University
LECTURE
Series

Applied
Mathematics

Volume 55

A Primer on Pseudorandom Generators

Oded Goldreich

American Mathematical Society

http://dx.doi.org/10.1090/ulect/055

A Primer on Pseudorandom Generators

University
LECTURE
Series

Volume 55

A Primer on Pseudorandom Generators

Oded Goldreich

American Mathematical Society
Providence, Rhode Island

2010 *Mathematics Subject Classification.* Primary 68-01, 68-02, 68Q01, 68R01; Secondary 68Q15, 68Q17, 68W20.

For additional information and updates on this book, visit
www.ams.org/bookpages/ulect-55

Library of Congress Cataloging-in-Publication Data

Goldreich, Oded.
A primer on pseudorandom generators / Oded Goldreich.
p. cm. — (University lecture series ; v. 55)
Includes bibliographical references and index.
ISBN 978-0-8218-5192-0 (alk. paper)
1. Computational complexity. 2. Random number generators. 3. Computer science–Mathematics. I. Title

QA267.7.G654 2010
004.01′51–dc22 2010018152

---

10 9 8 7 6 5 4 3 2 1 15 14 13 12 11 10

Contents

Preface

Indistinguishable things are identical.[1]

G.W. Leibniz (1646–1714)

This primer to the theory of pseudorandomness presents a fresh look at the *question of randomness*, which arises from a complexity theoretic approach to randomness. The crux of this (complexity theoretic) approach is the postulate that a distribution is random (or rather pseudorandom) if it cannot be distinguished from the uniform distribution by *any efficient procedure*. Thus, (pseudo)randomness is not an inherent property of an object, but is rather subjective to the observer.

At the extreme, this approach says that the question of whether the world is actually deterministic or allows for some free choice (which may be viewed as a source of randomness) is irrelevant. *What matters is how the world looks to us and to various computationally bounded devices*. That is, if some phenomenon looks random, then we may treat it as if it is random. Likewise, if we can generate sequences that cannot be distinguished from the uniform distribution by any efficient procedure, then we can use these sequences in any efficient randomized application instead of the ideal coin tosses that are postulated in the design of this application.

The pivot of the foregoing approach is the notion of *computational indistinguishability*, which refers to pairs of distributions that cannot be distinguished by efficient procedures. The most fundamental incarnation of this notion associates efficient procedures with polynomial-time algorithms, but other incarnations that restrict attention to different classes of distinguishing procedures also lead to important insights. Likewise, the *effective generation* of pseudorandom objects, which is of major concern, is actually a general paradigm with numerous useful incarnations (which differ in the computational complexity limitations imposed on the generation process).

Following the foregoing principles, we briefly outline some of the key elements of the theory of pseudorandomness. Indeed, the key concept is that of a pseudorandom generator, which is an efficient deterministic procedure that stretches short random seeds into longer pseudorandom sequences. Thus, a generic formulation of pseudorandom generators consists of specifying three fundamental aspects – the *stretch measure* of the generators; the class of distinguishers that the generators are

[1] This is Leibniz's *Principle of Identity of Indiscernibles*. Leibniz admits that counterexamples to this principle are conceivable but will not occur in real life because God is much too benevolent. We thus believe that he would have agreed to the theme of this text, which asserts that *indistinguishable things should be considered as if they were identical*.

supposed to fool (i.e., the algorithms with respect to which the *computational indistinguishability* requirement should hold); and the resources that the generators are allowed to use (i.e., their own *computational complexity*).

The archetypical case of pseudorandom generators refers to efficient generators that fool any feasible procedure; that is, the potential distinguisher is any probabilistic polynomial-time algorithm, which may be more complex than the generator itself (which, in turn, has time-complexity bounded by a fixed polynomial). These generators are called general-purpose, because their output can be safely used in any efficient application. Such (general-purpose) pseudorandom generators exist if and only if there exist functions (called one-way functions) that are easy to evaluate but hard to invert.

