Bibliography

[1] L. Adleman. Two theorems on random polynomial time. In *Proceedings of the 19th Annual IEEE Symposium on Foundations of Computer Science*, pages 75–83, 1978.

[2] L. Adleman, K. Manders, and G.L. Miller. On taking roots in finite fields. In *Proceedings of the 18th Annual IEEE Symposium on Foundations of Computer Science*, pages 151–163, 1977.

[3] L. M. Adleman and A. M.-D. Huang. Recognizing primes in random polynomial time. In *Proceedings of the 19th Annual ACM Symposium on Theory of Computing*, pages 462–469, 1987.

[4] A. Aggarwal and R.J. Anderson. A random $\mathcal{NC}$ algorithm for depth first search. *Combinatorica*, 8:1–12, 1988.

[5] A. V. Aho, J. E. Hopcroft, and J. D. Ullman. *The Design and Analysis of Computer Algorithms.* Addison-Wesley, 1974.

[6] A. V. Aho, J. E. Hopcroft, and J. D. Ullman. *Data Structures and Algorithms.* Addison-Wesley, Reading, MA, 1983.

[7] R.K. Ahuja, T.L. Magnanti, and J.B. Orlin. *Network Flows: Theory, Algorithms, and Applications.* Prentice-Hall, Englewood Cliffs, NJ, 1993.

[8] M. Ajtai, J. Komlós, and E. Szemerédi. Sorting in $c \log n$ parallel steps. *Combinatorica*, 3(1):1–19, 1983.

[9] M. Ajtai, J. Komlós, and E. Szemerédi. Determinsitic simulation in logspace. In *Proceedings of the 19th Annual ACM Symposium on Theory of Computing*, pages 132–140, 1987.

[10] S. Albers. Improved randomized on-line algorithms for the list update problem. To appear in the 1995 ACM-SIAM Symposium on Discrete Algorithms.

[11] D.J. Aldous. Random walks on finite groups and rapidly mixing Markov chains. In *Seminaire de Probabilites*, volume 986 of *Springer-Verlag Lecture Notes in Mathematics XVII*, pages 243–297. Springer-Verlag, 1981-82.

[12] D.J. Aldous. *Probability Approximations via the Poisson Clumping Heuristic.* Springer-Verlag, New York, 1989.

[13] D.J. Aldous. Reversible Markov chains and random walks on graphs, 1994. Unpublished Monograph, Berkeley.

[14] R. Aleliunas. Randomized parallel communication. In *ACM-SIGOPS Symposium on Principles of Distributed Systems*, pages 60–72, 1982.

[15] 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 *Proceedings of the 20th Annual Symposium on Foundations of Computer Science*, pages 218–223, San Juan, Puerto Rico, October 1979.

[16] W.R. Alford, A. Granville, and C. Pomerance. There are infinitely many Carmichael numbers. *University of Georgia Mathematics Preprint Series*, 1992.

[17] N. Alon. Eigenvalues and expanders. *Combinatorica*, 6(2):83–96, 1986.

[18] N. Alon. A parallel algorithmic version of the local lemma. In *32nd Annual IEEE Symposium on Foundations of Computer Science*, pages 586–593, 1991.

[19] N. Alon, L. Babai, and A. Itai. A fast and simple randomized algorithm for the maximal independent set problem. *Journal of Algorithms*, 7:567–583, 1986.

[20] N. Alon and F.R.K. Chung. Explicit construction of linear sized tolerant networks. *Discrete Mathematics*, 72:15–19, 1988.

[21] N. Alon, Z. Galil, and O. Margalit. On the exponent of the all pairs shortest path problem. In *Proceedings of the 32nd Annual IEEE Symposium on Foundations of Computer Science*, pages 569–575, 1991.

[22] N. Alon, Z. Galil, O. Margalit, and M. Naor. Witnesses for boolean matrix multiplication and for shortest paths. In *Proceedings of the 33rd Annual IEEE Symposium on Foundations of Computer Science*, pages 417–426, 1992.

[23] N. Alon and V.D. Milman. Eigenvalues, expanders and superconcentrators. In *Proceedings of the 25th Annual IEEE Symposium on Foundations of Computer Science*, 1984.

[24] N. Alon and J. Spencer. *The Probabilistic Method.* Wiley Interscience, New York, 1992.

[25] H. Alt, L.J. Guibas, K. Mehlhorn, R.M. Karp, and A. Wigderson. A method for obtaining randomized algorithms with small tail probabilites. Technical Report TR-91-057, International Computer Science Institute, Berkeley, 1991.

[26] I. Althöfer. On sparse approximations to randomized strategies and convex combinations. *Linear Algebra and its Applications*, 199:339–355, 1994.

[27] D. Angluin. Lecture notes on the complexity of some problems in number theory. Technical Report 243, Department of Computer Science, Yale University, 1982.

[28] D. Angluin and L.G. Valiant. Fast probabilistic algorithms for Hamiltonian circuits and matchings. *Journal of Computer and System Sciences*, 19:155–193, 1979.

