Full text available at: http://dx.doi.org/10.1561/0400000010

Pseudorandomness

Full text available at: http://dx.doi.org/10.1561/0400000010

Pseudorandomness

Salil P. Vadhan

Harvard University
Cambridge, MA 02138
USA
salil@seas.harvard.edu

the essence of knowledge

Boston – Delft

Full text available at: http://dx.doi.org/10.1561/0400000010

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. P. Vadhan, Pseudorandomness, Foundation and Trends® in Theoretical Computer Science, vol 7, nos 1–3, pp 1–336, 2011

ISBN: 978-1-60198-594-1
© 2012 S. P. Vadhan

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, mechanical, photocopying, recording or otherwise, without prior written permission of the publishers.

Photocopying. In the USA: This journal is registered at the Copyright Clearance Center, Inc., 222 Rosewood Drive, Danvers, MA 01923. Authorization to photocopy items for internal or personal use, or the internal or personal use of specific clients, is granted by now Publishers Inc. for users registered with the Copyright Clearance Center (CCC). The 'services' for users can be found on the internet at: www.copyright.com

For those organizations that have been granted a photocopy license, a separate system of payment has been arranged. Authorization does not extend to other kinds of copying, such as that for general distribution, for advertising or promotional purposes, for creating new collective works, or for resale. In the rest of the world: Permission to photocopy must be obtained from the copyright owner. Please apply to now Publishers Inc., PO Box 1024, Hanover, MA 02339, USA; Tel. +1-781-871-0245; www.nowpublishers.com; sales@nowpublishers.com

now Publishers Inc. has an exclusive license to publish this material worldwide. Permission to use this content must be obtained from the copyright license holder. Please apply to now Publishers, PO Box 179, 2600 AD Delft, The Netherlands, www.nowpublishers.com; e-mail: sales@nowpublishers.com

Full text available at: http://dx.doi.org/10.1561/0400000010

Foundations and Trends® in Theoretical Computer Science
Volume 7 Issues 1–3, 2011

Editorial Board

Editor-in-Chief:
Madhu Sudan
Microsoft Research New England
One Memorial Drive
Cambridge, Massachusetts 02142
USA

Editors
Bernard Chazelle (Princeton)
Oded Goldreich (Weizmann Inst.)
Shafi Goldwasser (MIT and Weizmann Inst.)
Jon Kleinberg (Cornell University)
László Lovász (Microsoft Research)
Christos Papadimitriou (UC. Berkeley)
Prabhakar Raghavan (Yahoo! Research)
Peter Shor (MIT)
Madhu Sudan (Microsoft Research)
Éva Tardos (Cornell University)
Avi Wigderson (IAS)

Full text available at: http://dx.doi.org/10.1561/0400000010

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, 2011, Volume 7, 4 issues. ISSN paper version 1551-305X. ISSN online version 1551-3068. Also available as a combined paper and online subscription.

Full text available at: http://dx.doi.org/10.1561/0400000010

Foundations and Trends® in
Theoretical Computer Science
Vol. 7, Nos. 1–3 (2011) 1–336
© 2012 S. P. Vadhan
DOI: 10.1561/0400000010

now
the essence of knowledge

Pseudorandomness

Salil P. Vadhan

School of Engineering and Applied Sciences, Harvard University, Cambridge, MA, 02138, USA, salil@seas.harvard.edu

Abstract

This is a survey of *pseudorandomness*, the theory of efficiently generating objects that "look random" despite being constructed using little or no randomness. This theory has significance for a number of areas in computer science and mathematics, including computational complexity, algorithms, cryptography, combinatorics, communications, and additive number theory. Our treatment places particular emphasis on the intimate connections that have been discovered between a variety of fundamental "pseudorandom objects" that at first seem very different in nature: expander graphs, randomness extractors, list-decodable error-correcting codes, samplers, and pseudorandom generators. The structure of the presentation is meant to be suitable for teaching in a graduate-level course, with exercises accompanying each section.

Full text available at: http://dx.doi.org/10.1561/0400000010

Contents

Full text available at: http://dx.doi.org/10.1561/0400000010

Full text available at: http://dx.doi.org/10.1561/0400000010

Full text available at: http://dx.doi.org/10.1561/0400000010

1

Introduction

1.1 Overview of this Survey

Over the past few decades, *randomization* has become one of the most pervasive paradigms in computer science. Its widespread uses include:

Algorithm Design: For a number of important algorithmic problems, the most efficient algorithms known are randomized. For example:

- Primality Testing: This was shown to have a randomized polynomial-time algorithm in 1977. It wasn't until 2002 that a deterministic polynomial-time algorithm was discovered. (We will see this algorithm, but not its proof.)
- *Approximate Counting*: Many approximate counting problems (e.g., counting perfect matchings in a bipartite graph) have randomized polynomial-time algorithms, but the fastest known deterministic algorithms take exponential time.
- Undirected S-T Connectivity: This was shown to have a randomized logspace algorithm in 1979. It wasn't until 2005 that a deterministic logspace algorithm was discovered — using tools from the theory of pseudorandomness, as we will see.

Full text available at: http://dx.doi.org/10.1561/0400000010

- Perfect Matching: This was shown to have a randomized *polylogarithmic*-time parallel algorithm in the late 1970s. Deterministically, we only know polynomial-time algorithms.

Even in the cases where deterministic algorithms of comparable complexity were eventually found, the randomized algorithms remain considerably simpler and more efficient than the deterministic ones.

Cryptography: Randomization is central to cryptography. Indeed, cryptography is concerned with protecting secrets, and how can something be secret if it is deterministically fixed? For example, we assume that cryptographic keys are chosen at random (e.g., uniformly from the set of n-bit strings). In addition to the keys, it is known that often the cryptographic algorithms themselves (e.g., for encryption) must be randomized to achieve satisfactory notions of security (e.g., that no partial information about the message is leaked).

Combinatorial Constructions: Randomness is often used to prove the *existence* of combinatorial objects with a desired property. Specifically, if one can show that a randomly chosen object has the property with nonzero probability, then it follows that such an object must, in fact, exist. A famous example due to Erdős is the existence of *Ramsey graphs*: A randomly chosen n-vertex graph has no clique or independent set of size $2\log n$ with high probability. We will see several other applications of this "Probabilistic Method" in this survey, such as with two important objects mentioned below: expander graphs and error-correcting codes.

Though these *applications* of randomness are interesting and rich topics of study in their own right, they are not the focus of this survey. Rather, we ask the following:

Main Question: Can we reduce or even eliminate the use of randomness in these settings?

We have several motivations for doing this.

- *Complexity Theory*: We are interested in understanding and comparing the power of various kinds of computational resources. Since randomness is such a widely used resource,

Full text available at: http://dx.doi.org/10.1561/0400000010

we want to know how it relates to other resources such as time, space, and parallelism. In particular, we ask: *Can every randomized algorithm be derandomized with only a small loss in efficiency?*

- *Using Physical Random Sources*: It is unclear whether the real world has physical sources of perfect randomness. We may use sources that seem to have some unpredictability, like the low order bits of a system clock or thermal noise, but these sources will generally have biases and, more problematically, correlations. Thus we ask: What can we do with a source of biased and correlated bits?
- *Explicit Constructions*: Probabilistic constructions of combinatorial objects often do not provide us with efficient algorithms for using those objects. Indeed, the randomly chosen object often has a description that is exponential in the relevant parameters. Thus, we look for *explicit* constructions — ones that are deterministic and efficient. In addition to their applications, improvements in explicit constructions serve as a measure of our progress in understanding the objects at hand. Indeed, Erdős posed the explicit construction of near-optimal Ramsey graphs as an open problem, and substantial progress on this problem was recently made using the theory of pseudorandomness (namely randomness extractors).
- *Unexpected Applications*: In addition, the theory of pseudorandomness has turned out to have many applications to problems that seem to have no connection to derandomization. These include data structures, distributed computation, circuit lower bounds and completeness results in complexity theory, reducing interaction in interactive protocols, saving memory in streaming algorithms, and more. We will see some of these applications in this survey (especially the exercises).

The paradigm we will use to study the Main Question is that of *pseudorandomness*: efficiently generating objects that "look random" using little or no randomness.

Full text available at: http://dx.doi.org/10.1561/0400000010

Specifically, we will study four "pseudorandom" objects:

Pseudorandom Generators: A pseudorandom generator is an algorithm that takes as input a short, perfectly random *seed* and then returns a (much longer) sequence of bits that "looks random." That the bits output cannot be perfectly random is clear — the output is determined by the seed and there are far fewer seeds than possible bit sequences. Nevertheless, it is possible for the output to "look random" in a very meaningful and general-purpose sense. Specifically, we will require that no *efficient* algorithm can distinguish the output from a truly random sequence. The study of pseudorandom generators meeting this strong requirement originated in cryptography, where they have numerous applications. In this survey, we will emphasize their role in derandomizing algorithms.

Note that asserting that a function is a pseudorandom generator is a statement about something that efficient algorithms can't do (in this case, distinguish two sequences). But proving that efficient algorithms cannot compute things is typically out of reach for current techniques in theoretical computer science; indeed this is why the **P** vs. **NP** question is so hard. Thus, we will settle for conditional statements. An ideal theorem would be something like: "If $\mathbf{P} \neq \mathbf{NP}$, then pseudorandom generators exist." (The assumptions we make won't exactly be $\mathbf{P} \neq \mathbf{NP}$, but hypotheses of a similar flavor.)

Randomness Extractors: A randomness extractor takes as input a source of biased and correlated bits, and then produces a sequence of almost-uniform bits as output. Their original motivation was the simulation of randomized algorithms with sources of biased and correlated bits, but they have found numerous other applications in theoretical computer science. Ideally, extractors would be deterministic, but as we will see this proves to be impossible for general sources of biased and correlated bits. Nevertheless, we will get close — constructing extractors that are only "mildly" probabilistic, in that they use small (logarithmic) number of truly random bits as a seed for the extraction.

Expander Graphs: Expanders are graphs with two seemingly contradictory properties: they are sparse (e.g., having degree that is

Full text available at: http://dx.doi.org/10.1561/0400000010

a constant, independent of the number of vertices), but also "well-connected" in some precise sense. For example, the graph cannot be bisected without cutting a large (say, constant) fraction of the edges.

Expander graphs have numerous applications in theoretical computer science. They were originally studied for their use in designing fault-tolerant networks (e.g., for telephone lines), ones that maintain good connectivity even when links or nodes fail. But they also have less obvious applications, such as an $O(\log n)$-time algorithm for sorting in parallel.

It is not obvious that expander graphs exist, but in fact it can be shown, via the Probabilistic Method, that a random graph of degree 3 is a "good" expander with high probability. However, many applications of expander graphs need *explicit constructions*, and these have taken longer to find. We will see some explicit constructions in this survey, but even the state-of-the-art does not always match the bounds given by the probabilistic method (in terms of the degree/expansion tradeoff).

Error-Correcting Codes: Error-correcting codes are tools for communicating over noisy channels. Specifically, they specify a way to encode messages into longer, redundant codewords so that even if the codeword gets somewhat corrupted along the way, it is still possible for the receiver to decode the original message. In his landmark paper that introduced the field of coding theory, Shannon also proved the existence of good error-correcting codes via the Probabilistic Method. That is, a random mapping of n-bit messages to $O(n)$-bit codewords is a "good" error-correcting code with high probability. Unfortunately, these probabilistic codes are not feasible to actually use — a random mapping requires an exponentially long description, and we know of no way to decode such a mapping efficiently. Again, explicit constructions are needed.

In this survey, we will focus on the problem of *list decoding*. Specifically, we will consider scenarios where the number of corruptions is so large that unique decoding is impossible; at best one can produce a short list that is guaranteed to contain the correct message.

A Unified Theory: Each of the above objects has been the center of a large and beautiful body of research, but until recently these corpora

Full text available at: http://dx.doi.org/10.1561/0400000010

were largely distinct. An exciting development over the past decade has been the realization that all four of these objects are almost *the same* when interpreted appropriately. Their intimate connections will be a major focus of this survey, tying together the variety of constructions and applications that we will see.

The surprise and beauty of these connections has to do with the seemingly different nature of each of these objects. Pseudorandom generators, by asserting what efficient algorithms cannot do, are objects of complexity theory. Extractors, with their focus on extracting the entropy in a correlated and biased sequence, are information-theoretic objects. Expander graphs are of course combinatorial objects (as defined above), though they can also be interpreted algebraically, as we will see. Error-correcting codes involve a mix of combinatorics, information theory, and algebra. Because of the connections, we obtain new perspectives on each of the objects, and make substantial advances on our understanding of each by translating intuitions and techniques from the study of the others.

1.2 Background Required and Teaching Tips

The presentation assumes a good undergraduate background in the theory of computation, and general mathematical maturity. Specifically, it is assumed that the reader is familiar with basic algorithms and discrete mathematics as covered in [109], including some exposure to randomized algorithms; and with basic computational complexity including P, NP, and reductions, as covered in [366]. Experience with elementary abstract algebra, particularly finite fields, is helpful; recommended texts are [36, 263].