In contrast to such (general-purpose) pseudorandom generators, for the purpose of derandomization (i.e., converting randomized algorithms into corresponding deterministic ones), a relaxed definition of pseudorandom generators suffices. In particular, for such a purpose, one may use pseudorandom generators that are somewhat more complex than the potential distinguisher (which represents a randomized algorithm to be derandomized). Following this approach, adequate pseudorandom generators yield a full derandomization of probabilistic polynomial-time algorithms (e.g., $\mathcal{BPP} = \mathcal{P}$), and such generators can be constructed based on the assumption that some exponential-time solvable problems (i.e., problems in $\mathcal{E}$) have no sub-exponential size circuits.

Indeed, both the general-purpose pseudorandom generators and the aforementioned "derandomizers" demonstrate that randomness and computational difficulty are related. This trade-off is not surprising in light of the fact that the very definition of pseudorandomness refers to computational difficulty (i.e., the difficulty of distinguishing the pseudorandom distribution from a truly random one).

Finally, we mention that it is also beneficial to consider pseudorandom generators that fool space-bounded distinguishers and generators that exhibit some limited random behavior (e.g., outputting a pairwise independent or a small-bias sequence). Such (special-purpose) pseudorandom generators can be constructed without relying on any computational complexity assumptions, because the behavior of the corresponding (limited) distinguishers can be analyzed even at the current historical time. Nevertheless, such (special-purpose) pseudorandom generators offer numerous applications.

Note: The study of pseudorandom generators is part of complexity theory (cf. e.g., [24]), and some basic familiarity with complexity theory will be assumed in the current text. In fact, the current primer is an abbreviated (and somewhat revised) version of [24, Chap. 8]. Nevertheless, we believe that there are merits to providing a separate treatment of the theory of pseudorandomness, since this theory is of natural interest to various branches of mathematics and science. In particular, we hope to reach readers that may not have a general interest in complexity theory at large and/or do not wish to purchase a book on the latter topic.

Acknowledgments. We are grateful to Alina Arbitman and Ron Rothblum for their comments and suggestions regarding this primer.

Oded Goldreich
Weizmann Institute of Science

Bibliography

[1] M. Agrawal, N. Kayal, and N. Saxena. PRIMES is in P. *Annals of Mathematics*, Vol. 160 (2), pages 781–793, 2004.

[2] M. Ajtai, J. Komlos, E. Szemerédi. Deterministic Simulation in LogSpace. In *19th ACM Symposium on the Theory of Computing*, pages 132–140, 1987.

[3] 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 *20th IEEE Symposium on Foundations of Computer Science*, pages 218–223, 1979.

[4] N. Alon, L. Babai and A. Itai. A Fast and Simple Randomized Algorithm for the Maximal Independent Set Problem. *J. of Algorithms*, Vol. 7, pages 567–583, 1986.

[5] N. Alon, O. Goldreich, J. Håstad, R. Peralta. Simple Constructions of Almost k-wise Independent Random Variables. *Journal of Random Structures and Algorithms*, Vol. 3, No. 3, pages 289–304, 1992. Preliminary version in *31st FOCS*, 1990.

[6] N. Alon and J.H. Spencer. *The Probabilistic Method*. John Wiley & Sons, Inc., 1992. Second edition, 2000.

[7] R. Armoni. On the Derandomization of Space-Bounded Computations. In the proceedings of *Random98*, Springer-Verlag, Lecture Notes in Computer Science (Vol. 1518), pages 49–57, 1998.

[8] H. Attiya and J. Welch. *Distributed Computing: Fundamentals, Simulations and Advanced Topics*. McGraw-Hill, 1998.

[9] L. Babai, L. Fortnow, N. Nisan and A. Wigderson. BPP has Subexponential Time Simulations Unless EXPTIME has Publishable Proofs. *Complexity Theory*, Vol. 3, pages 307–318, 1993.