[29] N. C. Ankney. The least quadratic nonresidue. *Annals of Mathematics*, 55:65–72, 1986.

[30] C.R. Aragon and R.G. Seidel. Randomized search trees. In *Proceedings of the 30th Annual IEEE Symposium on Foundations of Computer Science*, pages 540–545, 1989.

[31] S. Arora. *Probabilistic Checking of Proofs and Hardness of Approximation Problems.* PhD thesis, University of California at Berkeley, 1994.

[32] S. Arora, C. Lund, R. Motwani, M. Sudan, and M. Szegedy. Proof verification and hardness of approximation problems. In *Proceedings of the 33rd Annual IEEE Symposium on Foundations of Computer Science*, pages 14–23, 1992.

[33] S. Arora and S. Safra. Probabilistic checking of proofs: A new characterization of $\mathcal{NP}$. In *Proceedings of the 33rd Annual IEEE Symposium on Foundations of Computer Science*, pages 2–13, 1992.

[34] J. Aspnes and O. Waarts. Randomized consensus in expected $O(n \log^2 n)$ operations per processor. In *Proceedings of the 33rd Annual IEEE Symposium on Foundations of Computer Science*, pages 137–146, 1992.

[35] Y. Azar, A.Z. Broder, A.R. Karlin, and E. Upfal. Balanced allocations. In *Proceedings of the 26th Annual ACM Symposium on Theory of Computing*, pages 593–602, 1994.

[36] K. Azuma. Weighted sums of certain dependent random variables. *Tohoku Mathematical Journal*, 19:357–367, 1967.

[37] L. Babai. Monte-Carlo algorithms in graph isomorphism testing. Technical Report DMS 79-10, Département de Mathématique et de Statistique, Université de Montréal, 1979.

[38] L. Babai. Trading group theory for randomness. In *Proceedings of the 17th Annual ACM Symposium on Theory of Computing*, pages 421–429, 1985.

[39] L. Babai. E-mail and the unexpected power of interaction. In *Proceedings of the 5th Annual Conference on Structure in Complexity Theory*, pages 30–44, 1990.

[40] L. Babai. Transparent (holographic) proofs. In *Proceedings 10th Annual Symposium on Theoretical Aspects of Computer Science*, pages 525–534, 1993.

[41] L. Babai and L. Fortnow. Arithmetization: a new method in structural complexity theory. *Computational Complexity*, 1:41–66, 1991.

[42] L. Babai, L. Fortnow, L. Levin, and M. Szegedy. Checking computations in polylogarithmic time. In *Proceedings of the 23rd Annual ACM Symposium on Theory of Computing*, pages 21–31, 1991.

[43] L. Babai, L. Fortnow, and C. Lund. Non-deterministic exponential time has two-prover interactive protocols. *Computational Complexity*, 1:3–40, 1991.

[44] E. Bach. Number-theoretic algorithms. *Annual Review of Computer Science*, 4:119–172, 1990.

[45] A. Bar-Noy, R. Motwani, and J. Naor. The greedy algorithm is optimal for on-line edge coloring. *Information Processing Letters*, 44:251–253, 1992.

[46] I. Bárány and Z. Füredi. Computing the volume is difficult. *Discrete and Computational Geometry*, 2:319–326, 1987.

[47] D. Beaver and J. Feigenbaum. Hiding instances in multioracle queries. In *Proceedings of the 7th Annual Symposium on Theoretical Aspects of Computer Science*, Lecture Notes in Computer Science, pages 37–48. Springer-Verlag, 1990.

[48] J. Beck. An algorithmic approach to the Lovász local lemma I. *Random Structures and Algorithms*, pages 343–365, 1991.

[49] L.A. Belady. A study of replacement algorithms for virtual storage computers. *IBM Systems Journal*, 5:78–101, 1966.

[50] M. Bellare and M. Sudan. Improved non-approximability results. In *Proceedings of the 26th Annual ACM Symposium on Theory of Computing*, pages 184–193, 1994.

[51] S. Ben-David, A. Borodin, R.M. Karp, G. Tardos, and A. Wigderson. On the power of randomization in on-line algorithms. *Algorithmica*, 11(1):2–14, 1994.

[52] M. Ben-Or. Probabilistic algorithms in finite fields. In *Proceedings of the 22nd Annual IEEE Symposium on Foundations of Computer Science*, pages 394–398, 1981.

[53] M. Ben-Or, S. Goldwasser, J. Kilian, and A. Wigderson. Multi-prover interactive proofs: How to remove intractability assumptions. In *Proceedings of the 20th Annual ACM Symposium on Theory of Computing*, pages 113–131, 1988.

[54] S.W. Bent and J.W. John. Finding the median requires $2n$ comparisons. In *Proceedings of the 17th ACM Annual Symposium on Theory of Computing*, pages 213–216, 1985.

