Complexity Lower Bounds using Linear Algebra

Complexity Lower Bounds using Linear Algebra

Satyanarayana V. Lokam
Microsoft Research India
Bangalore – 560080
India
satya@microsoft.com

now
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
USA
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 S. V. Lokam, Complexity Lower Bounds using Linear Algebra, Foundation and Trends® in Theoretical Computer Science, vol 4, nos 1–2, pp 1–155, 2008

ISBN: 978-1-60198-242-1

Foundations and Trends® in Theoretical Computer Science

Volume 4 Issues 1–2, 2008

Editorial Scope

Foundations and Trends® in Theoretical Computer Science will publish 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, 2008, Volume 4, 4 issues. ISSN paper version 1551-305X. ISSN online version 1551-3068. Also available as a combined paper and online subscription.

Foundations and Trends® in
Theoretical Computer Science
Vol. 4, Nos. 1–2 (2008) 1–155
© 2009 S. V. Lokam
DOI: 10.1561/0400000011

now
the essence of knowledge

Complexity Lower Bounds using Linear Algebra

Satyanarayana V. Lokam

Microsoft Research India, Bangalore – 560080, India, satya@microsoft.com

Abstract

We survey several techniques for proving lower bounds in Boolean, algebraic, and communication complexity based on certain linear algebraic approaches. The common theme among these approaches is to study robustness measures of matrix rank that capture the complexity in a given model. Suitably strong lower bounds on such robustness functions of explicit matrices lead to important consequences in the corresponding circuit or communication models. Many of the linear algebraic problems arising from these approaches are independently interesting mathematical challenges.

Contents

1

Introduction

1.1 Scope

Understanding the inherent computational complexity of problems is of fundamental importance in mathematics and theoretical computer science. While rapid progress has been made on upper bounds (algorithms), progress on lower bounds on the complexity of explicit problems has remained slow despite intense efforts over several decades. As is natural with typical impossibility results, lower bound questions are hard mathematical problems and hence are unlikely to be resolved by *ad hoc* attacks. Instead, techniques based on mathematical notions that capture computational complexity are necessary.

This paper surveys some approaches based on linear algebra to proving lower bounds on computational complexity. Linear algebraic methods are extensively used in the study of algorithms and complexity. Our focus here is on their applications to lower bounds in various models of circuits and communication complexity. We further consider mainly classical — as opposed to quantum — models of computation. Linear algebra plays an obviously pervasive role in the study of quantum complexity. Indeed, some of the techniques studied in this paper have natural extensions to quantum models. However, to keep the scope of this survey narrow enough to limit its length, we restrict ourselves to classical models. Even within classical complexity theory, we do not touch upon several applications where linear algebra plays a critical role, most notably techniques related to spectra of graphs and coding theory. Our choice of topics is centered around the theme of deriving complexity lower bounds from lower bounds on ranks of matrices or dimensions of subspaces — often after the matrices or the subspaces are altered in various ways. Such a theme occurs in several contexts in complexity theory. The rough overall approach in this theme consists of (i) distilling a rank robustness or a dimension criterion to solve a lower bound problem in complexity, (ii) developing techniques to solve such linear algebraic problems, and (iii) exploring the consequent implications to complexity lower bounds.

In the remaining sub-sections of this section, we give a brief introduction and preview of the material to be presented in detail in the later sections.

1.2 Matrix Rigidity

The most classical notion of rank robustness is *matrix rigidity*. The rigidity of a matrix A for target rank r is the minimum Hamming distance between A and a matrix of rank at most r. Valiant [98] introduced this notion to define a criterion for proving superlinear size lower bounds on linear circuits of logarithmic depth. Linear circuits are algebraic circuits consisting only of gates that compute linear combinations of their inputs. This is a natural model for computing linear transformations. Given the ubiquitous role linear transformations play in computing, understanding the inherent complexity of explicit linear transformations is important. For example, a fascinating open question is whether the Fourier transform requires a superlinear number of arithmetic operations. Furthermore, no superlinear lower bounds are known on the algebraic circuit complexity of any explicit function of constant degree, even when the circuit depth is restricted to be logarithmic. Thus, a superlinear lower bound on the size of a log-depth linear circuit computing an explicit linear transformation would be significant. Valiant showed that if the rigidity of an $n \times n$ matrix A for target rank ϵn is at least $n^{1+\delta}$ for positive constants ϵ and δ, then a linear circuit of log-depth computing the linear transformation $x \mapsto Ax$ must have superlinear number of edges. Hence, proving sufficiently strong lower bounds on the rigidity of explicit matrices would yield important consequences in complexity theory. However, the best known lower bound on the rigidity of an explicit matrix is only $\Omega\left(\frac{n^2}{r} \log \frac{n}{r}\right)$ [31, 56, 93] for target rank r. This bound is known for several explicit matrices, including the Fourier transform matrix of a prime order. Using certain algebraic dimension arguments, rigidity lower bounds of $\Omega(n^2)$ (for target rank $r = \epsilon n$ for a constant $\epsilon > 0$) are proved in [59] for the matrices whose entries are square roots of distinct primes and for matrices whose entries are primitive roots of unity of the first n^2 prime orders. While these matrices are mathematically succinct enough to describe, they are not explicit enough since their entries live in number fields of exponentially large dimensions. In Section 2, we study the notion of rigidity and its application to lower bounds on linear circuits. We will give several lower bound proofs on the rigidity of various matrices and the implied circuit lower bounds. We will also review two notions of a geometric flavor [70] that are similar to rigidity and have applications to circuit lower bounds.