[10] M. Bellare, O. Goldreich and M. Sudan. Free Bits, PCPs and Non-Approximability – Towards Tight Results. *SIAM Journal on Computing*, Vol. 27, No. 3, pages 804–915, 1998. Extended abstract in *36th FOCS*, 1995.

[11] M. Blum and S. Micali. How to Generate Cryptographically Strong Sequences of Pseudo-Random Bits. *SIAM Journal on Computing*, Vol. 13, pages 850–864, 1984. Preliminary version in *23rd FOCS*, 1982.

[12] M. Braverman. Poly-logarithmic Independence Fools AC0 Circuits. In *24th IEEE Conference on Computational Complexity*, pages 3–8, 2009.

[13] L. Carter and M. Wegman. Universal Hash Functions. *Journal of Computer and System Science*, Vol. 18, 1979, pages 143–154.

[14] G.J. Chaitin. On the Length of Programs for Computing Finite Binary Sequences. *Journal of the ACM*, Vol. 13, pages 547–570, 1966.

[15] B. Chor and O. Goldreich. On the Power of Two–Point Based Sampling. *Jour. of Complexity*, Vol. 5, pages 96–106, 1989. Preliminary version dates 1985.

[16] T.M. Cover and G.A. Thomas. *Elements of Information Theory*. John Wiley & Sons, Inc., New York, 1991.

[17] W. Diffie, and M.E. Hellman. New Directions in Cryptography. *IEEE Transactions on Information Theory*, IT-22 (Nov. 1976), pages 644–654.

[18] O. Gaber and Z. Galil. Explicit Constructions of Linear Size Superconcentrators. *Journal of Computer and System Science*, Vol. 22, pages 407–420, 1981.

[19] M.R. Garey and D.S. Johnson. *Computers and Intractability: A Guide to the Theory of NP-Completeness*. W.H. Freeman and Company, New York, 1979.

[20] O. Goldreich. A Note on Computational Indistinguishability. *Information Processing Letters*, Vol. 34, pages 277–281, May 1990.

[21] O. Goldreich. *Modern Cryptography, Probabilistic Proofs and Pseudorandomness*. Algorithms and Combinatorics series (Vol. 17), Springer, 1999.

[22] O. Goldreich. *Foundation of Cryptography: Basic Tools*. Cambridge University Press, 2001.

[23] O. Goldreich. *Foundation of Cryptography: Basic Applications*. Cambridge University Press, 2004.

[24] O. Goldreich. *Computational Complexity: A Conceptual Perspective*. Cambridge University Press, 2008.

[25] O. Goldreich, S. Goldwasser, and S. Micali. How to Construct Random Functions. *Journal of the ACM*, Vol. 33, No. 4, pages 792–807, 1986.

[26] O. Goldreich, S. Goldwasser, and A. Nussboim. On the Implementation of Huge Random Objects. In *44th IEEE Symposium on Foundations of Computer Science*, pages 68–79, 2003.

[27] O. Goldreich and L.A. Levin. Hard-core Predicates for any One-Way Function. In *21st ACM Symposium on the Theory of Computing*, pages 25–32, 1989.

[28] O. Goldreich and B. Meyer. Computational Indistinguishability – Algorithms vs. Circuits. *Theoretical Computer Science*, Vol. 191, pages 215–218, 1998. Preliminary version by Meyer in *Structure in Complexity Theory*, 1994.

[29] S. Goldwasser and S. Micali. Probabilistic Encryption. *Journal of Computer and System Science*, Vol. 28, No. 2, pages 270–299, 1984. Preliminary version in *14th STOC*, 1982.

[30] V. Guruswami, C. Umans, and S. Vadhan. Unbalanced Expanders and Randomness Extractors from Parvaresh-Vardy Codes. *Journal of the ACM*, Vol. 56 (4), Article No. 20, 2009. Preliminary version in *22nd CCC*, 2007.

[31] I. Haitner, O. Reingold, and S. Vadhan. Efficiency Improvements in Constructing Pseudorandom Generator from any One-way Function. In *42nd ACM Symposium on the Theory of Computing*, to appear.