Most of the material in the survey is covered in a one-semester graduate course that the author teaches at Harvard University, which consists of 24 lectures of 1.5 hours each. Most of the students in that course take at least one graduate-level course in theoretical computer science before this one.

The exercises are an important part of the survey, as they include proofs of some key facts, introduce some concepts that will be used in later sections, and illustrate applications of the material to other topics.

Full text available at: http://dx.doi.org/10.1561/0400000010

Problems that are particularly challenging or require more creativity than most are marked with a star.

1.3 Notational Conventions

We denote the set of numbers $\{1,\ldots,n\}$ by $[n]$. We write $\mathbb{N}$ for the set of nonnegative integers (so we consider 0 to be a natural number). We write $S \subset T$ to mean that S is a subset of T (not necessarily strict), and $S \subsetneq T$ for S being a strict subset of T. An inequality we use often is $\binom{n}{k} \leq (ne/k)^k$. All logarithms are base 2 unless otherwise specified. We often use the convention that lowercase letters are the logarithm (base 2) of the corresponding capital letter (e.g., $N = 2^n$).

Throughout, we consider random variables that can take values in arbitrary discrete sets (as well as real-valued random variables). We generally use capital letters, e.g., X, to denote random variables and lowercase letters, e.g., x, to denote specific values. We write $x \xleftarrow{R} X$ to indicate that x is sampled according to X. For a set S, we write $x \xleftarrow{R} S$ to mean that x is selected uniformly at random from S. We use the convention that multiple occurrences of a random variable in an expression refer to the same instantiation, e.g., $\Pr[X = X] = 1$. The *support* of a random variable X is denoted by $\mathrm{Supp}(X) \stackrel{\text{def}}{=} \{x : \Pr[X = x] > 0\}$. For an event E, we write $X|_E$ to denote the random variable X conditioned on the event E. For a set S, we write U_S to denote a random variable distributed uniformly over S. For $n \in \mathbb{N}$, U_n is a random variable distributed uniformly over $\{0,1\}^n$.

1.4 Chapter Notes and References

In this section, we only provide pointers to general surveys and textbooks on the topics covered, plus citations for specific results mentioned.

General introductions to the theory of pseudorandomness (other than this survey) include [162, 288, 393].

Recommended textbooks focused on randomized algorithms are [290, 291]. The specific randomized and deterministic algorithms

Full text available at: http://dx.doi.org/10.1561/0400000010

mentioned are due to [6, 13, 220, 236, 237, 267, 287, 314, 327, 369]; for more details see Section 2.6.

Recommended textbooks on cryptography are [157, 158, 238]. The idea that encryption should be randomized is due to Goldwasser and Micali [176].

The Probabilistic Method for combinatorial constructions is the subject of the book [25]. Erdős used this method to prove the existence of Ramsey graphs in [132]. Major recent progress on explicit constructions of Ramsey graphs was recently obtained by Barak, Rao, Shaltiel, and Widgerson [48] via the theory of randomness extractors.

The modern notion of a pseudorandom generator was formulated in the works of Blum and Micali [72] and Yao [421], motivated by cryptographic applications. We will spend most of our time on a variant of the Blum–Micali–Yao notion, proposed by Nisan and Wigderson [302], where the generator is allowed more running time than the algorithms it fools. A detailed treatment of the Blum–Micali–Yao notion can be found in [157].

Surveys on randomness extractors are [301, 352, 354]. The notion of extractor that we will focus on is the one due to Nisan and Zuckerman [303].

A detailed survey of expander graphs is [207]. The probabilistic construction of expander graphs is due to Pinsker [309]. The application of expanders to sorting in parallel is due to Ajtai, Komlós, and Szemerédi [10].

A classic text on coding theory is [282]. For a modern, computer science-oriented treatment, we recommend Sudan's lecture notes [380]. Shannon started this field with the paper [361]. The notion of list decoding was proposed by Elias [129] and Wozencraft [420], and was reinvigorated in the work of Sudan [378]. Recent progress on list decoding is covered in [184].

Full text available at: http://dx.doi.org/10.1561/0400000010

References

[1] S. Aaronson and D. van Melkebeek, "On circuit lower bounds from derandomization," *Theory of Computing. An Open Access Journal*, vol. 7, pp. 177–184, 2011.

[2] M. Abadi, J. Feigenbaum, and J. Kilian, "On hiding information from an oracle," *Journal of Computer and System Sciences*, vol. 39, no. 1, pp. 21–50, 1989.

[3] L. Adleman, "Two theorems on random polynomial time," in *Annual Symposium on Foundations of Computer Science (Ann Arbor, Mich., 1978)*, pp. 75–83, Long Beach, California, 1978.

[4] M. Agrawal, "On derandomizing tests for certain polynomial identities," in *IEEE Conference on Computational Complexity*, pp. 355–, 2003.

[5] M. Agrawal and S. Biswas, "Primality and identity testing via Chinese remaindering," *Journal of the ACM*, vol. 50, no. 4, pp. 429–443, 2003.

[6] M. Agrawal, N. Kayal, and N. Saxena, "PRIMES is in P," *Annals of Mathematics. Second Series*, vol. 160, no. 2, pp. 781–793, 2004.

[7] M. Agrawal and V. Vinay, "Arithmetic circuits: A chasm at depth four," in *FOCS*, pp. 67–75, 2008.

[8] A. V. Aho, ed., *Proceedings of the Annual ACM Symposium on Theory of Computing, 1987*, New York, USA, 1987.

[9] M. Ajtai, H. Iwaniec, J. Komlós, J. Pintz, and E. Szemerédi, "Construction of a thin set with small Fourier coefficients," *Bulletin of the London Mathematical Society*, vol. 22, no. 6, pp. 583–590, 1990.

[10] M. Ajtai, J. Komlós, and E. Szemerédi, "Sorting in $c \log n$ parallel steps," *Combinatorica*, vol. 3, no. 1, pp. 1–19, 1983.

Full text available at: http://dx.doi.org/10.1561/0400000010

[11] M. Ajtai, J. Komlós, and E. Szemerédi, "Deterministic Simulation in LOGSPACE," in *Annual ACM Symposium on Theory of Computing*, pp. 132–140, New York City, 25–27 May 1987.

[12] M. Ajtai and A. Wigderson, "Deterministic simulation of probabilistic constant depth circuits," in *Randomness and Computation,* vol. 5 of *Advances in Computing Research*, (F. P. Preparata and S. Micali, eds.), pp. 199–223, 1989.

[13] R. Aleliunas, R. M. Karp, R. J. Lipton, L. Lovász, and C. Rackoff, "Random walks, universal traversal sequences, and the complexity of maze problems," in *Annual Symposium on Foundations of Computer Science (San Juan, Puerto Rico, 1979)*, pp. 218–223, New York, 1979.

[14] E. Allender, H. Buhrman, M. Koucký, D. van Melkebeek, and D. Ronneburger, "Power from random strings," *SIAM Journal on Computing*, vol. 35, no. 6, pp. 1467–1493, 2006.

[15] N. Alon, "Eigenvalues and expanders," *Combinatorica*, vol. 6, no. 2, pp. 83–96, 1986.

[16] N. Alon, "Eigenvalues, geometric expanders, sorting in rounds, and Ramsey theory," *Combinatorica*, vol. 6, no. 3, pp. 207–219, 1986.

[17] N. Alon and M. R. Capalbo, "Explicit unique-neighbor expanders," in *Symposium on Foundations of Computer Science (Vancouver, BC, 2002)*, pp. 73–79, 2002.

[18] N. Alon and F. R. K. Chung, "Explicit construction of linear sized tolerant networks," *Discrete Mathematics*, vol. 72, no. 1–3, pp. 15–19, 1988.

[19] N. Alon, O. Goldreich, J. Håstad, and R. Peralta, "Simple constructions of almost k-wise independent random variables," *Random Structures & Algorithms*, vol. 3, no. 3, pp. 289–304, 1992. (See also addendum in issue 4(1), 1993, pp. 199–120).

[20] N. Alon, V. Guruswami, T. Kaufman, and M. Sudan, "Guessing secrets efficiently via list decoding," *ACM Transactions on Algorithms*, vol. 3, no. 4, pp. Art 42, 16, 2007.

[21] N. Alon and Y. Mansour, "ϵ-discrepancy sets and their application for interpolation of sparse polynomials," *Information Processing Letters*, vol. 54, no. 6, pp. 337–342, 1995.

[22] N. Alon, Y. Matias, and M. Szegedy, "The space complexity of approximating the frequency moments," *Journal of Computer and System Sciences*, vol. 58, no. 1, pp. 137–147, (Part 2) 1999.

[23] N. Alon and V. D. Milman, "Eigenvalues, expanders and superconcentrators (Extended Abstract)," in *Annual Symposium on Foundations of Computer Science*, pp. 320–322, Singer Island, Florida, 24–26 October 1984.

[24] N. Alon and Y. Roichman, "Random Cayley graphs and expanders," *Random Structures and Algorithms*, vol. 5, no. 2, pp. 271–284, 1994.

[25] N. Alon and J. H. Spencer, *The Probabilistic Method. Wiley-Interscience Series in Discrete Mathematics and Optimization.* New York: Wiley-Interscience [John Wiley & Sons], Second Edition, 2000. (With an appendix on the life and work of Paul Erdős).

[26] N. Alon and B. Sudakov, "Bipartite subgraphs and the smallest eigenvalue," *Combinatorics, Probability and Computing*, vol. 9, no. 1, pp. 1–12, 2000.

Full text available at: http://dx.doi.org/10.1561/0400000010

[27] A. E. Andreev, A. E. F. Clementi, and J. D. P. Rolim, "Worst-case hardness suffices for derandomization: A new method for hardness-randomness trade-offs," in *Automata, Languages and Programming, 24th International Colloquium*, vol. 1256 of *Lecture Notes in Computer Science*, (P. Degano, R. Gorrieri, and A. Marchetti-Spaccamela, eds.), pp. 177–187, Bologna, Italy: Springer-Verlag, 7–11 July 1997.

[28] A. E. Andreev, A. E. F. Clementi, J. D. P. Rolim, and L. Trevisan, "Weak random sources, hitting sets, and BPP simulations," *SIAM Journal on Computing*, vol. 28, no. 6, pp. 2103–2116, (electronic) 1999.

[29] D. Angluin and D. Lichtenstein, "Provable security of cryptosystems: A survey," Technical Report YALEU/DCS/TR-288, Yale University, Department of Computer Science, 1983.

[30] S. Ar, R. J. Lipton, R. Rubinfeld, and M. Sudan, "Reconstructing algebraic functions from mixed data," *SIAM Journal on Computing*, vol. 28, no. 2, pp. 487–510, 1999.

[31] R. Armoni, M. Saks, A. Wigderson, and S. Zhou, "Discrepancy sets and pseudorandom generators for combinatorial rectangles," in *Annual Symposium on Foundations of Computer Science (Burlington, VT, 1996)*, pp. 412–421, Los Alamitos, CA, 1996.

[32] S. Arora and B. Barak, *Computational complexity*. Cambridge: Cambridge University Press, 2009. (A modern approach).

[33] S. Arora, C. Lund, R. Motwani, M. Sudan, and M. Szegedy, "Proof verification and the hardness of approximation problems," *Journal of the ACM*, vol. 45, pp. 501–555, May 1998.

[34] S. Arora and S. Safra, "Probabilistic checking of proofs: A new characterization of NP," *Journal of the ACM*, vol. 45, pp. 70–122, January 1998.

[35] S. Arora and M. Sudan, "Improved low degree testing and its applications," in *Proceedings of the Annual ACM Symposium on Theory of Computing*, pp. 485–495, El Paso, Texas, 4–6 May 1997.

[36] M. Artin, *Algebra*. Englewood Cliffs, NJ: Prentice Hall Inc., 1991.

[37] V. Arvind and J. Köbler, "On pseudorandomness and resource-bounded measure," *Theoretical Computer Science*, vol. 255, no. 1–2, pp. 205–221, 2001.

[38] B. Aydinlioğlu, D. Gutfreund, J. M. Hitchcock, and A. Kawachi, "Derandomizing Arthur-Merlin games and approximate counting implies exponential-size lower bounds," *Computational Complexity*, vol. 20, no. 2, pp. 329–366, 2011.

[39] B. Aydinlioğlu and D. van Melkebeek, "Nondeterministic circuit lower bounds from mildly derandomizing Arthur-Merlin games," *Electronic Colloquium on Computational Complexity (ECCC)*, vol. 19, p. 80, 2012.

[40] Y. Azar, R. Motwani, and J. Naor, "Approximating probability distributions using small sample spaces," *Combinatorica*, vol. 18, no. 2, pp. 151–171, 1998.

[41] L. Babai, L. Fortnow, L. A. Levin, and M. Szegedy, "Checking computations in polylogarithmic time," in *STOC*, (C. Koutsougeras and J. S. Vitter, eds.), pp. 21–31, ACM, 1991.