1.3 Spectral Techniques

Several rank robustness functions similar to rigidity have been defined in the literature and applied to derive lower bounds in complexity theory. In Section 3, we discuss several such variations. The simplest of them considers the ℓ_2-norm of changes needed to reduce the rank of a given matrix to a target rank (notions considered in Section 3 are defined over $\mathbb{R}$ or $\mathbb{C}$). This measure of rank robustness is effectively related to the singular values of the matrix and hence lower bounds are easily proved using spectral techniques [57]. Using spectral techniques, we can also prove lower bounds on the rigidity (in the sense of Valiant) of certain matrices. The most notable of these is an Hadamard matrix [26, 42], for which a lower bound of $\Omega(n^2/r)$ is known. Spectrum of a matrix is also related to values of its sub-determinants (volumes).

Lower bounds on these measures imply lower bounds on linear circuits (over $\mathbb{C}$) with *bounded coefficients*, i.e., the coefficients in the linear combinations computed by the gates in such a circuit are bounded by a constant. Algebraic circuits over $\mathbb{C}$ with bounded coefficients is a realistic restricted model of computation since real computers can only use arithmetic operations with bounded precision in a given step. Several lower bound results have been proved in the models of bounded coefficients [22, 24, 57, 69, 75, 83]. Indeed, a classical result in [65] gives an $\Omega(n \log n)$ lower bound on the size of a linear circuit with bounded coefficients (with no restriction on depth) computing the Fourier transform. In a more recent development, Raz [83] proved a remarkable lower bound of $\Omega(n^2 \log n)$ on $n \times n$ matrix multiplication in the model of *bilinear* circuits with bounded coefficients. Raz defines a geometric variant of ℓ_2-rigidity and uses spectral techniques to prove lower bounds on the linear circuits obtained when one of the matrices in the input to a bilinear circuit performing matrix multiplication is fixed. Subsequently, Bürgisser and Lotz [22] proved lower bounds on several bilinear transformations using spectral and volume techniques. We will describe these results as well in Section 3.

1.4 Sign-Rank

In Section 4, we study a rank robustness notion called the *sign-rank* of a matrix with ±1 entries. The sign-rank of a matrix A is the minimum rank of a real matrix each of whose entries agrees in sign with the corresponding entry of A. In other words, by making sign-preserving changes to A (changes are allowed to all entries of A), its rank cannot be brought down below its sign-rank. This notion was first introduced by Paturi and Simon [71] in the context of *unbounded error probabilistic communication complexity*. Proving nontrivial, i.e., superlogarithmic, lower bounds on sign ranks of explicit matrices remained a long-standing open question until Forster [28] achieved a breakthrough by proving that the sign-rank of an $n \times n$ Hadamard matrix is at least $\sqrt{n}$. Interestingly, Forster's result and subsequent techniques for proving lower bounds on sign-rank rely on spectral techniques. Forster also considers the notion of *margin complexity* from learning theory and uses the same techniques to prove lower bounds on margin complexity. Recent results in [53, 54, 55], give new insights into sign-rank, margin complexity, and discrepancy of sign matrices by studying them all in the framework of factorization norms of operators. This general approach reveals several connections among the various complexity measures of sign matrices and led to exciting new techniques to prove lower bounds on them. In particular, they show that the discrepancy and the margin of a sign matrix are within a constant factor of each other. Lower bounds on sign-rank, margin complexity, and discrepancy are immensely useful in proving lower bounds in a variety of models such as communication complexity, circuit complexity, and learning theory. We will discuss several such applications in Section 4. Very recently, Razborov and Sherstov [88] proved a very interesting lower bound on the sign-rank of a matrix constructed from a Boolean function in AC^0. As an immediate consequence, they show that Σ_2^{cc} (the communication complexity analog of the complexity class Σ_2) is not contained in the communication complexity class UPP defined by [71]. This solves a long-standing open question [5] in two-party communication complexity. The sign-rank lower bound of [88] also has interesting consequences to lower bounds on circuit complexity and learning theory. Their result combines Forster's main argument with a number of novel techniques including the use of the pattern matrix method [90]. These techniques usher in exciting new developments and are likely to find more applications.