[55] B. Berger and J. Rompel. Simulating $(\log^c n)$-wise independence in $calNC$. *Journal of the ACM*, 38:1026–1046, 1991.

[56] S.J. Berkowitz. On computing the determinant in small parallel time using a small number of processors. *Information Processing Letters*, 18:147–150, 1984.

[57] E. R. Berlekamp. Factoring polynomials over large finite fields. *Mathematics of Computation*, 24:713–735, 1970.

[58] D. Bertsimas and R. Vohra. Linear programming relaxations, approximation algorithms and randomization: a unified view of covering problems. Technical Report OR 285-94, MIT, 1994.

[59] F. Bien. Constructions of telephone networks by group representations. *Notices of the American Mathematical Society*, 36:5–22, 1989.

[60] N. Biggs. *Algebraic Graph Theory.* Cambridge University Press, 1974.

[61] P. Billingsley. *Probability and Measure.* John Wiley and Sons, New York, 1979.

[62] A. Blum, H.J. Karloff, Y. Rabani, and M. Saks. A decomposition theorem and bounds for randomized server problems. In *Proceedings of the 33rd Annual IEEE Symposium on Foundations of Computer Science*, pages 197–207, 1992.

[63] A. Blum, P. Raghavan, and B. Schieber. Navigating in unfamiliar geometric terrain. In *Proceedings of the 23rd Annual ACM Symposium on Theory of Computing*, pages 494–504, 1991.

[64] M. Blum, A.K. Chandra, and M.N. Wegman. Equivalence of free Boolean graphs can be decided probabilistically in polynomial time. *Information Processing Letters*, 10:80–82, 1980.

[65] M. Blum, R.W. Floyd, V. Pratt, R.L. Rivest, and R.E. Tarjan. Time bounds for selection. *Journal of Computer and System Sciences*, 7:448–461, 1973.

[66] M. Blum and S. Kannan. Designing programs that check their work. In *Proceedings of the 21st Annual ACM Symposium on Theory of Computing*, pages 86–97. ACM, 1989.

[67] M. Blum, R.M. Karp, O. Vornberger, C.H. Papadimitriou, and M. Yannakakis. The complexity of testing whether a graph is a superconcentrator. *Information Processing Letters*, 13:164–167, 1981.

[68] M. Blum, M. Luby, and R. Rubinfeld. Self-testing/correcting with applications to numerical problems. In *Proceedings of the 22nd Annual ACM Symposium on Theory of Computing*, pages 73–83, 1990.

[69] B. Bollobás. *Random Graphs.* Academic Press, 1985.

[70] B. Bollobás. The chromatic number of random graphs. *Combinatorica*, 8:49–55, 1988.

[71] J. A. Bondy and U.S. R. Murty. *Graph Theory With Applications.* American Elsevier, 1977.

[72] R.B. Boppana, J. Hastad, and S. Zachos. Does co-$\mathcal{NP}$ have short interactive proofs? *Information Processing Letters*, 25:127–133, 1987.

[73] R.B. Boppana and R. Hirschfeld. Pseudo-random generators and complexity classes. In S. Micali, editor, *Randomness and Computing (Advances in Computing Research, vol. 5)*, pages 1–26. JAI Press, 1989.

[74] A. Borodin, S. A. Cook, P. W. Dymond, W. L. Ruzzo, and M. Tompa. Two applications of inductive counting for complementation problems. *SIAM Journal on Computing*, 18(3):559–578, June 1989. See also 18(6): 1283, December 1989.

[75] A. Borodin and J. E. Hopcroft. Routing, merging, and sorting on parallel models of computation. *Journal of Computer and System Sciences*, 30:130–145, 1985.

[76] A. Borodin, N. Linial, and M. Saks. An optimal online algorithm for metrical task systems. *Journal of the ACM*, 39:745–763, 1992.

[77] A. Borodin, P. Raghavan, B. Schieber, and E. Upfal. How much can hardware help routing? In *Proceedings of the 25th Annual ACM Symposium on Theory of Computing*, pages 573–582, 1993.

[78] A. Borodin, W. L. Ruzzo, and M. Tompa. Lower bounds on the length of universal traversal sequences. *Journal of Computer and System Sciences*, 45(2):180–203, October 1992.

[79] A. Borodin, J. von zur Gathen, and J. E. Hopcroft. Fast parallel matrix and gcd computations. *Information and Computation*, 32:251–264, 1986.

[80] O. Borůvka . O jistém problému minimálním. *Práca Moravské Přírodovědecké Společnosti*, 3:37–58, 1926.

[81] D.P. Bovet and P. Crescenzi. *Introduction to the Theory of Complexity.* Prentice-Hall, New York, 1994.

[82] R. S. Boyer and J. S. Moore. A fast string searching algorithm. *Communications of the ACM*, 20(10), 1977.

[83] A.Z. Broder. How hard is it to marry at random? In *Proceedings of the 18th Annual ACM Symposium on Theory of Computing*, pages 50–58, May 1986.