[42] L. Babai, L. Fortnow, and C. Lund, "Nondeterministic exponential time has two-prover interactive protocols," *Computational Complexity*, vol. 1, no. 1, pp. 3–40, 1991.

Full text available at: http://dx.doi.org/10.1561/0400000010

[43] L. Babai, L. Fortnow, N. Nisan, and A. Wigderson, "BPP has subexponential time simulations unless EXPTIME has publishable proofs," *Computational Complexity*, vol. 3, no. 4, pp. 307–318, 1993.

[44] L. Babai and S. Moran, "Arthur-Merlin games: A randomized proof system, and a hierarchy of complexity classes," *Journal of Computer and System Sciences*, vol. 36, no. 2, pp. 254–276, 1988.

[45] B. Barak, M. Hardt, and S. Kale, "The uniform hardcore lemma via approximate Bregman projections," in *Proceedings of the Annual ACM-SIAM Symposium on Discrete Algorithms*, pp. 1193–1200, Philadelphia, PA, 2009.

[46] B. Barak, R. Impagliazzo, and A. Wigderson, "Extracting randomness using few independent sources," *SIAM Journal on Computing*, vol. 36, no. 4, pp. 1095–1118, 2006.

[47] B. Barak, G. Kindler, R. Shaltiel, B. Sudakov, and A. Wigderson, "Simulating independence: New constructions of condensers, Ramsey graphs, dispersers, and extractors," *Journal of the ACM*, vol. 57, no. 4, no. 4, pp. Art 20, 52, 2010.

[48] B. Barak, A. Rao, R. Shaltiel, and A. Wigderson, "2-source dispersers for $n^{o(1)}$ entropy and Ramsey graphs beating the Frankl–Wilson construction," *Annals of Mathematics*, 2012. (To appear. Preliminary version in *STOC '06*).

[49] B. Barak, R. Shaltiel, and A. Wigderson, "Computational analogues of entropy," in *Approximation, randomization, and combinatorial optimization,* vol. 2764 of *Lecture Notes in Computer Science*, pp. 200–215, Berlin: Springer, 2003.

[50] B. Barak, L. Trevisan, and A. Wigderson, *Additive Combinatorics and Computer Science*. http://www.cs.princeton.edu/theory/index.php/Main/AdditiveCombinatoricsMinicourse, August 2007.

[51] E. Barker and J. Kelsey, "Recommendation for random number generation using deterministic random bit generators," Special Publication 800-90A, National Institute of Standards and Technology, U.S. Department of Commerce, January 2012.

[52] L. A. Bassalygo, "Asymptotically optimal switching circuits," *Problems of Information Transmission*, vol. 17, no. 3, pp. 206–211, 1981.

[53] J. D. Batson, D. A. Spielman, and N. Srivastava, "Twice-ramanujan sparsifiers," in *Annual ACM Symposium on Theory of Computing (Bethesda, MD)*, pp. 255–262, 2009.

[54] D. Beaver and J. Feigenbaum, "Hiding instances in multioracle queries (Extended Abstract)," in *STACS 90 (Rouen, 1990),* vol. 415 of *Lecture Notes in Computer Science*, pp. 37–48, Berlin: Springer, 1990.

[55] M. Bellare, O. Goldreich, and S. Goldwasser, "Randomness in interactive proofs," *Computational Complexity*, vol. 3, no. 4, pp. 319–354, 1993.

[56] M. Bellare, S. Goldwasser, and D. Micciancio, ""Pseudo-Random" number generation within cryptographic algorithms: The DDS case," in *CRYPTO,* vol. 1294 of *Lecture Notes in Computer Science*, (B. S. K. Jr., ed.), pp. 277–291, Springer, 1997.

[57] M. Bellare and J. Rompel, "Randomness-efficient oblivious sampling," in *Annual Symposium on Foundations of Computer Science*, pp. 276–287, Santa Fe, New Mexico, 20–22 November 1994.

Full text available at: http://dx.doi.org/10.1561/0400000010

[58] A. Ben-Aroya and A. Ta-Shma, "A combinatorial construction of almost-Ramanujan graphs using the zig-zag product," in *Annual ACM Symposium on Theory of Computing (Victoria, British Columbia)*, pp. 325–334, 2008.

[59] E. Ben-Sasson, O. Goldreich, P. Harsha, M. Sudan, and S. Vadhan, "Robust PCPs of proximity, shorter PCPs and applications to coding," *SIAM Journal on Computing*, vol. 36, no. 4, pp. 889–974, 2006.

[60] E. Ben-Sasson and S. Kopparty, "Affine dispersers from subspace polynomials," in *STOC'09 — Proceedings of the 2009 ACM International Symposium on Theory of Computing*, pp. 65–74, New York, 2009.

[61] E. Ben-Sasson, M. Sudan, S. Vadhan, and A. Wigderson, "Randomness-efficient low degree tests and short PCPs via epsilon-biased sets," in *Proceedings of the Annual ACM Symposium on Theory of Computing*, pp. 612–621, New York, 2003.

[62] E. Ben-Sasson and N. Zewi, "From affine to two-source extractors via approximate duality," in *STOC*, (L. Fortnow and S. P. Vadhan, eds.), pp. 177–186, ACM, 2011.

[63] C. H. Bennett, G. Brassard, and J.-M. Robert, "Privacy amplification by public discussion," *SIAM Journal on Computing*, vol. 17, no. 2, pp. 210–229, 1988. Special issue on cryptography.

[64] S. J. Berkowitz, "On computing the determinant in small parallel time using a small number of processors," *Information Processing Letters*, vol. 18, no. 3, pp. 147–150, 1984.

[65] E. R. Berlekamp, *Algebraic Coding Theory.* New York: McGraw-Hill Book Co., 1968.

[66] E. R. Berlekamp, "Factoring polynomials over large finite fields," *Mathematics of Computation*, vol. 24, pp. 713–735, 1970.

[67] J. Bierbrauer, T. Johansson, G. Kabatianskii, and B. Smeets, "On families of hash functions via geometric codes and concatenation," in *Advances in cryptology — CRYPTO '93 (Santa Barbara, CA, 1993)*, vol. 773 of *Lecture Notes in Computer Science*, pp. 331–342, Berlin: Springer, 1994.

[68] Y. Bilu and N. Linial, "Lifts, discrepancy and nearly optimal spectral gap," *Combinatorica*, vol. 26, no. 5, pp. 495–519, 2006.

[69] M. Blum, "Independent unbiased coin flips from a correlated biased source — a finite state Markov chain," *Combinatorica*, vol. 6, no. 2, pp. 97–108, 1986. Theory of computing (Singer Island, Fla., 1984).

[70] M. Blum and S. Kannan, "Designing programs that check their work," *Journal of the ACM*, vol. 42, no. 1, pp. 269–291, 1995.

[71] M. Blum, M. Luby, and R. Rubinfeld, "Self-testing/correcting with applications to numerical problems," *Journal of Computer and System Sciences*, vol. 47, no. 3, pp. 549–595, 1993.

[72] M. Blum and S. Micali, "How to generate cryptographically strong sequences of pseudorandom bits," *SIAM Journal on Computing*, vol. 13, no. 4, pp. 850–864, 1984.

[73] A. Bogdanov, Z. Dvir, E. Verbin, and A. Yehudayoff, "Pseudorandomness for Width 2 Branching Programs," *Electronic Colloquium on Computational Complexity (ECCC)*, vol. 16, p. 70, 2009.

Full text available at: http://dx.doi.org/10.1561/0400000010

[74] A. Bogdanov and L. Trevisan, "Average-case complexity," *Foundations and Trends® in Theoretical Computer Science*, vol. 2, no. 1, pp. 1–106, 2006.

[75] A. Bogdanov and E. Viola, "Pseudorandom bits for polynomials," *SIAM Journal on Computing*, vol. 39, no. 6, pp. 2464–2486, 2010.

[76] A. Borodin, J. von zur Gathen, and J. Hopcroft, "Fast parallel matrix and GCD computations," *Information and Control*, vol. 52, no. 3, pp. 241–256, 1982.

[77] C. Bosley and Y. Dodis, "Does privacy require true randomness?," in *Theory of cryptography,* vol. 4392 of *Lecture Notes in Computer Science*, pp. 1–20, Berlin: Springer, 2007.

[78] J. Bourgain, "On the construction of affine extractors," *Geometric and Functional Analysis*, vol. 17, no. 1, pp. 33–57, 2007.

[79] J. Bourgain, N. Katz, and T. Tao, "A sum-product estimate in finite fields, and applications," *Geometric and Functional Analysis*, vol. 14, no. 1, pp. 27–57, 2004.

[80] J. Boyar, "Inferring sequences produced by pseudo-random number generators," *Journal of the Association for Computing Machinery*, vol. 36, no. 1, pp. 129–141, 1989.

[81] M. Braverman, "Polylogarithmic independence fools AC^0 circuits," *Journal of the ACM*, vol. 57, no. 5, pp. Art 28, 10, 2010.

[82] M. Braverman, A. Rao, R. Raz, and A. Yehudayoff, "Pseudorandom generators for regular branching programs," in *FOCS*, pp. 40–47, IEEE Computer Society, 2010.

[83] A. Z. Broder, "How hard is to marry at random? (On the approximation of the permanent)," in *Annual ACM Symposium on Theory of Computing (Berkeley, CA)*, pp. 50–58, 1986.

[84] J. Brody and E. Verbin, "The coin problem and pseudorandomness for branching programs," in *FOCS*, pp. 30–39, IEEE Computer Society, 2010.

[85] H. Buhrman and L. Fortnow, "One-sided two-sided error in probabilistic computation," in *STACS 99 (Trier),* vol. 1563 of *Lecture Notes in Computer Science*, pp. 100–109, Berlin: Springer, 1999.

[86] H. Buhrman, L. Fortnow, and T. Thierauf, "Nonrelativizing separations," in *Annual IEEE Conference on Computational Complexity (Buffalo, NY, 1998)*, pp. 8–12, Los Alamitos, CA, 1998.

[87] H. Buhrman, P. B. Miltersen, J. Radhakrishnan, and S. Venkatesh, "Are bitvectors optimal?," *SIAM Journal on Computing*, vol. 31, no. 6, pp. 1723–1744, 2002.

[88] J. Buresh-Oppenheim, V. Kabanets, and R. Santhanam, "Uniform hardness amplification in NP via monotone codes," *Electronic Colloquium on Computational Complexity (ECCC)*, vol. 13, no. 154, 2006.

[89] P. Bürgisser, M. Clausen, and M. A. Shokrollahi, *Algebraic Complexity Theory,* volume 315 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Berlin: Springer-Verlag, 1997. (With the collaboration of Thomas Lickteig).

Full text available at: http://dx.doi.org/10.1561/0400000010

[90] R. Canetti, Y. Dodis, S. Halevi, E. Kushilevitz, and A. Sahai, "Exposure-resilient functions and all-or-nothing transforms," in *Advances in Cryptology — EUROCRYPT 00, Lecture Notes in Computer Science*, (B. Preneel, ed.), Springer-Verlag, 14–18 May 2000.

[91] R. Canetti, G. Even, and O. Goldreich, "Lower bounds for sampling algorithms for estimating the average," *Information Processing Letters*, vol. 53, no. 1, pp. 17–25, 1995.

[92] M. Capalbo, O. Reingold, S. Vadhan, and A. Wigderson, "Randomness conductors and constant-degree lossless expanders," in *Annual ACM Symposium on Theory of Computing (STOC '02)*, pp. 659–668, Montréal, CA, May 2002. (Joint session with *CCC '02*).

[93] J. L. Carter and M. N. Wegman, "Universal classes of hash functions," *Journal of Computer and System Sciences*, vol. 18, no. 2, pp. 143–154, 1979.

[94] J. Cheeger, "A lower bound for the smallest eigenvalue of the Laplacian," in *Problems in analysis (Papers dedicated to Salomon Bochner, 1969)*, pp. 195–199, Princeton, NJ: Princeton Univ. Press, 1970.

[95] H. Chernoff, "A measure of asymptotic efficiency for tests of a hypothesis based on the sum of observations," *Annals of Mathematical Statistics*, vol. 23, pp. 493–507, 1952.

[96] B. Chor and O. Goldreich, "Unbiased bits from sources of weak randomness and probabilistic communication complexity," *SIAM Journal on Computing*, vol. 17, pp. 230–261, April 1988.

[97] B. Chor and O. Goldreich, "On the power of two-point based sampling," *Journal of Complexity*, vol. 5, no. 1, pp. 96–106, 1989.

[98] B. Chor, O. Goldreich, J. Håstad, J. Friedman, S. Rudich, and R. Smolensky, "The bit extraction problem of t-resilient functions (Preliminary Version)," in *FOCS*, pp. 396–407, IEEE, 1985.

[99] B. Chor, O. Goldreich, E. Kushilevitz, and M. Sudan, "Private information retrieval," *Journal of the ACM*, vol. 45, no. 6, pp. 965–982, 1998.

[100] F. Chung and R. Graham, "Sparse quasi-random graphs," *Combinatorica*, vol. 22, no. 2, pp. 217–244, 2002. (Special issue: Paul Erdős and his mathematics).