1.5 Communication Complexity

Ever since Mehlhorn and Schmidt [63] proved the fundamental result that the log-rank of a 0–1 matrix is a lower bound on the two-party communication complexity of the associated Boolean function, the relation between rank, and more generally rank robustness, and communication complexity has been widely investigated and exploited. Yet, the most basic question of whether log-rank and communication complexity are polynomially related to each other is still open (this is also known as the log-rank conjecture). In this conjecture, rank over $\mathbb{R}$ is considered. We begin Section 5 by discussing what is known about this conjecture. Nisan and Wigderson [68] exhibit a Boolean matrix with communication complexity at least (log-rank)$^{\alpha}$, where $\alpha \approx \log_3 6$. They also show that, to prove that the communication complexity of *every* $\{0,1\}$-matrix is bounded above by some polynomial function of log-rank of the matrix, it suffices to show that every $\{0,1\}$-matrix of rank r contains a sufficiently large submatrix of rank at most, say $r/4$. On the other hand, Nisan and Wigderson [68] succeed in showing that low rank matrices have high discrepancy (under the uniform distribution) using spectral arguments. Proving upper bounds on discrepancy is a common and very useful method to prove lower bounds on *probabilistic* communication complexity. In the result mentioned earlier, Linial et al. [53] show that discrepancy (under any distribution) is at least $\Omega(r^{-1/2})$ for any rank-r $\{0,1\}$-matrix. The proof of this bound uses connections among discrepancy, rank, and factorization norms of matrices discussed in Section 4. Strengthening these connections, Linial and Shraibman [54] prove general lower bounds on the bounded error probabilistic and quantum communication complexity of a sign matrix in terms of a factorization norm, called the γ_2^{α}-norm, of the matrix. As we noted before, the log-sign-rank of a matrix is essentially equal to the unbounded error communication complexity of the matrix. We will also see that the communication complexity analog of PP is characterized by margin complexity. Thus rank robustness measures such as sign-rank and γ_2-norm of sign matrices yield lower bounds, sometimes even characterizations, of probabilistic communication complexity. Babai et al. [5] defined two-party communication complexity analogs of traditional complexity classes such as Σ_k, PH, PSPACE, etc. While analogs of low complexity classes such as P, NP, Co–NP, and BPP were all separated from each other in two-party communication complexity, questions such as PH versus PSPACE, Σ_2 vs. PH are still open. In [84] and [57], it was shown that sufficiently strong lower bounds on rigidity (over finite fields) and a variant of rigidity (over reals) with bounds on changes would separate PH and PSPACE in communication complexity. As mentioned before, a recent result in [88] separates Σ_2^{cc} from UPP by proving a strong lower bound on the sign-rank of an AC^0-function. We conclude that lower bounds on rank and rank robustness have significant consequences to various lower bound questions in two-party communication complexity.