[84] A.Z. Broder, A.M. Frieze, and E. Upfal. Existence and construction of edge disjoint paths on expander graphs. In *Proceedings of the 24th Annual ACM Symposium on Theory of Computing*, pages 140–149, 1992.

[85] A.Z. Broder and A.R. Karlin. Bounds on covering times. In *29th Annual Symposium on Foundations of Computer Science*, pages 479–487, White Plains, NY, October 1988.

[86] G. Buffon. Essai d'arithmétique morale. *Supplément à l'Histoire Naturelle*, 4, 1777.

[87] R. D. Carmichael. On composite numbers which satisfy the Fermat congruence. *Americal Mathematical Monthly*, 19:22–27, 1912.

[88] J.L. Carter and M.N. Wegman. Universal classes of hash functions. *Journal of Computer and System Sciences*, 18(2):143–154, 1979.

[89] A. K. Chandra, P. Raghavan, W.L. Ruzzo, R. Smolensky, and P. Tiwari. The electrical resistance of a graph captures its commute and cover times. In *Proceedings of the 21st Annual ACM Symposium on Theory of Computing*, pages 574–586, Seattle, May 1989.

[90] B. Chazelle and H. Edelsbrunner. An optimal algorithm for intersecting line segments in the plane. *Journal of the ACM*, 39:1–54, 1992.

[91] B. Chazelle and J. Friedman. A deterministic view of random sampling and its use in geometry. *Combinatorica*, 10(3):229–249, 1990.

[92] B. Chazelle and J. Friedman. Point location among hyperplanes and undirectional ray-shooting. *Computational Geometry: Theory and Applications*, 4:53–62, 1994.

[93] H. Chernoff. A measure of asymptotic efficiency for tests of a hypothesis based on the sum of observations. *Annals of Mathematical Statistics*, 23:493–509, 1952.

[94] L. P. Chew. Building Voronoi diagrams for convex polygons in linear expected time. Report, Deptartment of Mathematics and Computer Science, Dartmouth College, Hanover, NH, 1985.

[95] A.L. Chistov. Fast parallel calculation of the rank of matrices over a field of arbitrary characteristic. In *Proceedings of the International Conference on the Foundations of Computation Theory, Springer-Verlag Lecture Notes in Computer Science, 199*, pages 63–69, 1985.

[96] B. Chor and C. Dwork. Randomization in Byzantine agreement. In S. Micali, editor, *Randomness and Computing (Advances in Computing Research, vol. 5)*, pages 443–497. JAI Press, 1989.

[97] B. Chor and O. Goldreich. On the power of two-point sampling. *Journal of Complexity*, 5:96–106, 1989.

[98] M. Chrobak, H.J. Karloff, T. Payne, and S. Vishwanathan. New results on server problems. In *Proceedings of the 1st Annual ACM-SIAM Symposium on Discrete Algorithms*, pages 291–300, 1990.

[99] M. Chrobak and L.L. Larmore. HARMONIC is 3-competitive for 2 servers. *Theoretical Computer Science*, 98:339–346, May 1992.

[100] V. Chvátal. *Linear Programming.* W. H. Freeman, New York, NY, 1983.

[101] K. L. Clarkson. A probabilistic algorithm for the post office problem. In *Proceedings of the 17th Annual ACM Symposium on Theory of Computing*, pages 175–184, 1985.

[102] K. L. Clarkson. New applications of random sampling in computational geometry. *Discrete and Computational Geometry*, 2:195–222, 1987.

[103] K. L. Clarkson. Applications of random sampling in computational geometry, II. In *Proceedings of the 4th Annual ACM Symposium on Computational Geometry*, pages 1–11, 1988.

[104] K. L. Clarkson. A Las Vegas algorithm for linear programming when the dimension is small. In *Proceedings of the 29th Annual IEEE Symposium Foundations of Computer Science*, pages 452–456, 1988.

[105] K. L. Clarkson. A randomized algorithm for closest-point queries. *SIAM Journal on Computing*, 17:830–847, 1988.

[106] K. L. Clarkson and P. W. Shor. Algorithms for diametral pairs and convex hulls that are optimal, randomized, and incremental. In *Proceedings of the 4th Annual ACM Symposium on Computational Geometry*, pages 12–17, 1988.

[107] K. L. Clarkson and P. W. Shor. Applications of random sampling in computational geometry, II. *Discrete and Computational Geometry*, 4:387–421, 1989.

[108] A. Cohen and A. Wigderson. Dispersers, deterministic amplification, and weak random sources. In *Proceedings of the 30th Annual IEEE Symposium on Foundations of Computer Science*, pages 14–19, 1989.

[109] C.J. Colbourn. *The Combinatorics of Network Reliability.* Oxford University Press, New York, 1987.

[110] R. Cole. Parallel merge sort. *SIAM Journal on Computing*, 17(4):770–785, 1988.

[111] S. A. Cook. A taxonomy of problems with fast parallel algorithms. *Information and Control*, 64(1-3):2–22, 1985.