[101] F. Chung and R. Graham, "Quasi-random graphs with given degree sequences," *Random Structures and Algorithms*, vol. 32, no. 1, pp. 1–19, 2008.

[102] F. Chung, R. Graham, and T. Leighton, "Guessing secrets," *Electronic Journal of Combinatorics*, vol. 8, no. 1, p. 25 (electronic), 2001. Research Paper 13.

[103] F. R. K. Chung, "Diameters and eigenvalues," *Journal of the American Mathematical Society*, vol. 2, no. 2, pp. 187–196, 1989.

[104] F. R. K. Chung, R. L. Graham, and R. M. Wilson, "Quasi-random graphs," *Combinatorica*, vol. 9, no. 4, pp. 345–362, 1989.

[105] K.-M. Chung, "Efficient parallel repetition theorems with applications to security amplification," PhD Thesis, Harvard University, 2011.

[106] K.-M. Chung, Y. T. Kalai, F.-H. Liu, and R. Raz, "Memory delegation," in *Advances in Cryptology — CRYPTO 2011,* vol. 6841 of *Lecture Notes in Computer Science*, pp. 151–168, Heidelberg: Springer, 2011.

Full text available at: http://dx.doi.org/10.1561/0400000010

[107] A. Cohen and A. Wigderson, "Dispersers, deterministic amplification, and weak random sources (extended abstract)," in *Annual Symposium on Foundations of Computer Science (Research Triangle Park, North Carolina)*, pp. 14–19, 1989.

[108] D. Coppersmith and S. Winograd, "Matrix multiplication via arithmetic progressions," *Journal of Symbolic Computation*, vol. 9, no. 3, pp. 251–280, 1990.

[109] T. H. Cormen, C. E. Leiserson, R. L. Rivest, and C. Stein, *Introduction to Algorithms*. Cambridge, MA: MIT Press, Second Edition, 2001.

[110] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. Wiley Series in Telecommunications: John Wiley & Sons, Inc., Second Edition, 1991.

[111] L. Csanky, "Fast parallel matrix inversion algorithms," *SIAM Journal on Computing*, vol. 5, no. 4, pp. 618–623, 1976.

[112] G. Davidoff, P. Sarnak, and A. Valette, "Elementary number theory, group theory, and Ramanujan graphs," in vol. 55 of *London Mathematical Society Student Texts*, Cambridge: Cambridge University Press, 2003.

[113] A. De, "Pseudorandomness for permutation and regular branching programs," in *IEEE Conference on Computational Complexity*, pp. 221–231, 2011.

[114] A. De and T. Watson, "Extractors and lower bounds for locally samplable sources," in *Approximation, Randomization, and Combinatorial Optimization,* vol. 6845 of *Lecture Notes in Computer Science*, pp. 483–494, Heidelberg: Springer, 2011.

[115] R. de Wolf, "A Brief Introduction to Fourier analysis on the Boolean cube," *Theory of Computing, Graduate Surveys*, vol. 1, pp. 1–20, 2008.

[116] R. A. DeMillo and R. J. Lipton, "A probabilistic remark on algebraic program testing," *Information Processing Letters*, vol. 7, no. 4, pp. 193–195, 1978.

[117] W. Diffie and M. E. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, vol. IT-22, no. 6, pp. 644–654, 1976.

[118] I. Dinur, "The PCP theorem by gap amplification," *Journal of the ACM*, vol. 54, no. 3, article 12, p. 44 (electronic), 2007.

[119] Y. Dodis, R. Impagliazzo, R. Jaiswal, and V. Kabanets, "Security amplification for *interactive* cryptographic primitives," in *Theory of Cryptography,* vol. 5444 of *Lecture Notes in Computer Science*, pp. 128–145, Berlin: Springer, 2009.

[120] Y. Dodis, T. Ristenpart, and S. Vadhan, "Randomness condensers for efficiently samplable, seed-dependent sources," in *Proceedings of the IACR Theory of Cryptography Conference (TCC '12),* vol. 7194 of *Lecture Notes in Computer Science*, (R. Cramer, ed.), pp. 618–635, Springer-Verlag, 19–21 March 2012.

[121] D. Dubhashi and A. Panconesi, *Concentration of Measure for the Analysis of Randomized Algorithms*. Cambridge University Press, 2009.

[122] Z. Dvir, "Extractors for varieties," in *IEEE Conference on Computational Complexity*, pp. 102–113, 2009.

[123] Z. Dvir, A. Gabizon, and A. Wigderson, "Extractors and rank extractors for polynomial sources," *Computational Complexity*, vol. 18, no. 1, pp. 1–58, 2009.

Full text available at: http://dx.doi.org/10.1561/0400000010

[124] Z. Dvir, S. Kopparty, S. Saraf, and M. Sudan, "Extensions to the method of multiplicities, with applications to Kakeya sets and mergers," in *2009 Annual IEEE Symposium on Foundations of Computer Science (FOCS 2009)*, pp. 181–190, Los Alamitos, CA, 2009.

[125] Z. Dvir and S. Lovett, "Subspace evasive sets," in *Symposium on Theory of Computing*, (H. J. Karloff and T. Pitassi, eds.), pp. 351–358, ACM, 2012.

[126] Z. Dvir and A. Shpilka, "Locally decodable codes with two queries and polynomial identity testing for depth 3 circuits," *SIAM Journal on Computing*, vol. 36, no. 5, pp. 1404–1434 (electronic), 2006/07.

[127] S. Dziembowski and K. Pietrzak, "Leakage-resilient cryptography," in *Symposium on Foundations of Computer Science*, pp. 293–302, 2008.

[128] K. Efremenko, "3-query locally decodable codes of subexponential length," in *STOC'09 — Proceedings of the 2009 ACM International Symposium on Theory of Computing*, pp. 39–44, New York, 2009.

[129] P. Elias, *List Decoding for Noisy Channels,* Research Laboratory of Electronics, Massachusetts Institute of Technology. Rep. No. 335: Cambridge, MA, 1957.

[130] P. Elias, "The efficient construction of an unbiased random sequence," *The Annals of Mathematical Statistics*, vol. 43, no. 3, pp. 865–870, June 1972.

[131] P. Elias, "Error-correcting codes for list decoding," *IEEE Transactions on Information Theory*, vol. 37, no. 1, pp. 5–12, 1991.

[132] P. Erdős, "Some remarks on the theory of graphs," *Bulletin of the American Mathematical Society*, vol. 53, pp. 292–294, 1947.

[133] P. Erdős, "Problems and results in chromatic graph theory," in *Proof Techniques in Graph Theory (Proceedings of Ann Arbor Graph Theory Conference, Ann Arbor, Michigan, 1968)*, pp. 27–35, New York, 1969.

[134] P. Erdős, P. Frankl, and Z. Füredi, "Families of finite sets in which no set is covered by the union of r others," *Israel Journal of Mathematics*, vol. 51, no. 1–2, pp. 79–89, 1985.

[135] G. Even, "Construction of small probabilistic spaces for deterministic simulation," Master's Thesis, The Technion, 1991.

[136] G. Even, O. Goldreich, M. Luby, N. Nisan, and B. Velickovic, "Efficient approximation of product distributions," *Random Struct. Algorithms*, vol. 13, no. 1, pp. 1–16, 1998.

[137] S. Even, A. L. Selman, and Y. Yacobi, "The complexity of promise problems with applications to public-key cryptography," *Information and Control*, vol. 61, no. 2, pp. 159–173, 1984.

[138] U. Feige, S. Goldwasser, L. Lovász, S. Safra, and M. Szegedy, "Interactive proofs and the hardness of approximating cliques," *Journal of the ACM*, vol. 43, no. 2, pp. 268–292, 1996.

[139] J. A. Fill, "Eigenvalue bounds on convergence to stationarity for nonreversible Markov chains, with an application to the exclusion process," *Annals of Applied Probability*, vol. 1, no. 1, pp. 62–87, 1991.

[140] G. D. Forney, *Concatenated Codes.* MIT Press, 1966.

[141] P. Frankl and R. M. Wilson, "Intersection theorems with geometric consequences," *Combinatorica*, vol. 1, no. 4, pp. 357–368, 1981.

Full text available at: http://dx.doi.org/10.1561/0400000010

[142] M. L. Fredman, J. Komlós, and E. Szemerédi, "Storing a sparse table with $O(1)$ worst case access time," *Journal of the ACM*, vol. 31, no. 3, pp. 538–544, 1984.

[143] J. Friedman, "A proof of Alon's second eigenvalue conjecture and related problems," *Memoirs of the American Mathematical Society*, vol. 195, no. 910, p. viii+100, 2008.

[144] A. M. Frieze, J. Håstad, R. Kannan, J. C. Lagarias, and A. Shamir, "Reconstructing truncated integer variables satisfying linear congruences," *SIAM Journal on Computing*, vol. 17, no. 2, pp. 262–280, 1988. (Special issue on cryptography).

[145] B. Fuller, A. O'Neill, and L. Reyzin, "A unified approach to deterministic encryption: New constructions and a connection to computational entropy," in *TCC,* vol. 7194 of *Lecture Notes in Computer Science*, (R. Cramer, ed.), pp. 582–599, 2012.

[146] O. Gabber and Z. Galil, "Explicit constructions of linear-sized superconcentrators," *Journal of Computer and System Sciences*, vol. 22, pp. 407–420, June 1981.

[147] A. Gabizon and R. Raz, "Deterministic extractors for affine sources over large fields," *Combinatorica*, vol. 28, no. 4, pp. 415–440, 2008.

[148] R. G. Gallager, *Low-Density Parity-Check Codes*. MIT Press, 1963.

[149] P. Gemmell, R. J. Lipton, R. Rubinfeld, M. Sudan, and A. Wigderson, "Self-testing/correcting for polynomials and for approximate functions," in *STOC*, (C. Koutsougeras and J. S. Vitter, eds.), pp. 32–42, 1991.

[150] P. Gemmell and M. Sudan, "Highly resilient correctors for polynomials," *Information Processing Letters*, vol. 43, no. 4, pp. 169–174, 1992.

[151] E. Gilbert, "A comparison of signalling alphabets," *Bell Systems Technical Journal*, vol. 31, pp. 504–522, 1952.

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

[153] D. Gillman, "A Chernoff bound for random walks on expander graphs," *SIAM Journal on Computing*, vol. 27, no. 4, pp. 1203–1220 (electronic), 1998.

[154] M. X. Goemans and D. P. Williamson, "Improved approximation algorithms for maximum cut and satisfiability problems using semidefinite programming," *Journal of the ACM*, vol. 42, no. 6, pp. 1115–1145, 1995.

[155] O. Goldreich, "A sample of samplers — a computational perspective on sampling (survey)," *Electronic Colloquium on Computational Complexity (ECCC)*, vol. 4, no. 20, 1997.

[156] O. Goldreich, *Modern Cryptography, Probabilistic Proofs and Pseudorandomness,* vol. 17 of *Algorithms and Combinatorics*. Berlin: Springer-Verlag, 1999.

[157] O. Goldreich, *Foundations of Cryptography*. Cambridge: Cambridge University Press, 2001. (Basic tools).

[158] O. Goldreich, *Foundations of Cryptography II*. Cambridge: Cambridge University Press, 2004. (Basic Applications).

[159] O. Goldreich, "On promise problems: A survey," in *Theoretical Computer Science,* vol. 3895 of *Lecture Notes in Computer Science*, pp. 254–290, Berlin: Springer, 2006.