1.6 Graph Complexity

Graph complexity was introduced by Pudlák et al. [79]. In this model, a graph — typically bipartite — on a vertex set V is constructed by starting from a family of basic graphs, e.g., complete bipartite graphs, on V and using the elementary operations of union and intersection on edge sets. The model of graph complexity is a common generalization of Boolean circuit and two-party communication complexity. In particular, proving sufficiently strong lower bounds on the complexity of explicit bipartite graphs would imply lower bounds on formula size complexity, branching program size, and two-party communication complexity of Boolean functions. Naturally, proving lower bounds in models of graph complexity is even harder than proving lower bounds in circuit and communication complexity models. However, graph–theoretic formulations of lower bound questions have the potential to lead to new insights. In particular, such formulations involving *linear algebraic* representations of graphs have led to new approaches to proving lower bounds on branching program size, formula size, and separation questions in two-party communication complexity. In Section 6, we review such approaches. A linear algebraic representation of a graph places a vector, or more generally a subspace, at each vertex of the graph such that the adjacency relations among vertices can be expressed, or implied, in terms of orthogonality or intersection properties of the associated subspaces. The lowest dimension in which such a representation can be realized for a given graph is the parameter of interest. Such representations have been extensively studied, e.g., in the context of the Shannon capacity of a graph [61], Colin de Verdière's invariant of graphs [45], etc. These and many similar combinatorial-linear algebraic problems are not only of inherent mathematical interest, but also have found numerous applications in algorithms and complexity. In Section 6, we define the affine and projective representations of graphs and pose questions about the lowest dimensions in which explicit graphs can be realized by such representations. Unfortunately, only weak lower bounds — $\Omega(\log n)$ for $n \times n$ explicit bipartite graphs — are known on these dimensions. Lower bounds exceeding $\Omega(\log^3 n)$ on the affine dimension of explicit graphs are needed to derive new lower bounds on the formula size of explicit Boolean functions. Pudlák and Rödl [76] showed that a lower bound on the projective dimension of a bipartite graph implies a lower bound on the branching program size of the associated Boolean function. In relating formula size of bipartite graphs (thereby deriving lower bounds on the associated Boolean functions) to affine dimension, Razborov [85] developed an elegant approach based on rectangle covers of matrices closely related to communication complexity. A rank robustness parameter (given a partially specified matrix, what is the minimum rank of a full matrix that completes it) plays a central role in establishing this connection. This same parameter and the underlying techniques are also used in characterizing the size of span programs in Section 7. Nontrivial lower bounds are known on graph complexity when we restrict the model to be of depth-3 graph formulas. In this case, building on polynomial approximations of the OR function and Forster's lower bound on the sign-rank of an Hadamard matrix, we show [58] $\tilde{\Omega}(\log^3 n)$ lower bounds on the depth-3 complexity of explicit bipartite graphs.

1.7 Span Programs

Karchmer and Wigderson [41] introduced a linear algebraic model of computation called *span programs*. A span program associates a subspace with each of the $2n$ literals of an n variable Boolean function. The result of its computation on a given input x is 1 if and only a fixed nonzero vector, e.g., the all 1's vector, is in the span of the subspaces "activated" by x. The sum of the dimensions of the subspaces is the *size* of the span program. Proving lower bounds on span program size of explicit Boolean functions is a challenging research direction since such results imply lower bounds on Boolean formulas, symmetric branching programs, algebraic proof systems, and secret sharing schemes. The model of span programs realizes the *fusion method* for proving circuit lower bounds [103]. Currently, superpolynomial lower bounds are known only on *monotone* span programs. Monotone span programs are more powerful than monotone Boolean circuits [6]. Hence, proving lower bounds on monotone span programs is more challenging. Early results in this area include a combinatorial criterion on certain bipartite graphs that led to $\Omega(n^{5/2})$ monotone size lower bounds [9]. Subsequently, Babai et al. [6] proved the first superpolynomial monotone lower bound of $n^{\Omega(\log n/\log\log n)}$ exploiting the criterion from [9] but using Paley-type graphs. The most striking result to date on span program size is by Gál [32] who proves a *characterization* of span program size in terms of a rank robustness measure originally introduced by Razborov [85] and referred to above in Section 1.6 and discussed in Section 6. Specializing this characterization to the monotone situation and using previously known lower bounds on the rank robustness measure of certain matrices derived from Paley-type bipartite graphs [85], Gál proved the best known lower bound of $n^{\Omega(\log n)}$ on monotone span programs. We discuss Gál's characterization and her lower bound in Section 7.

References

[1] M. Alekhnovich, “More on average case vs approximation complexity,” in *FOCS*, pp. 298–307, IEEE Computer Society, 2003.

[2] N. Alon, P. Frankl, and V. Rödl, “Geometric realizations of set systems and probabilistic communication complexity,” *Proceedings of the 26th IEEE Symposium on Foundations of Computer Science*, pp. 277–280, 1985.

[3] R. I. Arriaga and S. Vempala, “An algorithmic theory of learning: Robust concepts and random projection,” *IEEE Symposium on Foundations of Computer Science*, pp. 616–623, 1999.

[4] L. Babai and P. Frankl, *Linear Algebra Methods in Combinatorics, Preliminary version 2.* Department of Computer Science, University of Chicago, 1992.

[5] L. Babai, P. Frankl, and J. Simon, “Complexity classes in communication complexity theory,” *Proceedings of the 27th IEEE Symposium on Foundations of Computer Science*, pp. 337–347, 1986.

[6] L. Babai, A. Gál, and A. Wigderson, “Superpolynomial lower bounds for monotone span programs,” *Combinatorica*, vol. 19, no. 3, pp. 301–319, 1999.

[7] W. Baur, “Simplified lower bounds for polynomials with algebraic coefficients,” *Journal of Complexity*, vol. 13, pp. 38–41, 1997.

[8] W. Baur and V. Strassen, “The complexity of partial derivatives,” *Theoretical Computer Science*, vol. 22, pp. 317–330, 1983.