[112] D. Coppersmith, P. Doyle, P. Raghavan, and M. Snir. Random walks on weighted graphs, and applications to on-line algorithms. *Journal of the ACM*, 40:454–476, 1993.

[113] D. Coppersmith and S. Winograd. Matrix multiplication via arithmetic progressions. *Journal of Symbolic Computation*, 9:251–280, 1990.

[114] T. Cormen, C.E. Leiserson, and R.L. Rivest. *Introduction to algorithms.* MIT Press and Mc-Graw Hill, New York, 1990.

[115] L. Csanky. Fast parallel matrix inversion algorithms. *SIAM Journal on Computing*, 5:618–623, 1976.

[116] J.H. Curtiss. Monte Carlo method. *National Bureau of Standards Applied Mathematics Series*, 12, 1951.

[117] D.M. Cvetkovic, M. Doob, and H. Sachs. *Spectra of Graphs.* Academic Press, 1979.

[118] P. Dagum, M. Mihail, M. Luby, and U.V. Vazirani. Polytopes, permanents and graphs with large factors. In *Proceedings of the 29th Annual IEEE Symposium on Foundations of Computer Science*, pages 412–422, 1988.

[119] G.B. Dantzig. Minimization of a linear function of variables subject to linear inequalities. In T.C. Koopman, editor, *Activity Analysis of Production and Allocation*, pages 339–347. John Wiley, New York, 1951.

[120] G.B. Dantzig. *Linear Programming and Extensions.* Princeton University Press, Princeton, 1963.

[121] H. Davenport. *Multiplicative Number Theory.* Springer-Verlag, New York, 1980.

[122] K. de Leeuw, E.F. Moore, C.E. Shannon, and N. Shapirio. Computability by probabilistic machines. In C.E. Shannon and J. McCarthy, editors, *Automata Studies*, pages 183–212. Princeton University Press, Princeton, NJ, 1955.

[123] R.A. DeMillo and R.J. Lipton. A probabilistic remark on algebraic program testing. *Information Processing Letters*, 7:193–195, 1978.

[124] M. Dietzfelbinger, A. Karlin, K. Mehlhorn, F.Meyer auf der Heide, H. Rohnert, and R.E. Tarjan. Dynamic perfect hashing: Upper and lower bounds. In *29th Annual IEEE Symposium on Foundations of Computer Science*, pages 524–531, 1988.

[125] E.W. Dijkstra. A note on two problems in connection with graphs. *Numerische Mathematik*, 1:83–89, 1976.

[126] I.H. Dinwoodie. A probability inequality for the occupation measure of a reversible Markov chain. Unpublished manuscript, Department of Mathematics, Tulane University, 1994.

[127] B. Dixon, M. Rauch, and R. E. Tarjan. Verification and sensitivity analysis of minimum spanning trees in linear time. *SIAM Journal on Computing*, 21:1184–1192, 1992.

[128] W.E. Donath and A.J. Hoffman. Lower bounds for the partitioning of graphs. *IBM Journal of Research and Development*, 17:420–425, 1973.

[129] J.L. Doob. *Stochastic Processes.* John Wiley, New York, 1953.

[130] P.G. Doyle and J.L. Snell. *Random Walks and Electric Networks.* The Mathematical Association of America, 1984.

[131] D.R.Karger. Random sampling in matroids, with applications to graph connectivity and minimum spanning trees. In *Proceedings of the 34th Annual IEEE Symposium on Foundations of Computer Science*, pages 84–93, 1993.

[132] L.E. Dubins and L.J.Savage. *How to gamble if you must.* Mc-Graw Hill, New York, 1965.

[133] M. Dyer, A. Frieze, and R. Kannan. A random polynomial algorithm for approximating the volume of convex bodies. *Journal of the ACM*, pages 1–17, 1991.

[134] H. Edelsbrunner. *Algorithms in Combinatorial Geometry*, volume 10 of *EATCS Monographs on Theoretical Computer Science.* Springer-Verlag, Heidelberg, West Germany, 1987.

[135] J. Edmonds. Systems of distinct representatives and linear algebra. *Journal of Research of the National Bureau of Standards, 71B*, 4:241–245, 1967.

[136] R. El-Yaniv, A. Fiat, R.M. Karp, and G. Turpin. Competitive analysis of financial games. In *Proceedings of the 33rd Annual IEEE Symposium on Foundations of Computer Science*, pages 327–333, October 1992.

[137] P. Elias, A. Feinstein, and C. E. Shannon. Note on maximum flow through a network. *IRE Transactions on Information Theory*, IT-2:117–199, 1956.

[138] P. Erdös and L. Lovász. Problems and results on 3-chromatic hypergraphs and some related questions. In A. Hajnal et al., editor, *Infinite and Finite Sets*, pages 609–628. North-Holland, Amsterdam, 1975.

[139] P. Erdös and J.L. Selfridge. On a combinatorial game. *Journal of Combinatorial Theory, Series A*, 14:298–301, 1973.