Full text available at: http://dx.doi.org/10.1561/0400000010

[160] O. Goldreich, "Probabilistic proof systems: A primer," *Foundations and Trends in Theoretical Computer Science*, vol. 3, no. 1, pp. 1–91 (2008), 2007.
[161] O. Goldreich, *Computational Complexity: A Conceptual Perspective*. Cambridge: Cambridge University Press, 2008.
[162] O. Goldreich, *A Primer on Pseudorandom Generators,* vol. 55 of *University Lecture Series*. Providence, RI: American Mathematical Society, 2010.
[163] O. Goldreich, "In a World of P=BPP," in *Studies in Complexity and Cryptography. Miscellanea on the Interplay of Randomness and Computation,* vol. 6650 of *Lecture Notes in Computer Science*, pp. 191–232, Springer, 2011.
[164] O. Goldreich, S. Goldwasser, and S. Micali, "How to construct random functions," *Journal of the ACM*, vol. 33, pp. 792–807, October 1986.
[165] O. Goldreich, S. Goldwasser, and D. Ron, "Property testing and its connection to learning and approximation," *Journal of the ACM*, vol. 45, no. 4, pp. 653–750, 1998.
[166] O. Goldreich, R. Impagliazzo, L. Levin, R. Venkatesan, and D. Zuckerman, "Security preserving amplification of hardness," in *Annual Symposium on Foundations of Computer Science, Vol. I, II (St. Louis, MO, 1990)*, pp. 318–326, Los Alamitos, CA: IEEE Computer Society Press, 1990.
[167] O. Goldreich, H. Krawczyk, and M. Luby, "On the existence of pseudorandom generators," *SIAM Journal on Computing*, vol. 22, no. 6, pp. 1163–1175, 1993.
[168] O. Goldreich and L. A. Levin, "A hard-core predicate for all one-way functions," in *Proceedings of the Annual ACM Symposium on Theory of Computing*, pp. 25–32, Seattle, Washington, 15–17 May 1989.
[169] O. Goldreich and B. Meyer, "Computational indistinguishability: algorithms vs. circuits," *Theoretical Computer Science*, vol. 191, no. 1–2, pp. 215–218, 1998.
[170] O. Goldreich, S. Micali, and A. Wigderson, "Proofs that yield nothing but their validity, or All languages in NP have zero-knowledge proof systems," *Journal of the ACM*, vol. 38, no. 3, pp. 691–729, 1991.
[171] O. Goldreich, N. Nisan, and A. Wigderson, "On Yao's XOR lemma," Technical Report TR95–050, revision 2, Electronic Colloquium on Computational Complexity, http://www.eccc.uni-trier.de/eccc, June 2010.
[172] O. Goldreich and M. Sudan, "Computational indistinguishability: A sample hierarchy," *Journal of Computer and System Sciences*, vol. 59, no. 2, pp. 253–269, 1999. (13th Annual IEEE Conference on Computation Complexity (Buffalo, NY, 1998)).
[173] O. Goldreich, S. Vadhan, and A. Wigderson, "Simplified derandomization of BPP using a hitting set generator," in *Studies in Complexity and Cryptography. Miscellanea on the Interplay of Randomness and Computation,* vol. 6650 of *Lecture Notes in Computer Science*, pp. 59–67, Springer, 2011.
[174] O. Goldreich and A. Wigderson, "Tiny families of functions with random properties: A quality-size trade-off for hashing," *Random Structures & Algorithms*, vol. 11, no. 4, pp. 315–343, 1997.
[175] S. Goldwasser, "Cryptography without (hardly any) secrets?," in *Advances in cryptology — EUROCRYPT 2009,* vol. 5479 of *Lecture Notes in Computer Science*, pp. 369–370, Berlin: Springer, 2009.

Full text available at: http://dx.doi.org/10.1561/0400000010

[176] S. Goldwasser and S. Micali, "Probabilistic Encryption," *Journal of Computer and System Sciences*, vol. 28, pp. 270–299, April 1984.

[177] S. Goldwasser, S. Micali, and C. Rackoff, "The knowledge complexity of interactive proof systems," *SIAM Journal on Computing*, vol. 18, no. 1, pp. 186–208, 1989.

[178] P. Gopalan, R. Meka, and O. Reingold, "DNF Sparsification and a faster deterministic counting algorithm," in *IEEE Conference on Computational Complexity*, pp. 126–135, 2012.

[179] P. Gopalan, R. Meka, O. Reingold, L. Trevisan, and S. Vadhan, "Better pseudorandom generators via milder pseudorandom restrictions," in *Proceedings of the Annual IEEE Symposium on Foundations of Computer Science (FOCS '12)*, 20–23 October 2012. (To appear).

[180] W. T. Gowers, "A new proof of Szemerédi's theorem for arithmetic progressions of length four," *Geometric and Functional Analysis*, vol. 8, no. 3, pp. 529–551, 1998.

[181] W. T. Gowers, "A new proof of Szemerédi's theorem," *Geometric and Functional Analysis*, vol. 11, no. 3, pp. 465–588, 2001.

[182] R. L. Graham, B. L. Rothschild, and J. H. Spencer, *Ramsey Theory. Wiley-Interscience Series in Discrete Mathematics and Optimization.* New York: John Wiley & Sons Inc., Second Edition, 1990.

[183] V. Guruswami, "Guest column: Error-correcting codes and expander graphs," *SIGACT News*, vol. 35, no. 3, pp. 25–41, 2004.

[184] V. Guruswami, *Algorithmic Results in List Decoding.* volume 2, number 2 of *Foundations and Trends in Theoretical Computer Science.* now publishers, 2006.

[185] V. Guruswami, "Linear-algebraic list decoding of folded reed-solomon codes," in *IEEE Conference on Computational Complexity*, pp. 77–85, 2011.

[186] V. Guruswami, J. Håstad, and S. Kopparty, "On the list-decodability of random linear codes," *IEEE Transactions on Information Theory*, vol. 57, no. 2, pp. 718–725, 2011.

[187] V. Guruswami, J. Håstad, M. Sudan, and D. Zuckerman, "Combinatorial bounds for list decoding," *IEEE Transactions on Information Theory*, vol. 48, no. 5, pp. 1021–1034, 2002.

[188] V. Guruswami and A. Rudra, "Explicit codes achieving list decoding capacity: error-correction with optimal redundancy," *IEEE Transactions on Information Theory*, vol. 54, no. 1, pp. 135–150, 2008.

[189] V. Guruswami and M. Sudan, "Improved decoding of Reed-Solomon and algebraic-geometry codes," *Institute of Electrical and Electronics Engineers. Transactions on Information Theory*, vol. 45, no. 6, pp. 1757–1767, 1999.

[190] V. Guruswami and M. Sudan, "List decoding algorithms for certain concatenated codes," in *STOC*, pp. 181–190, 2000.

[191] V. Guruswami and M. Sudan, "Extensions to the Johnson bound," Unpublished Manuscript, February 2001.

[192] V. Guruswami, C. Umans, and S. Vadhan, "Unbalanced expanders and randomness extractors from Parvaresh–Vardy codes," *Journal of the ACM*, vol. 56, no. 4, pp. 1–34, 2009.

Full text available at: http://dx.doi.org/10.1561/0400000010

[193] V. Guruswami and C. Wang, "Optimal rate list decoding via derivative codes," in *Approximation, randomization, and combinatorial optimization,* vol. 6845 of *Lecture Notes in Computer Science*, pp. 593–604, Heidelberg: Springer, 2011.

[194] V. Guruswami and C. Xing, "Folded codes from function field towers and improved optimal rate list decoding," in *STOC*, (H. J. Karloff and T. Pitassi, eds.), pp. 339–350, ACM, 2012.

[195] D. Gutfreund, R. Shaltiel, and A. Ta-Shma, "Uniform hardness versus randomness tradeoffs for Arthur-Merlin games," *Computational Complexity*, vol. 12, no. 3–4, pp. 85–130, 2003.

[196] J. Håstad, *Computational Limitations of Small-Depth Circuits.* MIT Press, 1987.

[197] J. Håstad, R. Impagliazzo, L. A. Levin, and M. Luby, "A pseudorandom generator from any one-way function," *SIAM Journal on Computing*, vol. 28, no. 4, pp. 1364–1396, 1999.

[198] I. Haitner, O. Reingold, and S. Vadhan, "Efficiency improvements in constructing pseudorandom generators from one-way functions," in *Proceedings of the Annual ACM Symposium on Theory of Computing (STOC '10)*, pp. 437–446, 6–8 June 2010.

[199] R. W. Hamming, "Error detecting and error correcting codes," *The Bell System Technical Journal*, vol. 29, pp. 147–160, 1950.

[200] J. Hartmanis and R. E. Stearns, "On the computational complexity of algorithms," *Transactions of the American Mathematical Society*, vol. 117, pp. 285–306, 1965.

[201] N. J. A. Harvey, "Algebraic structures and algorithms for matching and matroid problems," in *Annual IEEE Symposium on Foundations of Computer Science (Berkeley, CA)*, pp. 531–542, 2006.

[202] A. Healy, S. Vadhan, and E. Viola, "Using nondeterminism to amplify hardness," *SIAM Journal on Computing*, vol. 35, no. 4, pp. 903–931, 2006.

[203] A. D. Healy, "Randomness-efficient sampling within NC^1," *Computational Complexity*, vol. 17, no. 1, pp. 3–37, 2008.

[204] W. Hoeffding, "Probability inequalities for sums of bounded random variables," *Journal of the American Statistical Association*, vol. 58, pp. 13–30, 1963.

[205] A. J. Hoffman, "On eigenvalues and colorings of graphs," in *Graph Theory and its Applications (Proceedings of Advanced Seminors, Mathematics Research Center, University of Wisconsin, Madison, Wisconsin, 1969)*, pp. 79–91, New York: Academic Press, 1970.

[206] T. Holenstein, "Key agreement from weak bit agreement," in *STOC'05: Proceedings of the Annual ACM Symposium on Theory of Computing*, pp. 664–673, New York, 2005.

[207] S. Hoory, N. Linial, and A. Wigderson, "Expander graphs and their applications," *Bulletin of the AMS*, vol. 43, no. 4, pp. 439–561, 2006.

[208] R. Impagliazzo, "Hard-core distributions for somewhat hard problems," in *Annual Symposium on Foundations of Computer Science*, pp. 538–545, Milwaukee, Wisconsin, 23–25 October 1995.

Full text available at: http://dx.doi.org/10.1561/0400000010

[209] R. Impagliazzo, "Hardness as randomness: A survey of universal derandomization," in *Proceedings of the International Congress of Mathematicians, Vol. III (Beijing, 2002)*, pp. 659–672, Beijing, 2002.

[210] R. Impagliazzo, R. Jaiswal, and V. Kabanets, "Approximate list-decoding of direct product codes and uniform hardness amplification," *SIAM Journal on Computing*, vol. 39, no. 2, pp. 564–605, 2009.

[211] R. Impagliazzo, R. Jaiswal, V. Kabanets, and A. Wigderson, "Uniform direct product theorems: Simplified, optimized, and derandomized," *SIAM Journal on Computing*, vol. 39, no. 4, pp. 1637–1665, 2009/2010.

[212] R. Impagliazzo, V. Kabanets, and A. Wigderson, "In search of an easy witness: Exponential time vs. probabilistic polynomial time," *Journal of Computer and System Sciences*, vol. 65, no. 4, pp. 672–694, 2002.

[213] R. Impagliazzo and S. Rudich, "Limits on the provable consequences of one-way permutations," in *Advances in cryptology — CRYPTO '88 (Santa Barbara, CA, 1988),* vol 403 of *Lecture Notes in Computer Science*, pp. 8–26, Berlin: Springer, 1990.

[214] R. Impagliazzo and A. Wigderson, "An information-theoretic variant of the inclusion-exclusion bound (preliminary version)," Unpublished manuscript, 1996.

[215] R. Impagliazzo and A. Wigderson, "$P = BPP$ if E requires exponential circuits: Derandomizing the XOR lemma," in *Proceedings of the Annual ACM Symposium on Theory of Computing*, pp. 220–229, El Paso, Texas, 4–6 May 1997.

[216] R. Impagliazzo and A. Wigderson, "Randomness vs time: Derandomization under a uniform assumption," *Journal of Computer and System Sciences*, vol. 63, no. 4, pp. 672–688, 2001. Special issue on FOCS 98 (Palo Alto CA).

[217] R. Impagliazzo and D. Zuckerman, "How to recycle random bits," in *Annual Symposium on Foundations of Computer Science (Research Triangle Park, North Carolina)*, pp. 248–253, 1989.

[218] K. Iwama and H. Morizumi, "An explicit lower bound of $5n - o(n)$ for Boolean circuits," in *Mathematical foundations of computer science 2002,* vol. 2420 of *Lecture Notes in Computer Science*, pp. 353–364, Berlin: Springer, 2002.

[219] M. Jerrum and A. Sinclair, "Approximating the permanent," *SIAM Journal on Computing*, vol. 18, no. 6, pp. 1149–1178, 1989.

[220] M. Jerrum, A. Sinclair, and E. Vigoda, "A polynomial-time approximation algorithm for the permanent of a matrix with nonnegative entries," *Journal of the ACM*, vol. 51, no. 4, pp. 671–697, 2004.

[221] S. Jimbo and A. Maruoka, "Expanders obtained from affine transformations," *Combinatorica*, vol. 7, no. 4, pp. 343–355, 1987.

[222] A. Joffe, "On a sequence of almost deterministic pairwise independent random variables," *Proceedings of the American Mathematical Society*, vol. 29, pp. 381–382, 1971.

[223] A. Joffe, "On a set of almost deterministic k-independent random variables," *Annals of Probability*, vol. 2, no. 1, pp. 161–162, 1974.

[224] S. Johnson, "Upper bounds for constant weight error correcting codes," *Discrete Mathematics*, vol. 3, pp. 109–124, 1972.