[9] A. Beimel, A. Gál, and M. Paterson, “Lower bounds for monotone span programs,” *Computational Complexity*, vol. 6, no. 1, pp. 29–45, 1996/97.

[10] A. Beimel and E. Weinreb, “Separting the power of monotone span programs over different fields,” *Proceedings of the 44th IEEE Symposium on Foundations of Computer Science*, pp. 428–437, 2003.

[11] S. Ben-David, N. Eiron, and H. U. Simon, "Limitations of learning via embeddings in Euclidean half spaces," *Journal of Machine Learning Research*, vol. 3, pp. 441–461, 2003.

[12] A. S. Besicovitch, "On the linear independence of fractional powers of integers," *Journal of the London Mathematical Society*, vol. 15, pp. 3–6, 1940.

[13] R. Bhatia, *Matrix Analysis.* Vol. 169 of *Graduate Texts in Mathematics*, New York, NY: Springer-Verlag, 1997.

[14] R. Blei, "An elementary proof of the grothendieck inequality," *Proceedings of the American Mathematical Society*, vol. 100, no. 1, pp. 58–60, 1987.

[15] B. Bollig, M. Sauerhoff, D. Sieling, and I. Wegener, "On the power of different types of restricted branching programs," *Electronic Colloquium on Computational Complexity (ECCC)*, vol. 1, no. 26, 1994.

[16] B. Bollobás, *Modern Graph Theory.* Vol. 184 of *Graduate Texts in Mathematics*, New York, NY: Springer-Verlag, 1998.

[17] B. Bollobás, *Linear Analysis.* Cambrdige Mathematical Textbooks. Cambridge Universty Press, Second ed., 1999.

[18] B. Bollobás, *Random Graphs.* Vol. 73 of *Cambrdige Studies in Advanced Mathematics*, Cambridge, United Kingdom: Cambridge University Press, Second ed., 2001.

[19] J. Bruck and R. Smolensky, "Polynomial threshold functions, AC^0 functions and spectral norms," *Proceedings of the 31st Symposium on Foundations of Computer Science*, pp. 632–641, 1990.

[20] P. Bürgisser, M. Clausen, and M. A. Shokhrollahi, *Algebraic Complexity Theory.* Springer-Verlag, 1997.

[21] P. Bürgisser and M. Lotz, "Lower bounds on the bounded coefficient complexity of bilinear maps," *Proceedings of the 43rd IEEE Symposium on Foundations of Computer Science*, pp. 659–668, 2002.

[22] P. Bürgisser and M. Lotz, "Lower bounds on the bounded coefficient complexity of bilinear maps," *Journal of the ACM*, vol. 51, no. 3, pp. 464–482, 2004.

[23] J.-Y. Cai and E. Bach, "On testing for zero polynomials by a set of points with bounded precision," *Theoretical Computer Science*, vol. 296, no. 1, pp. 15–25, 2003.

[24] B. Chazelle, "A spectral approach to lower bounds," *Proceedings of the 35th IEEE Symposium on Foundations of Computer Science*, pp. 674–682, 1994.

[25] Z. Chen and M. Kao, "Reducing randomness via irrational numbers," *Proceedings of the 29th Symposium Theory of Computing (STOC)*, pp. 200–209, 1997.

[26] R. de Wolf, "Lower bounds on matrix rigidity via a quantum argument," in *ICALP (1)*, (M. Bugliesi, B. Preneel, V. Sassone, and I. Wegener, eds.), pp. 62–71, Vol. 4051 of *Lecture Notes in Computer Science*, Springer, 2006.

[27] P. Erdős, R. Graham, and E. Szemerédi, "On sparse graphs with dense long paths," *Computers and Mathematics with Applications*, pp. 365–369, 1976.

[28] J. Forster, "A linear lower bound on the unbounded error probabilistic communication complexity," *Journal of Computer and System Sciences*, vol. 65, no. 4, pp. 612–625, Special issue on Complexity, (Chicago, IL, 2001), 2002.

[29] J. Forster, M. Krause, S. V. Lokam, R. Mubarakzjanov, N. Schmitt, and H. U. Simon, "Relations between communication complexity, linear arrangements, and computational complexity," in *FST TCS 2001: Foundations of Software Technology and Theoretical Computer Science (Bangalore)*, pp. 171–182, Vol. 2245 of *Lecture Notes in Computer Science*, Berlin: Springer, 2001.

[30] J. Forster and H.-U. Simon, "On the smallest possible dimension and the largest possible margin of linear arrangements representing given concept classes," *Theoretical Computer Science*, vol. 350, no. 1, pp. 40–48, 2006.