[140] P. Erdös and J. Spencer. *The Probabilistic Method in Combinatorics*. Academic Press, San Diego, 1974.

[141] T. Feder and R. Motwani. Clique partitions, graph compression and speeding-up algorithms. In *Proceedings of the 25th Annual ACM Symposium on Theory of Computing*, pages 123–133, 1991.

[142] U. Feige, S. Goldwasser, L. Lovász, S. Safra, and M. Szegedy. Approximating clique is almost $\mathcal{NP}$-complete. In *Proceedings of the 32nd Annual Symposium on Foundations of Computer Science*, pages 2–12, 1991.

[143] W. Feller. *An Introduction to Probability Theory and Its Applications*, volume I. John Wiley, New York, NY, 1968.

[144] W. Feller. *An Introduction to Probability Theory and Its Applications*, volume II. John Wiley, New York, NY, 1968.

[145] A. Fiat, D.P. Foster, H.J. Karloff, Y. Rabani, Y. Ravid, and S. Vishwanathan. Competitive algorithms for layered graph traversal. In *Proceedings of the 32nd Annual IEEE Symposium on Foundations of Computer Science*, pages 288–297, 1991.

[146] A. Fiat, R. M. Karp, M. Luby, L. A. McGeoch, D. D. Sleator, and N. Young. Competitive paging algorithms. *Journal of Algorithms*, 12:685–699, 1991.

[147] A. Fiat, Y. Rabani, and Y. Ravid. Competitive k-server algorithms. In *Proceedings of the 31st Annual IEEE Symposium on Foundations of Computer Science*, pages 454–463, 1990.

[148] F.E. Fich, F. Meyer auf der Heide, P.L. Ragde, and A. Wigderson. One, two, three ... infinity: Lower bounds for parallel computation. In *Proceedings of the 17th Annual ACM Symposium on Theory of Computing*, pages 48–58, 1985.

[149] M.J. Fischer and N.A. Lynch. A lower bound for the time to assure interactive consistency. *Information Processing Letters*, 14:183–186, 1982.

[150] M.J. Fischer, N.A. Lynch, and M.S. Paterson. Impossibility of distributed consensus with one faulty process. *Journal of the ACM*, 32:374–382, 1985.

[151] R. W. Floyd. Algorithm 97: Shortest path. *Communications of the ACM*, 5:345, 1962.

[152] R. W. Floyd and R.L. Rivest. Expected time bounds for selection. *Communications of the ACM*, 18:165–172, 1975.

[153] L. R. Ford and D. R. Fulkerson. Maximal flow through a network. *Canadian Journal of Mathematics*, 8:399–404, 1956.

[154] L. Fortnow, J. Rompel, and M. Sipser. On the power of multi-prover interactive protocols. In *Proceedings of the 3rd Annual Conference on Structure in Complexity Theory*, pages 156–161, 1988.

[155] M. Fredman and D. E. Willard. Trans-dichotomous algorithms for minimum spanning trees and shortest paths. In *Proceedings of the 31st Annual IEEE Symposium on Foundations of Computer Science*, pages 719–725, 1990.

[156] M.L. Fredman and J. Komlòs. On the size of separating systems and families of perfect hash functions. *SIAM Journal on Computing*, 5:61–68, 1984.

[157] M.L. Fredman, J. Komlós, and E. Szemerédi. Storing a sparse table with O(1) worst case access time. *Journal of the ACM*, 31:538–544, July 1984.

[158] R. Freivalds. Probabilistic machines can use less running time. In B. Gilchrist, editor, *Information Processing 77, Proceedings of IFIP Congress 77*, pages 839–842, Amsterdam, August 1977. North-Holland Publishing Company.

[159] O. Gabber and Z. Galil. Explicit construction of linear-sized superconcentrators. *Journal of Computer and System Sciences*, 22:407–420, 1981.

[160] H. N. Gabow, Z. Galil, T. Spencer, and R. E. Tarjan. Efficient algorithms for finding minimum spanning trees in undirected and directed graphs. *Combinatorica*, 6:109–122, 1986.

[161] H. N. Gabow, Z. Galil, and T. H. Spencer. Efficient implementation of graph algorithms using contraction. In *Proceedings of the 25th Annual IEEE Symposium on Foundations of Computer Science*, pages 347–357, 1984.

[162] D. Gale and L. S. Shapley. College admissions and the stability of marriage. *American Mathematical Monthly*, 69:6–15, 1962.

[163] Z. Galil and V. Pan. Improved processor bounds for combinatorial problems in $\mathcal{RNC}$. *Combinatorica*, 8:189–200, 1988.

[164] B. Gärtner and G.M. Ziegler. Random simplex algorithms on Klee-Minty cubes. In *Proceedings of the 35th Annual IEEE Symposium on Foundations of Computer Science*, 1994.