[32] J. Håstad, R. Impagliazzo, L.A. Levin and M. Luby. A Pseudorandom Generator from any One-way Function. *SIAM Journal on Computing*, Volume 28, Number 4, pages 1364–1396, 1999. Preliminary versions by Impagliazzo *et al.* in *21st STOC* (1989) and Håstad in *22nd STOC* (1990).

[33] A. Healy. Randomness-Efficient Sampling within NC1. *Computational Complexity*, Vol. 17 (1), pages 3–37, 2008.

[34] R. Impagliazzo and A. Wigderson. P=BPP If E Requires Exponential Circuits: Derandomizing the XOR Lemma. In *29th ACM Symposium on the Theory of Computing*, pages 220–229, 1997.

[35] R. Impagliazzo and A. Wigderson. Randomness vs Time: Derandomization under a Uniform Assumption. *Journal of Computer and System Science*, Vol. 63 (4), pages 672-688, 2001.

[36] N. Kahale. Eigenvalues and Expansion of Regular Graphs. *Journal of the ACM*, Vol. 42 (5), pages 1091–1106, September 1995.

[37] D.E. Knuth. *The Art of Computer Programming*, Vol. 2 (*Seminumerical Algorithms*). Addison-Wesley Publishing Company, Inc., 1969 (first edition) and 1981 (second edition).

[38] A. Kolmogorov. Three Approaches to the Concept of "The Amount of Information". *Probl. of Inform. Transm.*, Vol. 1/1, 1965.

[39] E. Kushilevitz and N. Nisan. *Communication Complexity*. Cambridge University Press, 1996.

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

[41] L.A. Levin. Randomness Conservation Inequalities: Information and Independence in Mathematical Theories. *Information and Control*, Vol. 61, pages 15–37, 1984.

[42] M. Li and P. Vitanyi. *An Introduction to Kolmogorov Complexity and its Applications*. Springer-Verlag, August 1993.

[43] A. Lubotzky, R. Phillips, and P. Sarnak. Ramanujan Graphs. *Combinatorica*, Vol. 8, pages 261–277, 1988.

[44] G.A. Margulis. Explicit Construction of Concentrators. *Prob. Per. Infor.*, Vol. 9 (4), pages 71–80, 1973 (in Russian). English translation in *Problems of Infor. Trans.*, pages 325–332, 1975.

[45] P.B. Miltersen and N.V. Vinodchandran. Derandomizing Arthur-Merlin Games using Hitting Sets. *Computational Complexity*, Vol. 14 (3), pages 256–279, 2005. Preliminary version in *40th FOCS*, 1999.

[46] M. Mitzenmacher and E. Upfal. *Probability and Computing: Randomized Algorithms and Probabilistic Analysis*. Cambridge University Press, 2005

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

[48] J. Naor and M. Naor. Small-bias Probability Spaces: Efficient Constructions and Applications. *SIAM Journal on Computing*, Vol. 22, 1993, pages 838–856. Preliminary version in *22nd STOC*, 1990.

[49] N. Nisan. Pseudorandom Bits for Constant Depth Circuits. *Combinatorica*, Vol. 11 (1), pages 63–70, 1991.

[50] N. Nisan. Pseudorandom Generators for Space Bounded Computation. *Combinatorica*, Vol. 12 (4), pages 449–461, 1992. Preliminary version in *22nd STOC*, 1990.

[51] N. Nisan. $\mathcal{RL} \subseteq \mathcal{SC}$. *Computational Complexity*, Vol. 4, pages 1-11, 1994. Preliminary version in *24th STOC*, 1992.

[52] N. Nisan and A. Wigderson. Hardness vs. Randomness. *Journal of Computer and System Science*, Vol. 49, No. 2, pages 149–167, 1994. Preliminary version in *29th FOCS*, 1988.

[53] N. Nisan and D. Zuckerman. Randomness is Linear in Space. *Journal of Computer and System Science*, Vol. 52 (1), pages 43–52, 1996. Preliminary version in *25th STOC*, 1993.