[31] J. Friedman, "A note on matrix rigidity," *Combinatorica*, vol. 13, no. 2, pp. 235–239, 1993.

[32] A. Gál, "A characterization of span program size and improved lower bounds for monotone span programs," *Computational Complexity*, vol. 10, no. 4, pp. 277–296, 2001.

[33] G. H. Golub and C. F. Van Loan, *Matrix Computations.* The Johns Hopkins University Press, Third ed., 1996.

[34] D. Grigoriev, "Using the notions of separability and indepndence for proving lower bounds on the circuit complexity," *Notes of the Leningrad Branch of the Steklov Mathematical Institute*, 1976.

[35] A. Hajnal, W. Maass, P. Pudlák, M. Szegedy, and G. Turan, "Threshold functions of bounded depth," *Journal of Computer and System Sciences*, vol. 46, pp. 129–154, 1993.

[36] B. Halstenberg and R. Reischuk, "Relations between communication complexity classes," *Journal of Computer and System Sciences*, vol. 41, pp. 402–429, 1990.

[37] J. Håstad and A. Wigderson, "The randomized communication complexity of set disjointness," *Theory of Computing*, vol. 3, no. 1, pp. 211–219, 2007.

[38] A. J. Hoffman and H. W. Wielandt, "The variation of the spectrum of a normal matrix," *Duke Mathematical Journal*, vol. 20, pp. 37–39, 1953.

[39] R. A. Horn and C. R. Johnson, *Matrix Analysis.* Cambridge University Press, February 1990.

[40] M. Karchmer and A. Wigderson, "Monotone circuits for connetivity require super-logarithmic depth," *SIAM Journal on Discrete Mathematics*, vol. 3, no. 2, pp. 255–265, 1990.

[41] M. Karchmer and A. Wigderson, "On span programs," in *Proceedings of the 8th Annual Structure in Complexity Theory Conference (San Diego, CA, 1993)*, pp. 102–111, Los Alamitos, CA, 1993. IEEE Computer Society Press.

[42] B. S. Kashin and A. A. Razborov, "Improved lower bounds on the rigidity of hadamard matrices," *Matematicheskie Zametki*, vol. 63, no. 4, pp. 535–540, English translation at http://www.mi.ras.ru/ razborov/hadamard.ps, 1998.

[43] H. Klauck, "Lower bounds for quantum communication complexity," *SIAM Journal on Computing*, vol. 37, no. 1, pp. 20–46, 2007.

[44] 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, pp. 303–318, 2004.

[45] A. Kotlov, L. Lovász, and S. Vempala, "The Colin de Verdière number and sphere representations of a graph," *Combinatorica*, vol. 17, pp. 483–521, 1997.

[46] M. Krause, "Geometric arguments yield better bounds for threshold circuits and distributed computing," *Theoretical Computer Science*, vol. 156, nos. 1&2, pp. 99–117, 1996.

[47] M. Krause and P. Pudlák, "On the computational power of depth 2 circuits with threshold and modulo gates," *STOC*, pp. 48–57, 1994.

[48] E. Kushilevitz and N. Nisan, *Communication Complexity*. Cambridge University Press, 1997.

[49] E. Kushilevitz and E. Weinreb, "On the complexity of communication complexity," *STOC 2009*, 2009.

[50] S. Lang, *Algebra*. Addison-Wesley Publishing Company, Third ed., 1993.

[51] D. Lewin and S. Vadhan, "Checking polynomial identities over any field: Towards a derandomization?," *Proceedings of the 30th Symposium on Theory of Computing (STOC)*, pp. 438–447, 1998.

[52] T. Lickteig, *Ein elementarer Beweis für eine geometrische Gradschranke für die Zahl der Operationen bei der Berechnung von Polynomen*. Diplomarbeit, Universität Konstanz, 1980.

[53] N. Linial, S. Mendelson, G. Schechtman, and A. Shraibman, "Complexity measures of sign matrices," *Combinatorica*, 2006.

[54] N. Linial and A. Shraibman, "Lower bounds in communication complexity based on factorization norms," in *STOC '07: Proceedings of the 39th Annual ACM Symposium on Theory of Computing*, pp. 699–708, New York, NY, USA: ACM, 2007.

[55] N. Linial and A. Shraibman, "Learning complexity vs communication complexity," *CCC '08: Conference on Computational Complexity*, 2008.

[56] S. V. Lokam, "On the rigidity of Vandermonde matrices," *Theoretical Computer Science*, vol. 237, nos. 1–2, pp. 477–483, Presented at the DIMACS-DIMATIA workshop on *Arithmetic Circuits and Algebraic Methods, June, 1999*, 2000.