Full text available at: http://dx.doi.org/10.1561/0400000010

[225] S. M. Johnson, "A new upper bound for error-correcting codes," *IRE Transactions on Information Theory*, vol. IT-8, pp. 203–207, 1962.
[226] V. Kabanets, "Derandomization: A brief overview," in *Current Trends in Theoretical Computer Science,* vol. 1 *Algorithms and Complexity*, (G. Paun, G. Rozenberg, and A. Salomaa, eds.), pp. 165–188, World Scientific, 2004.
[227] V. Kabanets and R. Impagliazzo, "Derandomizing polynomial identity tests means proving circuit lower bounds," *Computational Complexity*, vol. 13, no. 1–2, pp. 1–46, 2004.
[228] N. Kahale, "Eigenvalues and expansion of regular graphs," *Journal of the ACM*, vol. 42, no. 5, pp. 1091–1106, 1995.
[229] J. D. Kahn, N. Linial, N. Nisan, and M. E. Saks, "On the cover time of random walks on graphs," *Journal of Theoretical Probability*, vol. 2, no. 1, pp. 121–128, 1989.
[230] A. T. Kalai, "Unpublished manuscript," 2004.
[231] J. Kamp, A. Rao, S. Vadhan, and D. Zuckerman, "Deterministic extractors for small-space sources," *Journal of Computer and System Sciences*, vol. 77, no. 1, pp. 191–220, 2011.
[232] J. Kamp and D. Zuckerman, "Deterministic extractors for bit-fixing sources and exposure-resilient cryptography," *SIAM Journal on Computing*, vol. 36, no. 5, pp. 1231–1247, 2006/2007.
[233] H. J. Karloff and T. Pitassi, eds., *Proceedings of the Symposium on Theory of Computing Conference, STOC 2012, New York, NY, USA, May 19–22, 2012*, 2012.
[234] R. Karp, N. Pippenger, and M. Sipser, "A time-randomness tradeoff," in *AMS Conference on Probabilistic Computational Complexity*, Durham, New Hampshire, 1985.
[235] R. M. Karp and R. J. Lipton, "Turing machines that take advice," *L'Enseignement Mathématique. Revue Internationale. IIe Série*, vol. 28, no. 3–4, pp. 191–209, 1982.
[236] R. M. Karp, M. Luby, and N. Madras, "Monte Carlo approximation algorithms for enumeration problems," *Journal of Algorithms*, vol. 10, no. 3, pp. 429–448, 1989.
[237] R. M. Karp, E. Upfal, and A. Wigderson, "Constructing a perfect matching is in Random NC," *Combinatorica*, vol. 6, no. 1, pp. 35–48, 1986.
[238] J. Katz and Y. Lindell, *Introduction to modern cryptography. Chapman & Hall/CRC Cryptography and Network Security.* Boca Raton, FL: Chapman & Hall/CRC, 2008.
[239] J. Katz and L. Trevisan, "On the efficiency of local decoding procedures for error-correcting codes," in *Proceedings of the Annual ACM Symposium on Theory of Computing*, pp. 80–86 (electronic), New York, 2000.
[240] N. M. Katz, "An estimate for character sums," *Journal of the American Mathematical Society*, vol. 2, no. 2, pp. 197–200, 1989.
[241] N. Kayal and N. Saxena, "Polynomial identity testing for depth 3 circuits," *Computational Complexity*, vol. 16, no. 2, pp. 115–138, 2007.
[242] J. Kinne, D. van Melkebeek, and R. Shaltiel, "Pseudorandom generators, typically-correct derandomization, and dircuit lower bounds," *Computational Complexity*, vol. 21, no. 1, pp. 3–61, 2012.

Full text available at: http://dx.doi.org/10.1561/0400000010

[243] A. R. Klivans and R. A. Servedio, "Boosting and Hard-Core Set Construction," *Machine Learning*, vol. 51, no. 3, pp. 217–238, 2003.

[244] A. R. Klivans and D. van Melkebeek, "Graph nonisomorphism has subexponential size proofs unless the polynomial-time hierarchy collapses," *SIAM Journal on Computing*, vol. 31, no. 5, pp. 1501–1526 (electronic), 2002.

[245] D. E. Knuth, *The art of computer programming. Volume 2: Seminumerical Algorithms*. Addison–Wesley, Third Edition, 1998.

[246] R. König and U. M. Maurer, "Extracting randomness from generalized symbol-fixing and Markov sources," in *Proceedings of 2004 IEEE International Symposium on Information Theory*, p. 232, 2004.

[247] R. König and U. M. Maurer, "Generalized strong extractors and deterministic privacy amplification," in *IMA International Conference,* vol. 3796 of *Lecture Notes in Computer Science*, (N. P. Smart, ed.), pp. 322–339, Springer, 2005.

[248] S. Kopparty, "List-decoding multiplicity codes," *Electronic Colloquium on Computational Complexity (ECCC)*, vol. 19, p. 44, 2012.

[249] S. Kopparty, S. Saraf, and S. Yekhanin, "High-rate codes with sublinear-time decoding," in *STOC*, (L. Fortnow and S. P. Vadhan, eds.), pp. 167–176, ACM, 2011.

[250] M. Koucký, P. Nimbhorkar, and P. Pudlák, "Pseudorandom generators for group products: extended abstract," in *STOC*, (L. Fortnow and S. P. Vadhan, eds.), pp. 263–272, ACM, 2011.

[251] C. Koutsougeras and J. S. Vitter, eds., *Proceedings of the Annual ACM Symposium on Theory of Computing, May 5–8, 1991, New Orleans, Louisiana, USA*, ACM, 1991.

[252] H. Krawczyk, "How to predict congruential generators," *Journal of Algorithms*, vol. 13, no. 4, pp. 527–545, 1992.

[253] E. Kushilevitz and N. Nisan, *Communication complexity*. Cambridge: Cambridge University Press, 1997.

[254] O. Lachish and R. Raz, "Explicit lower bound of $4.5n - o(n)$ for Boolean circuits," in *Annual ACM Symposium on Theory of Computing*, pp. 399–408 (electronic), New York, 2001.

[255] H. O. Lancaster, "Pairwise statistical independence," *Annals of Mathematical Statistics*, vol. 36, pp. 1313–1317, 1965.

[256] C. Lautemann, "BPP and the polynomial hierarchy," *Information Processing Letters*, vol. 17, no. 4, pp. 215–217, 1983.

[257] C.-J. Lee, C.-J. Lu, and S.-C. Tsai, "Computational randomness from generalized hardcore sets," in *Fundamentals of Computation Theory,* vol. 6914 of *Lecture Notes in Computer Science*, pp. 78–89, Heidelberg: Springer, 2011.

[258] F. T. Leighton, *Introduction to Parallel Algorithms and Architectures: Arrays, Trees, and Hypercubes*. San Mateo, CA: Morgan Kaufmann, 1992.

[259] L. A. Levin, "One way functions and pseudorandom generators," *Combinatorica*, vol. 7, no. 4, pp. 357–363, 1987.

[260] D. Lewin and S. Vadhan, "Checking polynomial identities over any field: towards a derandomization?," in *Annual ACM Symposium on the Theory of Computing (Dallas, TX)*, pp. 438–447, New York, 1999.

Full text available at: http://dx.doi.org/10.1561/0400000010

[261] M. Li and P. Vitányi, *An Introduction to Kolmogorov Complexity and its Applications. Texts in Computer Science*. New York: Springer, Third Edition, 2008.

[262] X. Li, "A New Approach to Affine Extractors and Dispersers," in *IEEE Conference on Computational Complexity*, pp. 137–147, 2011.

[263] R. Lidl and H. Niederreiter, *Introduction to Finite Fields and their Applications*. Cambridge: Cambridge University Press, First Edition, 1994.

[264] N. Linial, M. Luby, M. Saks, and D. Zuckerman, "Efficient construction of a small hitting set for combinatorial rectangles in high dimension," *Combinatorica*, vol. 17, no. 2, pp. 215–234, 1997.

[265] N. Linial and N. Nisan, "Approximate inclusion-exclusion," *Combinatorica*, vol. 10, no. 4, pp. 349–365, 1990.

[266] R. J. Lipton, "New directions in testing," in *Distributed computing and cryptography (Princeton, NJ, 1989),* vol. 2 of *DIMACS Series Discrete Mathemtics and Theoretical Computer Science*, pp. 191–202, Providence, RI: American Mathematical Society, 1991.

[267] L. Lovász, "On determinants, matchings, and random algorithms," in *Fundamentals of Computation Theory (Berlin/Wendisch-Rietz)*, pp. 565–574, 1979.

[268] L. Lovász, "On the Shannon capacity of a graph," *IEEE Transactions on Information Theory*, vol. 25, no. 1, pp. 1–7, 1979.

[269] L. Lovász, *Combinatorial Problems and Exercises*. Providence, RI: AMS Chelsea Publishing, Second Edition, 2007.

[270] S. Lovett, "Unconditional pseudorandom generators for low-degree polynomials," *Theory of Computing. An Open Access Journal*, vol. 5, pp. 69–82, 2009.

[271] C.-J. Lu, "Improved pseudorandom generators for combinatorial rectangles," *Combinatorica*, vol. 22, no. 3, pp. 417–433, 2002.

[272] C.-J. Lu, O. Reingold, S. Vadhan, and A. Wigderson, "Extractors: optimal up to constant factors," in *Proceedings of the ACM Symposium on Theory of Computing (STOC '03)*, pp. 602–611, 2003.

[273] C.-J. Lu, S.-C. Tsai, and H.-L. Wu, "Improved hardness amplification in NP," *Theoretical Computer Science*, vol. 370, no. 1–3, pp. 293–298, 2007.

[274] C.-J. Lu, S.-C. Tsai, and H.-L. Wu, "Complexity of hard-core set proofs," *Computational Complexity*, vol. 20, no. 1, pp. 145–171, 2011.

[275] A. Lubotzky, *Discrete Groups, Expanding Graphs and Invariant Measures*. volume 125 of *Progress in Mathematics*. Basel: Birkhäuser Verlag, 1994. (With an appendix by Jonathan D. Rogawski).

[276] A. Lubotzky, "Expander graphs in pure and applied mathematics," *American Mathematical Society. Bulletin. New Series*, vol. 49, no. 1, pp. 113–162, 2012.

[277] A. Lubotzky, R. Phillips, and P. Sarnak, "Ramanujan graphs," *Combinatorica*, vol. 8, no. 3, pp. 261–277, 1988.

[278] M. Luby, "A simple parallel algorithm for the maximal independent set problem," *SIAM Journal on Computing*, vol. 15, no. 4, pp. 1036–1053, 1986.

[279] M. Luby, "Removing randomness in parallel computation without a processor penalty," *Journal of Computer and System Sciences*, vol. 47, no. 2, pp. 250–286, 1993.

Full text available at: http://dx.doi.org/10.1561/0400000010

[280] M. Luby, B. Veličković, and A. Wigderson, "Deterministic Approximate Counting of Depth-2 Circuits," in *ISTCS*, pp. 18–24, 1993.

[281] M. Luby and A. Wigderson, *Pairwise Independence and Derandomization.* Volume 1, number 4 of *Foundations and Trends in Theoretical Computer Science.* now publishers, 2005.

[282] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-correcting Codes.* Amsterdam: North-Holland Publishing Co., 1977. (North-Holland Mathematical Library, Vol. 16).

[283] G. A. Margulis, "Explicit constructions of expanders," *Problemy Peredači Informacii*, vol. 9, no. 4, pp. 71–80, 1973.

[284] G. A. Margulis, "Explicit group-theoretic constructions of combinatorial schemes and their applications in the construction of expanders and concentrators," *Problemy Peredači Informacii*, vol. 24, no. 1, pp. 51–60, 1988.

[285] R. Martin and D. Randall, "Disjoint decomposition of Markov chains and sampling circuits in Cayley graphs," *Combinatorics, Probability and Computing*, vol. 15, no. 3, pp. 411–448, 2006.

[286] M. Mihail, "Conductance and convergence of Markov Chains-A combinatorial treatment of expanders," in *Annual Symposium on Foundations of Computer Science (Research Triangle Park, North Carolina)*, pp. 526–531, 1989.

[287] G. L. Miller, "Riemann's hypothesis and tests for primality," *Journal of Computer and System Sciences*, vol. 13, no. 3, pp. 300–317, December 1976.

[288] P. Miltersen, *Handbook of Randomized Computing,* chapter *Derandomizing Complexity Classes.* Kluwer, 2001.

[289] P. B. Miltersen and N. V. Vinodchandran, "Derandomizing Arthur-Merlin games using hitting sets," *Computational Complexity*, vol. 14, no. 3, pp. 256–279, 2005.

[290] M. Mitzenmacher and E. Upfal, *Probability and Computing.* Cambridge: Cambridge University Press, 2005. (Randomized algorithms and probabilistic analysis).

[291] R. Motwani and P. Raghavan, *Randomized Algorithms.* Cambridge: Cambridge University Press, 1995.

[292] M. Mucha and P. Sankowski, "Maximum matchings via Gaussian elimination," in *Symposium on Foundations of Computer Science (Rome, Italy)*, pp. 248–255, IEEE Computer Society, 2004.

[293] D. E. Muller, "Boolean algebras in electric circuit design," *The American Mathematical Monthly*, vol. 61, no. 7 part II, pp. 27–28, 1954. (Proceedings of the symposium on special topics in applied mathematics, Northwestern University (1953)).

[294] K. Mulmuley, U. V. Vazirani, and V. V. Vazirani, "Matching is as easy as matrix inversion," *Combinatorica*, vol. 7, no. 1, pp. 105–113, 1987.

