multiparty communication with large versus unbounded error," *Theory of Computing*, vol. 14, no. 1, 2018, pp. 1–17.

[117] A. A. Sherstov, "The power of asymmetry in constant-depth circuits," *SIAM Journal on Computing*, vol. 47, no. 6, 2018, pp. 2362–2434.

[118] A. A. Sherstov, "The hardest halfspace," *computational complexity*, vol. 30, no. 2, 2021, pp. 1–85.

[119] A. A. Sherstov, "The approximate degree of dnf and cnf formulas," in *Proceedings of the 54th Annual ACM SIGACT Symposium on Theory of Computing*, pp. 1194–1207, 2022.

[120] A. A. Sherstov and J. Thaler, "Vanishing-error approximate degree and qma complexity," *arXiv preprint arXiv:1909.07498*, 2019.

[121] A. A. Sherstov and P. Wu, "Near-optimal lower bounds on the threshold degree and sign-rank of AC^0," in *Symposium on Theory of Computing*, pp. 401–412, 2019.

[122] A. A. Sherstov, "Separating AC^0 from depth-2 majority circuits," *SIAM Journal on Computing*, vol. 38, no. 6, 2009, pp. 2113–2129.

[123] Y. Shi and Y. Zhu, "Quantum communication complexity of block-composed functions," *Quantum Information & Computation*, vol. 9, no. 5, 2009, pp. 444–460.

[124] R. Špalek, "A dual polynomial for OR," *arXiv preprint arXiv: 0803.4516*, 2008.

[125] A. Tal, "Formula lower bounds via the quantum method," in *Symposium on Theory of Computing*, pp. 1256–1268, 2017.

[126] J. Thaler, "Lower bounds for the approximate degree of block-composed functions," in *43rd International Colloquium on Automata, Languages, and Programming (ICALP 2016)*, Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik, 2016.

[127] J. Thaler, J. Ullman, and S. Vadhan, "Faster algorithms for privately releasing marginals," in *International Colloquium on Automata, Languages, and Programming*, pp. 810–821, 2012.

[128] L. G. Valiant, "A theory of the learnable," *Communications of the ACM*, vol. 27, no. 11, 1984, pp. 1134–1142.

[129] V. V. Vazirani, *Approximation algorithms*, vol. 1. Springer, 2001.

[130] M. Vyalyi, "QMA= PP implies that PP contains PH," in *ECCCTR: Electronic Colloquium on Computational Complexity, technical reports*, Citeseer, 2003.

[131] R. de Wolf, "A note on quantum algorithms and the minimal degree of epsilon-error polynomials for symmetric functions," *arXiv preprint arXiv:0802.1816*, 2008.

[132] A. C.-C. Yao, "Quantum circuit complexity," in *Proceedings of 1993 IEEE 34th Annual Foundations of Computer Science*, IEEE, pp. 352–361, 1993.

[133] M. Zhandry, "A note on the quantum collision and set equality problems," *Quantum Information & Computation*, vol. 15, no. 7&8, 2015, pp. 557–567.