[54] N. Pippenger and M.J. Fischer. Relations Among Complexity Measures. *Journal of the ACM*, Vol. 26 (2), pages 361–381, 1979.

[55] A.R. Razborov and S. Rudich. Natural Proofs. *Journal of Computer and System Science*, Vol. 55 (1), pages 24–35, 1997. Preliminary version in *26th STOC*, 1994.

[56] O. Reingold. Undirected ST-Connectivity in Log-Space. In *37th ACM Symposium on the Theory of Computing*, pages 376–385, 2005.

[57] O. Reingold, S. Vadhan, and A. Wigderson. Entropy Waves, the Zig-Zag Graph Product, and New Constant-Degree Expanders and Extractors. *Annals of Mathematics*, Vol. 155 (1), pages 157–187, 2001. Preliminary version in *41st FOCS*, pages 3–13, 2000.

[58] R.L. Rivest, A. Shamir and L.M. Adleman. A Method for Obtaining Digital Signatures and Public Key Cryptosystems. *CACM*, Vol. 21, Feb. 1978, pages 120–126.

[59] M. Saks and S. Zhou. $\mathrm{BP_HSPACE}(S) \subseteq \mathrm{DSPACE}(S^{3/2})$. *Journal of Computer and System Science*, Vol. 58 (2), pages 376–403, 1999. Preliminary version in *36th FOCS*, 1995.

[60] J.T. Schwartz. Fast Probabilistic Algorithms for Verification of Polynomial Identities. *Journal of the ACM*, Vol. 27 (4), pages 701–717, October 1980.

[61] R. Shaltiel and C. Umans. Simple Extractors for All Min-Entropies and a New Pseudo-Random Generator. In *42nd IEEE Symposium on Foundations of Computer Science*, pages 648–657, 2001.

[62] R. Shaltiel. Recent Developments in Explicit Constructions of Extractors. In *Current Trends in Theoretical Computer Science: The Challenge of the New Century, Vol. 1: Algorithms and Complexity*, World Scientific, 2004. (Editors: G. Paun, G. Rozenberg and A. Salomaa.) Preliminary version in *Bulletin of the EATCS 77*, pages 67–95, 2002.

[63] C.E. Shannon. A Mathematical Theory of Communication. *Bell Sys. Tech. Jour.*, Vol. 27, pages 623–656, 1948.

[64] R.J. Solomonoff. A Formal Theory of Inductive Inference. *Information and Control*, Vol. 7/1, pages 1–22, 1964.

[65] L. Trevisan. Extractors and Pseudorandom Generators. *Journal of the ACM*, Vol. 48 (4), pages 860–879, 2001. Preliminary version in *31st STOC*, 1999.

[66] Y. Tzur. Notions of Weak Pseudorandomness and $\mathrm{GF}(2^n)$-Polynomials. Master Thesis, Weizmann Institute of Science, 2009. Available from the theses section of *ECCC*.

[67] C. Umans. Pseudo-random Generators for all Hardness. *Journal of Computer and System Science*, Vol. 67 (2), pages 419–440, 2003.

[68] S. Vadhan. *Lecture Notes for CS 225: Pseudorandomness*, Spring 2007. Available from `http://www.eecs.harvard.edu/~salil`.

[69] L.G. Valiant. A Theory of the Learnable. *CACM*, Vol. 27/11, pages 1134–1142, 1984.

[70] E. Viola. The Sum of d Small-Bias Generators Fools Polynomials of Degree d. *Computational Complexity*, Vol. 18 (2), pages 209–217, 2009. Preliminary version in *23rd CCC*, 2008.

[71] I. Wegener. *Branching Programs and Binary Decision Diagrams – Theory and Applications*. SIAM Monographs on Discrete Mathematics and Applications, 2000.

[72] A. Wigderson. The Amazing Power of Pairwise Independence. In *26th ACM Symposium on the Theory of Computing*, pages 645–647, 1994.