[165] P. Gemmell, R. Lipton, R. Rubinfeld, M. Sudan, and A. Wigderson. Self-testing/correcting for polynomials and for approximate functions. In *Proceedings of the 23nd Annual ACM Symposium on Theory of Computing*, pages 32–42, 1991.

[166] J. Gill. Computational complexity of probabilistic Turing machines. *SIAM Journal on Computing*, 6(4):675–695, December 1977.

[167] D. Gillman. A Chernoff bound for random walks on expander graphs. In *34th Annual IEEE Symposium on Foundations of Computer Science*, pages 680–691, 1994.

[168] F. Göbel and A.A. Jagers. Random walks on graphs. *Stochastic Processes and their Applications*, 2:311–336, 1974.

[169] M. X. Goemans and D. P. Williamson. New 3/4-approximation algorithms for MAX SAT. To appear in the *SIAM Journal on Discrete Mathematics*, 1993.

[170] M.X. Goemans and D.P. Williamson. 0.878-approximation algorithms for MAX-CUT and MAX-2SAT. In *Proceedings of the 26th Annual ACM Symposium on Theory of Computing*, pages 422–431, 1994.

[171] A. V. Goldberg and R. E. Tarjan. A new approach to the maximum flow problem. *Journal of the ACM*, 35:921–940, 1988.

[172] A.V. Goldberg, S.A. Plotkin, and P.M. Vaidya. Sublinear-time parallel algorithms for matching and related problems. *Journal of Algorithms*, 14:180–213, 1993.

[173] M. Goldberg and T. Spencer. A new parallel algorithm for the maximal independent set problem. In *Proceedings of the 28th Annual Symposium on Foundations of Computer Science*, pages 161–165, 1987.

[174] O. Goldreich. A taxonomy of proof systems. 1. *SIGACT NEWS*, 24:2–13, 1993.

[175] O. Goldreich. A taxonomy of proof systems. 2. *SIGACT NEWS*, 25:22–30, 1994.

[176] O. Goldreich, S. Micali, and A. Wigderson. Proofs that yield nothing but their validity or all languages in $\mathcal{NP}$ have zero-knowledge proof systems. *JACM*, 38:691–729, 1991.

[177] M. Goldwasser. Linear programming in randomized subexponential time. Unpublished manuscript, Computer Science Department, Stanford University, 1993.

[178] S. Goldwasser and J. Kilian. Almost all primes can be quickly certified. In *Proceedings of the 18th Annual ACM Symposium on Theory of Computing*, pages 316–329, May 1986.

[179] S. Goldwasser, S. Micali, and C. Rackoff. The knowledge complexity of interactive proof-systems. *SIAMJC*, 18:186–208, 1989.

[180] R. E. Gomory and T. C. Hu. Multi-terminal network flows. *SIAM Journal*, 9:551–570, 1961.

[181] R. L. Graham and P. Hell. On the history of the minimum spanning tree problem. *Annals of the History of Computing*, 7:43–57, 1985.

[182] R.L. Graham, D.E. Knuth, and O. Patashnik. *Concrete Mathematics.* Addison-Wesley Publishing Company, Reading, MA, 1989.

[183] P. E. Green. *Fiber-Optic Communication Networks.* Prentice Hall, 1992.

[184] D.H. Greene and D.E. Knuth. *Mathematics for the Analysis of Algorithms.* Birkhäuser, Boston, 1990.

[185] D. Grigoriev and M. Karpinski. The matching problem for bipartite graphs with polynomially bounded permanents. In *Proceedings of the 28th Annual IEEE Symposium on Foundations of Computer Science*, pages 166–172, 1987.

[186] G. R. Grimmett and D. R. Stirzaker. *Probability and Random Processes.* Oxford University Press, Oxford, 1988.

[187] E. Grove. The harmonic online k-server algorithm is competitive. In *Proceedings of the 23rd Annual ACM Symposium on Theory of Computing*, pages 260–266, 1991.

[188] L. J. Guibas, D. E. Knuth, and M. Sharir. Randomized incremental construction of Delaunay and Voronoi diagrams. *Algorithmica*, 7:381–413, 1992.

[189] D. Gusfield and R. W. Irving. *The stable marriage problem: structure and algorithms.* MIT Press, Cambridge, 1989.

[190] T. Hagerup and C. Rüb. A guided tour of Chernoff bounds. *Information Processing Letters*, 33:305–308, 1990.

[191] A. Hall. On an experimental determination of π. *Messeng. Math.*, 2:113–114, 1873.

[192] P. Hall and C.C. Heyde. *Martingale limit theory and its application.* Academic Press, 1980.

[193] J. Hao and J. B. Orlin. A faster algorithm for finding the minimum cut in a graph. In *Proceedings of the 3rd Annual ACM-SIAM Symposium on Discrete Algorithms*, pages 165–174, 1993.

[194] F. Harary and E.M. Palmer. *Graphical Enumeration.* Academic Press, New York, 1973.

[195] G. H. Hardy and E. M. Wright. *An Introduction to the Theory of Numbers.* Oxford University Press, London, 1965. 4th Edition.