[57] S. V. Lokam, "Spectral methods for matrix rigidity with applications to size-depth trade-offs and communication complexity," *Journal of Computer and System Sciences*, vol. 63, no. 3, pp. 449–473, 2001.

[58] S. V. Lokam, "Graph complexity and slice functions," *Theory of Computing Systems*, vol. 36, no. 1, pp. 71–88, 2003.

[59] S. V. Lokam, "Quadratic lower bounds on matrix rigidity," *Proceedings of Theory and Applications of Models of Computation (TAMC)*, vol. 3959, pp. 295–307, *Lecture Notes in Computer Science*, 2006.

[60] L. Lovász, "On the ratio of optimal integral and fractional covers," *Discrete Mathematics*, vol. 13, no. 4, pp. 383–390, 1975.

[61] L. Lovász, "On the shannon capacity of a graph," *IEEE Transactions on Information Theory*, vol. 25, pp. 1–7, 1979.

[62] L. Lovász and M. Saks, "Communication complexity and combinatorial lattice theory," *Journal of Computer and System Sciences*, vol. 47, no. 2, pp. 322–349, *29th Annual IEEE Symposium on Foundations of Computer Science*. White Plains, NY, 1988, 1993.

[63] K. Mehlhorn and E. M. Schmidt, "Las Vegas is better than determinism in VLSI and distributed computing (Extended Abstract)," in *STOC*, pp. 330–337, ACM, 1982.

[64] G. Midrijanis, "Three lines proof of the lower bound for the matrix rigidity," *CoRR*, vol. abs/cs/0506081, 2005.

[65] J. Morgenstern, "Note on a lower bound of the linear complexity of the fast Fourier transform," *Journal of the ACM*, vol. 20, no. 2, pp. 305–306, 1973.

[66] N. Nisan and M. Szegedy, "On the degree of boolean functions as real polynomials," *Computational Complexity*, vol. 4, pp. 301–313, 1994.

[67] N. Nisan and A. Wigderson, "Lower bounds on arithmetic circuits via partial derivatives," *Proceedings of the 36th IEEE Symposium on Foundations of Computer Science*, pp. 16–25, 1995.

[68] N. Nisan and A. Wigderson, "On rank vs communication complexity," *Combinatorica*, vol. 15, no. 4, pp. 557–565, 1995.

[69] N. Nisan and A. Wigderson, "On the complexity of bilinear forms," *Proceedings of the 27th ACM Symposium on the Theory of Computing*, pp. 723–732, 1995.

[70] R. Paturi and P. Pudlák, "Circuit lower bounds and linear codes," in *Teoria Slozhnosti Vychislenij IX*, (E. A. Hirsch, ed.), Vol. 316, pp. 188–204, Notes of Mathematical Seminars of St. Petersburg Department of Steklov Institute of Mathematics, 2004.

[71] R. Paturi and J. Simon, "Probabilistic communication complexity," *Journal of Computer and System Sciences*, vol. 33, no. 1, pp. 106–123, *25th Annual Symposium on Foundations of Computer Science* (Singer Island, Florida, 1984), 1986.

[72] N. Pippenger, "Superconcentrators," *SIAM Journal on Computing*, vol. 6, no. 2, pp. 298–304, 1977.

[73] G. Pólya and G. Szegö, *Problems and Theorems in Analysis, Volume II.* New York, NY: Springer-Verlag, 1976.

[74] P. Pudlák, "Large communication in constant depth circuits," *Combinatorica*, vol. 14, no. 2, pp. 203–216, 1994.

[75] P. Pudlák, "A note on the use of determinant for proving lower bounds on the size of linear circuits," *Electronic Colloquium on Computational Complexity (ECCC)*, 1998.

[76] P. Pudlák and V. Rödl, "A combinatorial approach to complexity," *Combinatorica*, vol. 12, no. 2, pp. 221–226, 1992.

[77] P. Pudlák and V. Rödl, "Modified ranks of tensors and the size of circuits," *Proceedings of the 25th ACM Symposium on the Theory of Computing*, pp. 523–531, 1993.

[78] P. Pudlák and V. Rödl, "Some combinatorial-algebraic problems from complexity theory," *Discrete Mathematics*, vol. 136, nos. 1–3, pp. 253–279, Trends in discrete mathematics, 1994.

[79] P. Pudlák, V. Rödl, and P. Savický, "Graph complexity," *Acta Informatica*, vol. 25, no. 5, pp. 515–535, 1988.

[80] P. Pudlák, V. Rödl, and J. Sgall, "Boolean circuits, tensor ranks and communication complexity," *Manuscript*, March 1994.