[73] A.C. Yao. Theory and Application of Trapdoor Functions. In *23rd IEEE Symposium on Foundations of Computer Science*, pages 80–91, 1982.

[74] R.E. Zippel. Probabilistic algorithms for sparse polynomials. In the *Proceedings of EUROSAM '79: International Symposium on Symbolic and Algebraic Manipulation*, E. Ng (Ed.), Lecture Notes in Computer Science (Vol. 72), pages 216–226, Springer, 1979.

Index

Titles in This Series

55 **Oded Goldreich,** A primer on pseudorandom generators, 2010

54 **John M. Mackay and Jeremy T. Tyson,** Conformal dimension: Theory and application, 2010

53 **John W. Morgan and Frederick Tsz-Ho Fong,** Ricci flow and geometrization of 3-manifolds, 2010

52 **Jan Nagel and Marian Aprodu,** Koszul cohomology and algebraic geometry, 2010

51 **J. Ben Hough, Manjunath Krishnapur, Yuval Peres, and Bálint Virág,** Zeros of Gaussian analytic functions and determinantal point processes, 2009

50 **John T. Baldwin,** Categoricity, 2009

49 **József Beck,** Inevitable randomness in discrete mathematics, 2009

48 **Achill Schürmann,** Computational geometry of positive definite quadratic forms, 2008

47 **Ernst Kunz (with the assistance of and contributions by David A. Cox and Alicia Dickenstein),** Residues and duality for projective algebraic varieties, 2008

46 **Lorenzo Sadun,** Topology of tiling spaces, 2008

45 **Matthew Baker, Brian Conrad, Samit Dasgupta, Kiran S. Kedlaya, and Jeremy Teitelbaum (David Savitt and Dinesh S. Thakur, Editors),** p-adic geometry: Lectures from the 2007 Arizona Winter School, 2008

44 **Vladimir Kanovei,** Borel equivalence relations: structure and classification, 2008

43 **Giuseppe Zampieri,** Complex analysis and CR geometry, 2008

42 **Holger Brenner, Jürgen Herzog, and Orlando Villamayor (Juan Elias, Teresa Cortadellas Benítez, Gemma Colomé-Nin, and Santiago Zarzuela, Editors),** Three Lectures on Commutative Algebra, 2008

41 **James Haglund,** The q, t-Catalan numbers and the space of diagonal harmonics (with an appendix on the combinatorics of Macdonald polynomials), 2008

40 **Vladimir Pestov,** Dynamics of infinite-dimensional groups. The Ramsey–Dvoretzky–Milman phenomenon, 2006

39 **Oscar Zariski,** The moduli problem for plane branches (with an appendix by Bernard Teissier), 2006

38 **Lars V. Ahlfors,** Lectures on Quasiconformal Mappings, Second Edition, 2006

37 **Alexander Polishchuk and Leonid Positselski,** Quadratic algebras, 2005

36 **Matilde Marcolli,** Arithmetic noncommutative geometry, 2005

35 **Luca Capogna, Carlos E. Kenig, and Loredana Lanzani,** Harmonic measure: Geometric and analytic points of view, 2005

34 **E. B. Dynkin,** Superdiffusions and positive solutions of nonlinear partial differential equations, 2004

33 **Kristian Seip,** Interpolation and sampling in spaces of analytic functions, 2004

32 **Paul B. Larson,** The stationary tower: Notes on a course by W. Hugh Woodin, 2004

31 **John Roe,** Lectures on coarse geometry, 2003

30 **Anatole Katok,** Combinatorial constructions in ergodic theory and dynamics, 2003

29 **Thomas H. Wolff (Izabella Łaba and Carol Shubin, editors),** Lectures on harmonic analysis, 2003

28 **Skip Garibaldi, Alexander Merkurjev, and Jean-Pierre Serre,** Cohomological invariants in Galois cohomology, 2003