[295] S. Muthukrishnan, *Data Streams: Algorithms and Applications,* volume 1, number 2 of *Foundations and Trends in Theoretical Computer Science.* now publishers, 2005.

[296] J. Naor and M. Naor, "Small-bias probability spaces: Efficient constructions and applications," *SIAM Journal on Computing*, vol. 22, pp. 838–856, August 1993.

Full text available at: http://dx.doi.org/10.1561/0400000010

[297] A. Nilli, "On the second eigenvalue of a graph," *Discrete Mathematics*, vol. 91, no. 2, pp. 207–210, 1991.
[298] N. Nisan, "Pseudorandom bits for constant depth circuits," *Combinatorica*, vol. 11, no. 1, pp. 63–70, 1991.
[299] N. Nisan, "Pseudorandom generators for space-bounded computation," *Combinatorica*, vol. 12, no. 4, pp. 449–461, 1992.
[300] N. Nisan, "RL $\subseteq$ SC," *Computational Complexity*, vol. 4, no. 1, pp. 1–11, 1994.
[301] N. Nisan and A. Ta-Shma, "Extracting randomness: A survey and new constructions," *Journal of Computer and System Sciences*, vol. 58, pp. 148–173, February 1999.
[302] N. Nisan and A. Wigderson, "Hardness vs Randomness," *Journal of Computer and System Sciences*, vol. 49, pp. 149–167, October 1994.
[303] N. Nisan and D. Zuckerman, "Randomness is linear in space," *Journal of Computer and System Sciences*, vol. 52, pp. 43–52, February 1996.
[304] R. O'Donnell, "Hardness amplification within NP," *Journal of Computer and System Sciences*, vol. 69, no. 1, pp. 68–94, 2004.
[305] R. O'Donnell, "Analysis of boolean functions," Book draft available at analysisofbooleanfunctions.org, 2012.
[306] F. Parvaresh and A. Vardy, "Correcting errors beyond the Guruswami-Sudan radius in polynomial time," in *Proceedings of the IEEE Symposium on Foundations of Computer Science*, pp. 285–294, 2005.
[307] Y. Peres, "Iterating von Neumann's procedure for extracting random bits," *The Annals of Statistics*, vol. 20, no. 1, pp. 590–597, 1992.
[308] W. W. Peterson, "Encoding and error-correction procedures for the Bose-Chaudhuri codes," *IRE Transactions on Information Theory*, vol. IT-6, pp. 459–470, 1960.
[309] M. Pinsker, "On the complexity of a concentrator," in *Annual Teletraffic Conference*, pp. 318/1–318/4, Stockholm, 1973.
[310] N. Pippenger, "On simultaneous resource bounds (Preliminary Version)," in *Annual Symposium on Foundations of Computer Science (San Juan, Puerto Rico)*, pp. 307–311, 1979.
[311] N. Pippenger and M. J. Fischer, "Relations among complexity measures," *Journal of the Association for Computing Machinery*, vol. 26, no. 2, pp. 361–381, 1979.
[312] R. L. Plackett and J. E. Burman, "The design of optimum multi-factorial experiments," *Biometrika*, vol. 33, pp. 305–325, 1945.
[313] V. S. Pless, W. C. Huffman, and R. A. Brualdi, eds., *Handbook of Coding Theory. Vol. I, II.* Amsterdam: North-Holland, 1998.
[314] M. O. Rabin, "Probabilistic algorithm for testing primality," *Journal of Number Theory*, vol. 12, no. 1, pp. 128–138, 1980.
[315] J. Radhakrishnan and A. Ta-Shma, "Bounds for dispersers, extractors, and depth-two superconcentrators," *SIAM Journal on Discrete Mathematics*, vol. 13, no. 1 (electronic), pp. 2–24, 2000.
[316] P. Raghavan, "Probabilistic construction of deterministic algorithms: approximating packing integer programs," *Journal of Computer and System Sciences*, vol. 37, no. 2, pp. 130–143, 1988. (Annual IEEE Symposium on the Foundations of Computer Science (Toronto, ON, 1986)).

Full text available at: http://dx.doi.org/10.1561/0400000010

[317] D. Randall, "Mixing," in *Symposium on Foundations of Computer Science (Cambridge, MA)*, pp. 4–15, 2003.

[318] A. Rao, "Extractors for a constant number of polynomially small min-entropy independent sources," *SIAM Journal on Computing*, vol. 39, no. 1, pp. 168–194, 2009.

[319] R. Raz and O. Reingold, "On recycling the randomness of states in space bounded computation," in *Annual ACM Symposium on Theory of Computing (Atlanta, GA, 1999)*, pp. 159–168 (electronic), New York: ACM, 1999.

[320] R. Raz, O. Reingold, and S. Vadhan, "Extracting all the Randomness and Reducing the Error in Trevisan's Extractors," *Journal of Computer and System Sciences*, vol. 65, pp. 97–128, August 2002.

[321] A. Razborov, E. Szemerédi, and A. Wigderson, "Constructing small sets that are uniform in arithmetic progressions," *Combinatorics Probability Computing*, vol. 2, no. 4, pp. 513–518, 1993.

[322] A. A. Razborov, "Lower bounds on the dimension of schemes of bounded depth in a complete basis containing the logical addition function," *Akademiya Nauk SSSR. Matematicheskie Zametki*, vol. 41, no. 4, pp. 598–607, 623, 1987.

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

[324] I. S. Reed, "A class of multiple-error-correcting codes and the decoding scheme," *IRE Transactions on Information Theory,* PGIT-4, pp. 38–49, 1954.

[325] I. S. Reed and G. Solomon, "Polynomial codes over certain finite fields," *Journal of the Society of Industrial and Applied Mathematics*, vol. 8, pp. 300–304, 1960.

[326] O. Reingold, "On black-box separations in cryptography," *Tutorial at the Third Theory of Cryptography Conference (TCC '06)*, March 2006. Slides available from http://research.microsoft.com/en-us/people/omreing/.

[327] O. Reingold, "Undirected connectivity in log-space," *Journal of the ACM*, vol. 55, no. 4, pp. Art 17, 24, 2008.

[328] O. Reingold, R. Shaltiel, and A. Wigderson, "Extracting randomness via repeated condensing," *SIAM Journal on Computing*, vol. 35, no. 5, pp. 1185–1209, (electronic), 2006.

[329] O. Reingold, L. Trevisan, M. Tulsiani, and S. Vadhan, "Dense subsets of pseudorandom sets," in *Proceedings of the Annual IEEE Symposium on Foundations of Computer Science (FOCS '08)*, pp. 76–85, 26–28 October 2008.

[330] O. Reingold, L. Trevisan, and S. Vadhan, "Notions of reducibility between cryptographic primitives," in *Proceedings of the First Theory of Cryptography Conference (TCC '04),* vol. 2951 of *Lecture Notes in Computer Science*, (M. Naor, ed.), pp. 1–20, Springer-Verlag, 19–21 February 2004.

[331] O. Reingold, L. Trevisan, and S. Vadhan, "Pseudorandom Walks in Regular Digraphs and the RL vs. L Problem," in *Proceedings of the Annual ACM Symposium on Theory of Computing (STOC '06)*, pp. 457–466, 21–23 May 2006. (Preliminary version as *ECCC* TR05-22, February 2005).

Full text available at: http://dx.doi.org/10.1561/0400000010

[332] O. Reingold, S. Vadhan, and A. Wigderson, "Entropy waves, the zig-zag graph product, and new constant-degree expanders and extractors," in *Proceedings of the Annual Symposium on Foundations of Computer Science (FOCS '00)*, pp. 3–13, Redondo Beach, CA, 17–19 October 2000.

[333] O. Reingold, S. Vadhan, and A. Wigderson, "Entropy waves, the zig-zag graph product, and new constant-degree expanders," *Annals of Mathematics*, vol. 155, no. 1, January 2001.

[334] O. Reingold, S. Vadhan, and A. Wigderson, "A note on extracting randomness from Santha–Vazirani sources," *Unpublished manuscript*, September 2004.

[335] A. Rényi, "On measures of entropy and information," in *Proceedings of Berkeley Symposium on Mathematics Statistics and Probability, Vol. I*, pp. 547–561, Berkeley, California: University of California Press, 1961.

[336] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the Association for Computing Machinery*, vol. 21, no. 2, pp. 120–126, 1978.

[337] D. Ron, "Property testing," in *Handbook of Randomized Computing, Vol. I, II, volume 9 of Comb. Optim.*, pp. 597–649, Dordrecht: Kluwer Academic Publications, 2001.

[338] E. Rozenman and S. Vadhan, "Derandomized squaring of graphs," in *Proceedings of the International Workshop on Randomization and Computation (RANDOM '05),* vol. 3624 of *Lecture notes in Computer Science*, pp. 436–447, Berkeley, CA, August 2005.

[339] R. Rubinfeld, "Sublinear time algorithms," in *International Congress of Mathematicians. Vol. III*, pp. 1095–1110, Zürich: European Mathematical Society, 2006.

[340] R. Rubinfeld and M. Sudan, "Robust characterizations of polynomials with applications to program testing," *SIAM Journal on Computing*, vol. 25, no. 2, pp. 252–271, 1996.

[341] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray, and S. Vo, "A statistical test suite for random and pseudorandom number generators for cryptographic applications," National Institute of Standards and Technology, U.S. Department of Commerce, Special Publication 800-22, Revision 1a, April 2010.

[342] S. Sahni and T. Gonzalez, "P-complete approximation problems," *Journal of the ACM*, vol. 23, no. 3, pp. 555–565, 1976.

[343] M. Saks, A. Srinivasan, and S. Zhou, "Explicit OR-dispersers with polylogarithmic degree," *Journal of the ACM*, vol. 45, no. 1, pp. 123–154, 1998.

[344] M. Saks and S. Zhou, "$\mathrm{BP_HSPACE}(S) \subseteq \mathrm{DSPACE}(S^{3/2})$," *Journal of Computer and System Sciences*, vol. 58, no. 2, pp. 376–403, 1999.

[345] M. Saks and D. Zuckerman, Unpublished manuscript. 1995.

[346] M. Sántha and U. V. Vazirani, "Generating quasirandom sequences from semirandom sources," *Journal of Computer and System Sciences*, vol. 33, no. 1, pp. 75–87, 1986. (Annual Symposium on Foundations of Computer Science (Singer Island, FL, 1984)).

Full text available at: http://dx.doi.org/10.1561/0400000010

[347] R. Santhanam, "Circuit lower bounds for Merlin-Arthur classes," in *STOC'07 — Proceedings of the Annual ACM Symposium on Theory of Computing*, pp. 275–283, New York, 2007.

[348] P. Sarnak, *Some Applications of Modular Forms.* Vol. 99 of *Cambridge Tracts in Mathematics.* Cambridge: Cambridge University Press, 1990.

[349] W. J. Savitch, "Relationships between nondeterministic and deterministic tape complexities," *Journal of Computer and System Sciences*, vol. 4, pp. 177–192, 1970.

[350] J. P. Schmidt, A. Siegel, and A. Srinivasan, "Chernoff-Hoeffding bounds for applications with limited independence," *SIAM Journal on Discrete Mathematics*, vol. 8, no. 2, pp. 223–250, 1995.

[351] J. T. Schwartz, "Fast probabilistic algorithms for verification of polynomial identities," *Journal of the ACM*, vol. 27, no. 4, pp. 701–717, 1980.

[352] R. Shaltiel, "Recent Developments in Extractors," in *Current Trends in Theoretical Computer Science,* vol. 1, (G. Paun, G. Rozenberg, and A. Salomaa, eds.), pp. 189–228, World Scientific, 2004.

[353] R. Shaltiel, "Dispersers for affine sources with sub-polynomial entropy," in *FOCS*, (R. Ostrovsky, ed.), pp. 247–256, IEEE, 2011.

[354] R. Shaltiel, "An introduction to randomness extractors," in *Automata, languages and programming. Part II, vol. 6756 of Lecture Notes in Computer Science*, pp. 21–41, Heidelberg: Springer, 2011.

[355] R. Shaltiel, "Weak derandomization of weak algorithms: explicit versions of Yao's lemma," *Computational Complexity*, vol. 20, no. 1, pp. 87–143, 2011.

[356] R. Shaltiel and C. Umans, "Simple extractors for all min-entropies and a new Pseudo-random generator," *Journal of the ACM*, vol. 52, no. 2, pp. 172–216, 2005.

[357] R. Shaltiel and C. Umans, "Pseudorandomness for approximate counting and sampling," *Computational Complexity*, vol. 15, no. 4, pp. 298–341, 2006.

[358] R. Shaltiel and C. Umans, "Low-end uniform hardness versus randomness tradeoffs for AM," *SIAM Journal on Computing*, vol. 39, no. 3, pp. 1006–1037, 2009.

[359] A. Shamir, "How to share a secret," *Communications of the Association for Computing Machinery*, vol. 22, no. 11, pp. 612–613, 1979.

[360] A. Shamir, "On the generation of cryptographically strong pseudorandom sequences," in *Automata, Languages and Programming (Akko, 1981),* vol. 115 of *Lecture Notes in Computer Science*, pp. 544–550, Berlin: Springer, 1981.