[81] P. Pudlák and Z. Vavřín, "Computation of rigidity of order n^2/r for one simple matrix," *Commentationes Mathematicae Universitatis Carolinae*, vol. 32, no. 2, pp. 213–218, 1991.

[82] J. Radhakrishnan and A. Ta-Shma, "Bounds for dispersers, extractors, and depth-two superconcentrators," *SIAM Journal on Discrete Mathematics*, vol. 13, no. 1, pp. 2–24 (electronic), 2000.

[83] R. Raz, "On the complexity of matrix product," in *Proceedings of the 34th Annual ACM Symposium on Theory of Computing*, pp. 144–151, ACM Press, 2002.

[84] A. A. Razborov, "On rigid matrices," *Manuscript, (Russian)*, 1989.

[85] A. A. Razborov, "Applications of matrix methods to the theory of lower bounds in computational complexity," *Combinatorica*, vol. 10, no. 1, pp. 81–93, 1990.

[86] A. A. Razborov, "A note on the use of determinant for proving lower bounds on the size of linear circuits," *Electronic Colloquium on Computational Complexity (ECCC)*, 1998.

[87] A. A. Razborov and S. Rudich, "Natural proofs," *Journal of Computer and System Sciences*, vol. 55, no. 1, part 1, pp. 24–35, *26th Annual ACM Symposium on the Theory of Computing (STOC '94)* (Montreal, PQ, 1994), 1997.

[88] A. A. Razborov and A. A. Sherstov, "The sign-rank of AC^0," *FOCS 2008, Proceedings of Symposium on Foundations of Computer Science*, 2008.

[89] L. Rónyai, L. Babai, and M. K. Ganapathy, "On the number of zero-patterns of a sequence of polynomials," *Journal of the American Mathematical Society*, vol. 14, no. 3, pp. 717–735 (electronic), 2001.

[90] A. A. Sherstov, "The pattern matrix method for lower bounds on quantum communication," in *STOC*, (R. E. Ladner and C. Dwork, eds.), pp. 85–94, ACM, 2008.

[91] V. Shoup and R. Smolensky, "Lower bounds for polynomial evaluation and interpolation," *Proceedings of the 32nd IEEE Symposium on Foundations of Computer Science*, pp. 378–383, 1991.

[92] J. W. Silverstein, "The smallest eigenvalue of a large dimensional wishart matrix," *The Annals of Probability*, vol. 13, no. 4, pp. 1364–1368, 1985.

[93] D. A. Spielman, V. Stemann, and M. A. Shokhrollahi, "A remark on matrix rigidity," *Information Processing Letters*, vol. 64, no. 6, pp. 283–285, 1997.

[94] P. Stevenhagen and H. W. Lenstr Jr., "Chebotarëv and his density theorem," *Mathematical Intelligencer*, vol. 18, no. 2, pp. 26–37, 1996.

[95] G. W. Stewart and J.-G. Sun, *Matrix Perturbation Theory.* Academic Press, 1990.

[96] T. Tao, "An uncertainty principle for cyclic groups of prime order," *Mathematical Research Letters*, vol. 12, pp. 121–127, 2005.

[97] J. Tarui, "Randomized polynomials, threshold circuits and polynomial hierarchy," *Theoretical Computer Science*, vol. 113, pp. 167–183, 1993.

[98] L. Valiant, "Graph–theoretic arguments in low-level complexity," in *Proceedings of the 6th Symposium on Mathematical Foundations of Computer Science*, pp. 121–127, 1977. *Lecture Notes in Computer Science.*

[99] V. Vapnik, *The Nature of Statistical Learning Theory.* Springer-Verlag, 1999. ISBN 0-387-98780-0.

[100] K. R. Varadarajan, S. Venkatesh, Y. Ye, and J. Zhang, "Approximating the radii of point sets," *SIAM Journal on Computing*, vol. 36, no. 6, pp. 1764–1776, 2007.

[101] J. von zur Gathen and J. Gerhard, *Modern Computer Algebra.* Cambridge University Press, 1999.

[102] H. E. Warren, “Lower bounds for approximation by nonlinear manifolds,” *Transactions of the American Mathematical Society*, vol. 133, pp. 167–178, 1968.

[103] A. Wigderson, “The fusion method for lower bounds in circuit complexity,” in *Combinatorics, Paul Erdős is Eighty,* Vol. 1, pp. 453–468, Budapest: János Bolyai Mathematical Society, Bolyai Society Mathematical Studies, 1993.

[104] A. C.-C. Yao, “Some complexity questions related to distributive computing,” *Proceedings of the 11th ACM Symposium on the Theory of Computing*, pp. 209–213, 1979.