27 **Sun-Yung A. Chang, Paul C. Yang, Karsten Grove, and Jon G. Wolfson,** Conformal, Riemannian and Lagrangian geometry, The 2000 Barrett Lectures, 2002

26 **Susumu Ariki,** Representations of quantum algebras and combinatorics of Young tableaux, 2002

25 **William T. Ross and Harold S. Shapiro,** Generalized analytic continuation, 2002

24 **Victor M. Buchstaber and Taras E. Panov,** Torus actions and their applications in topology and combinatorics, 2002

23 **Luis Barreira and Yakov B. Pesin,** Lyapunov exponents and smooth ergodic theory, 2002

22 **Yves Meyer,** Oscillating patterns in image processing and nonlinear evolution equations, 2001

21 **Bojko Bakalov and Alexander Kirillov, Jr.,** Lectures on tensor categories and modular functors, 2001

20 **Alison M. Etheridge,** An introduction to superprocesses, 2000

19 **R. A. Minlos,** Introduction to mathematical statistical physics, 2000

18 **Hiraku Nakajima,** Lectures on Hilbert schemes of points on surfaces, 1999

17 **Marcel Berger,** Riemannian geometry during the second half of the twentieth century, 2000

16 **Harish-Chandra,** Admissible invariant distributions on reductive p-adic groups (with notes by Stephen DeBacker and Paul J. Sally, Jr.), 1999

15 **Andrew Mathas,** Iwahori-Hecke algebras and Schur algebras of the symmetric group, 1999

14 **Lars Kadison,** New examples of Frobenius extensions, 1999

13 **Yakov M. Eliashberg and William P. Thurston,** Confoliations, 1998

12 **I. G. Macdonald,** Symmetric functions and orthogonal polynomials, 1998

11 **Lars Gårding,** Some points of analysis and their history, 1997

10 **Victor Kac,** Vertex algebras for beginners, Second Edition, 1998

9 **Stephen Gelbart,** Lectures on the Arthur-Selberg trace formula, 1996

8 **Bernd Sturmfels,** Gröbner bases and convex polytopes, 1996

7 **Andy R. Magid,** Lectures on differential Galois theory, 1994

6 **Dusa McDuff and Dietmar Salamon,** J-holomorphic curves and quantum cohomology, 1994

5 **V. I. Arnold,** Topological invariants of plane curves and caustics, 1994

4 **David M. Goldschmidt,** Group characters, symmetric functions, and the Hecke algebra, 1993

3 **A. N. Varchenko and P. I. Etingof,** Why the boundary of a round drop becomes a curve of order four, 1992

2 **Fritz John,** Nonlinear wave equations, formation of singularities, 1990

1 **Michael H. Freedman and Feng Luo,** Selected applications of geometry to low-dimensional topology, 1989

A fresh look at the question of randomness was taken in the theory of computing: A distribution is pseudorandom if it cannot be distinguished from the uniform distribution by any efficient procedure. This paradigm, originally associating efficient procedures with polynomial-time algorithms, has been applied with respect to a variety of natural classes of distinguishing procedures. The resulting theory of pseudorandomness is relevant to science at large and is closely related to central areas of computer science, such as algorithmic design, complexity theory, and cryptography.

Detail from a drawing by Joshua Grigsit

This primer surveys the theory of pseudorandomness, starting with the general paradigm, and discussing various incarnations while emphasizing the case of general-purpose pseudorandom generators (withstanding any polynomial-time distinguisher). Additional topics include the "derandomization" of arbitrary probabilistic polynomial-time algorithms, pseudorandom generators withstanding space-bounded distinguishers, and several natural notions of special-purpose pseudorandom generators.

The primer assumes basic familiarity with the notion of efficient algorithms and with elementary probability theory, but provides a basic introduction to all notions that are actually used. As a result, the primer is essentially self-contained, although the interested reader is at times referred to other sources for more detail.

For additional information
and updates on this book, visit

www.ams.org/bookpages/ulect-55

ISBN 978-0-8218-5192-0

9 780821 851920

ULECT/55