[361] C. E. Shannon, "A mathematical theory of communication," *The Bell System Technical Journal*, vol. 27, pp. 379–423, 623–656, 1948.

[362] A. Shpilka and A. Yehudayoff, "Arithmetic circuits: A survey of recent results and open questions," *Foundations and Trends® in Theoretical Computer Science*, vol. 5, no. 3–4, pp. 207–388 (2010), 2009.

[363] J. Síma and S. Zák, "Almost k-wise independent sets establish hitting sets for width-3 1-branching programs," in *CSR,* vol. 6651 of *Lecture Notes in Computer Science*, (A. S. Kulikov and N. K. Vereshchagin, eds.), pp. 120–133, Springer, 2011.

Full text available at: http://dx.doi.org/10.1561/0400000010

[364] M. Sipser, "A complexity theoretic approach to randomness," in *Annual ACM Symposium on Theory of Computing*, pp. 330–335, Boston, Massachusetts, 25–27 April 1983.

[365] M. Sipser, "Expanders, randomness, or time versus space," *Journal of Computer and System Sciences*, vol. 36, no. 3, pp. 379–383, 1988. (Structure in Complexity Theory Conference (Berkeley, CA, 1986)).

[366] M. Sipser, *Introduction to the Theory of Computation.* Course Technology, 2nd Edition, 2005.

[367] M. Sipser and D. A. Spielman, "Expander codes," *IEEE Transactions on Information Theory*, vol. 42, no. 6 part 1, pp. 1710–1722, 1996. (Codes and complexity).

[368] R. Smolensky, "Algebraic methods in the theory of lower bounds for Boolean circuit complexity," in *STOC*, (A. V. Aho, ed.), pp. 77–82, ACM, 1987.

[369] R. Solovay and V. Strassen, "A fast Monte-Carlo test for primality," *SIAM Journal on Computing*, vol. 6, no. 1, pp. 84–85, 1977.

[370] J. Spencer, *Ten Lectures on the Probabilistic Method,* volume 64 of *CBMS-NSF Regional Conference Series in Applied Mathematics.* Philadelphia, PA: Society for Industrial and Applied Mathematics (SIAM), Second Edition, 1994.

[371] D. A. Spielman, "Spectral graph theory and its applications," in *Symposium on Foundations of Computer Science (FOCS 2007), 21-23 October 2007, Providence, RI, USA, Proceedings*, pp. 29–38, 2007.

[372] A. Srinivasan and D. Zuckerman, "Computing with very weak random sources," *SIAM Journal on Computing*, vol. 28, no. 4, pp. 1433–1459 (electronic), 1999.

[373] T. Steinke, "Pseudorandomness for permutation branching programs without the group theory," Technical Report TR12-083, Electronic Colloquium on Computational Complexity (ECCC), July 2012.

[374] J. Stern, "Secret linear congruential generators are not cryptographically secure," in *FOCS*, pp. 421–426, IEEE Computer Society, 1987.

[375] H. Stichtenoth, *Algebraic Function Fields and Codes,* volume 254 of *Graduate Texts in Mathematics.* Berlin: Springer-Verlag, Second Edition, 2009.

[376] D. R. Stinson, "Combinatorial techniques for universal hashing," *Journal of Computer and System Sciences*, vol. 48, no. 2, pp. 337–346, 1994.

[377] V. Strassen, "Gaussian elimination is not optimal," *Numerische Mathematik*, vol. 13, pp. 354–356, 1969.

[378] M. Sudan, "Decoding of Reed Solomon codes beyond the error-correction bound," *Journal of Complexity*, vol. 13, pp. 180–193, March 1997.

[379] M. Sudan, "Algorithmic introduction to coding theory," Lecture notes, http://people.csail.mit.edu/madhu/FT01/, 2001.

[380] M. Sudan, "Essential coding theory (lecture notes)," http://people.csail.mit.edu/madhu/FT04/, 2004.

[381] M. Sudan, L. Trevisan, and S. Vadhan, "Pseudorandom generators without the XOR lemma," *Journal of Computer and System Sciences*, vol. 62, pp. 236–266, 2001.

[382] A. Ta-Shma, C. Umans, and D. Zuckerman, "Lossless condensers, unbalanced expanders, and extractors," *Combinatorica*, vol. 27, no. 2, pp. 213–240, 2007.

Full text available at: http://dx.doi.org/10.1561/0400000010

[383] A. Ta-Shma and D. Zuckerman, "Extractor codes," *IEEE Transactions on Information Theory*, vol. 50, no. 12, pp. 3015–3025, 2004.

[384] A. Ta-Shma, D. Zuckerman, and S. Safra, "Extractors from Reed-Muller codes," *Journal of Computer and System Sciences*, vol. 72, no. 5, pp. 786–812, 2006.

[385] M. R. Tanner, "Explicit concentrators from generalized N-gons," *SIAM Journal on Algebraic Discrete Methods*, vol. 5, no. 3, pp. 287–293, 1984.

[386] T. Tao, "Expansion in finite groups of Lie type," Lecture Notes, http://www.math.ucla.edu/ tao/254b.1.12w/, 2012.

[387] A. Terras, *Fourier Analysis on Finite Groups and Applications,* volume 43 of *London Mathematical Society Student Texts*. Cambridge: Cambridge University Press, 1999.

[388] S. Tessaro, "Computational indistinguishability amplification," PhD thesis, ETH Zurich, http://e-collection.library.ethz.ch/eserv/eth:1817/eth-1817-02.pdf, 2010.

[389] L. Trevisan, "Extractors and pseudorandom generators," *Journal of the ACM*, vol. 48, no. 4, pp. 860–879, (electronic), 2001.

[390] L. Trevisan, "List decoding using the XOR lemma," in *Proceedings of the IEEE Symposium on Foundations of Computer Science*, pp. 126–135, Cambridge, MA, October 2003.

[391] L. Trevisan, "Some applications of coding theory in computational complexity," *Quaderni di Matematica*, vol. 13, pp. 347–424, 2004.

[392] L. Trevisan, "On uniform amplification of hardness in NP," in *STOC'05: Proceedings of the Annual ACM Symposium on Theory of Computing*, pp. 31–38, New York, 2005.

[393] L. Trevisan, "Pseudorandomness and combinatorial constructions," in *International Congress of Mathematicians. Vol. III*, pp. 1111–1136, Zürich: European Mathematics Society, 2006.

[394] L. Trevisan, "Guest column: Additive combinatorics and theoretical computer science," *SIGACT News*, vol. 40, no. 2, pp. 50–66, 2009.

[395] L. Trevisan, "Dense model theorems and their applications," in *Theory of cryptography,* vol. 6597 of *Lecture Notes in Computer Science*, pp. 55–57, Heidelberg: Springer, 2011.

[396] L. Trevisan, M. Tulsiani, and S. Vadhan, "Regularity, boosting, and efficiently simulating every high-entropy distribution," in *Proceedings of the Annual IEEE Conference on Computational Complexity (CCC '09)*, pp. 126–136, 15–18 July 2009. (Preliminary version posted as *ECCC* TR08-103).

[397] L. Trevisan and S. Vadhan, "Pseudorandomness and average-case complexity via uniform reductions," *Computational Complexity*, vol. 16, pp. 331–364, December 2007.

[398] L. Trevisan and S. Vadhan, "Extracting randomness from samplable distributions," in *Proceedings of the Annual Symposium on Foundations of Computer Science (FOCS '00)*, pp. 32–42, Redondo Beach, CA, 17–19 October 2000.

[399] C. Umans, "Pseudo-random generators for all hardnesses," *Journal of Computer and System Sciences*, vol. 67, no. 2, pp. 419–440, 2003.

Full text available at: http://dx.doi.org/10.1561/0400000010

[400] S. Vadhan, "Probabilistic proof systems, Part I — interactive & zero-knowledge proofs," in *Computational Complexity Theory,* vol. 10 of *IAS/Park City Mathematics Series*, (S. Rudich and A. Wigderson, eds.), pp. 315–348, American Mathematical Society, 2004.

[401] S. Vadhan and C. J. Zheng, "Characterizing pseudoentropy and simplifying pseudorandom generator constructions," in *Proceedings of the Annual ACM Symposium on Theory of Computing (STOC '12)*, pp. 817–836, 19–22 May 2012.

[402] S. P. Vadhan, "Constructing locally computable extractors and cryptosystems in the bounded-storage model," *Journal of Cryptology*, vol. 17, no. 1, pp. 43–77, January 2004.

[403] L. G. Valiant, "Graph-theoretic properties in computational complexity," *Journal of Computer and System Sciences*, vol. 13, no. 3, pp. 278–285, 1976.

[404] L. G. Valiant, "The complexity of computing the permanent," *Theoretical Computer Science*, vol. 8, no. 2, pp. 189–201, 1979.

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

[406] R. Varshamov, "Estimate of the number of signals in error correcting codes," *Doklady Akademe Nauk SSSR*, vol. 117, pp. 739–741, 1957.

[407] U. V. Vazirani, "Towards a strong communication complexity theory or generating quasi-random sequences from two communicating slightly-random sources (extended abstract)," in *Proceedings of the Annual ACM Symposium on Theory of Computing*, pp. 366–378, Providence, Rhode Island, 6–8 May 1985.

[408] U. V. Vazirani, "Efficiency considerations in using semi-random sources (extended abstract)," in *STOC*, (A. V. Aho, ed.), pp. 160–168, ACM, 1987.

[409] U. V. Vazirani, "Strong communication complexity or generating quasirandom sequences from two communicating semirandom sources," *Combinatorica*, vol. 7, no. 4, pp. 375–392, 1987.

[410] U. V. Vazirani and V. V. Vazirani, "Random polynomial time is equal to slightly-random polynomial time," in *Annual Symposium on Foundations of Computer Science*, pp. 417–428, Portland, Oregon, 21–23 October 1985.

[411] E. Viola, "The complexity of constructing pseudorandom generators from hard functions," *Computational Complexity*, vol. 13, no. 3–4, pp. 147–188, 2004.

[412] E. Viola, "Pseudorandom bits for constant-depth circuits with few arbitrary symmetric gates," *SIAM Journal on Computing*, vol. 36, no. 5, pp. 1387–1403, (electronic), 2006/2007.

[413] E. Viola, "The sum of d small-bias generators fools polynomials of degree d," *Computational Complexity*, vol. 18, no. 2, pp. 209–217, 2009.

[414] E. Viola, "Extractors for circuit sources," in *FOCS*, (R. Ostrovsky, ed.), pp. 220–229, IEEE, 2011.

[415] E. Viola, "The complexity of distributions," *SIAM Journal on Computing*, vol. 41, no. 1, pp. 191–218, 2012.

[416] J. von Neumann, "Various techniques used in conjunction with random digits," in *Collected Works. Vol. V: Design of Computers, Theory of Automata and Numerical Analysis*, New York: The Macmillan Co., 1963.

Full text available at: http://dx.doi.org/10.1561/0400000010

[417] M. N. Wegman and J. L. Carter, "New hash functions and their use in authentication and set equality," *Journal of Computer and System Sciences*, vol. 22, no. 3, pp. 265–279, 1981.

[418] R. Williams, "Improving exhaustive search implies superpolynomial lower bounds," in *STOC'10 — Proceedings of the 2010 ACM International Symposium on Theory of Computing*, pp. 231–240, New York: ACM, 2010.

[419] R. Williams, "Non-uniform ACC circuit lower bounds," in *IEEE Conference on Computational Complexity*, pp. 115–125, 2011.

[420] J. Wozencraft, "List decoding," *Quarterly Progress Report, Research Laboratory of Electronics, MIT*, vol. 48, pp. 90–95, 1958.

[421] A. C. Yao, "Theory and applications of trapdoor functions (extended abstract)," in *Annual Symposium on Foundations of Computer Science*, pp. 80–91, Chicago, Illinois, 3–5 November 1982.

[422] A. Yehudayoff, "Affine extractors over prime fields," *Combinatorica*, vol. 31, no. 2, pp. 245–256, 2011.

[423] S. Yekhanin, "Towards 3-query locally decodable codes of subexponential length," *Journal of the ACM*, vol. 55, no. 1, pp. Art 1, 16, 2008.

[424] S. Yekhanin, *Locally Decodable Codes*. Now Publishers, 2012. (To appear).

[425] R. Zippel, "Probabilistic algorithms for sparse polynomials," in *EUROSAM,* vol. 72 of *Lecture Notes in Computer Science*, (E. W. Ng, ed.), pp. 216–226, Springer, 1979.

[426] D. Zuckerman, "Simulating BPP using a general weak random source," *Algorithmica*, vol. 16, pp. 367–391, October/November 1996.

[427] D. Zuckerman, "Randomness-optimal oblivious sampling," *Random Structures & Algorithms*, vol. 11, no. 4, pp. 345–367, 1997.

[428] V. V. Zyablov and M. S. Pinsker, "List cascade decoding (in Russian)," *Problems of Information Transmission*, vol. 17, no. 4, pp. 29–33, 1981.