[196] G.H. Hardy, J. E. Littlewood, and G. Pólya. *Inequalities.* Cambridge University Press, Cambridge, 1989.

[197] J. Håstad, F.T. Leighton, and M. Newman. Reconfiguring a hypercube in the presence of faults. In *Proceedings of the 19th Annual ACM Symposium on Theory of Computing*, pages 274–284, 1987.

[198] D. Haussler and E. Welzl. Epsilon-nets and simplex range queries. *Discrete and Computational Geometry*, 2:127–151, 1987.

[199] R. Hayward and C.J.H. McDiarmid. Average case analysis of heap building by repeated insertion. *Journal of Algorithms*, 12:126–153, 1991.

[200] I. N. Herstein. *Topics in Algebra.* Wiley, 1964.

[201] C.A.R. Hoare. Algorithm 63 (Partition) and algorithm 65 (Find). *Communications of the ACM*, 4:321–322, 1961.

[202] C.A.R. Hoare. Quicksort. *Computer Journal*, 5:10–15, 1962.

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

[204] J.E. Hopcroft and R.M. Karp. An $n^{5/2}$ algorithm for maximum matching in bipartite graphs. *SIAM Journal on Computing*, 2:225–231, 1973.

[205] L. K. Hua. *Introduction to Number Theory.* Springer-Verlag, Berlin, 1982.

[206] R. Impagliazzo and D. Zuckerman. How to recycle random bits. In *Proceedings of the 30th Annual IEEE Symposium on Foundations of Computer Science*, pages 222–227, 1989.

[207] S.S. Irani. Two results on the list update problem. *Information Processing Letters*, 38:301–306, 1991.

[208] A. Israeli and Y. Shiloach. An improved parallel algorithm for maximal matching. *Information Processing Letters*, 22:57–60, 1986.

[209] J. JáJá. *An Introduction to Parallel Algorithms.* Addison-Wesley, Reading, MA, 1992.

[210] S. Janson. Large deviation inequalities for sums of indicator variables. Technical Report 34, Department of Mathematics, Uppsala University, 1993.

[211] M. Jerrum and U. Vazirani. A mildly exponential approximation algorithm for the permanent. In *Proceedings of the 33rd Annual IEEE Symposium on Foundations of Computer Science*, pages 320–326, 1992.

[212] M.R. Jerrum and A. Sinclair. Approximating the permanent. *SIAM Journal on Computing*, 18(6):1149–1178, December 1989.

[213] M.R. Jerrum, L.G. Valiant, and V.V. Vazirani. Random generation of combinatorial structures from a uniform distribution. *Theoretical Computer Science*, 43:169–188, 1986.

[214] Wang Jianhua. *The Theory of Games.* Clarendon Press, 1988.

[215] A. Joffe. On a set of almost deterministic k-independent random variables. *Annals of Probability*, 2(1):161–162, 1974.

[216] D. B. Johnson. Efficient algorithms for shortest paths in sparse networks. *Journal of the ACM*, 24:1–13, 1977.

[217] D. S. Johnson. Computing in the Math Department: Part I (The $\mathcal{NP}$-completeness column: An ongoing guide). *Journal of Algorithms*, 7:584–601, 1986.

[218] D. S. Johnson. Interactive proof systems for fun and profit (the $\mathcal{NP}$-Completeness column: An ongoing guide). *Journal of Algorithms*, 9:426–444, 1988.

[219] D. S. Johnson. The tale of the 2nd prover (the $\mathcal{NP}$-Completeness column: An ongoing guide). *Journal of Algorithms*, 13:502–524, 1992.

[220] D.S. Johnson. Approximation algorithms for combinatorial problems. *Journal of Computer and System Sciences*, 9:256–278, 1974.

[221] D.S. Johnson. The $\mathcal{NP}$-Completeness colunm: An ongoing guide. *Journal of Algorithms*, 5:284–299, 1984.

[222] D.S. Johnson. The $\mathcal{NP}$-Completeness colunm: An ongoing guide. *Journal of Algorithms*, 5:433–447, 1984.

[223] N.L. Johnson and S. Kotz. *Urn Models and Their Applications.* John Wiley, New York, 1977.

[224] L. R. Ford Jr. and D. R. Fulkerson. *Flows in networks.* Princeton University Press, Princeton, 1962.

[225] J. D. Kahn, N. Linial, N. Nisan, and M. E. Saks. On the cover time of random walks in graphs. *Journal of Theoretical Probability*, 2(1):121–128, 1989.

[226] C. Kaklamanis, D. Krizanc, and T. Tsantilas. Tight bounds for oblivious routing in the hypercube. In *Proceedings of the 3rd Annual ACM Symposium on Parallel Algorithms and Architectures*, pages 31–36, 1991.

[227] G. Kalai. A subexponential randomized simplex algorithm. In *Proceedings of the 24th Annual ACM Symposium on Theory of Computing*, pages 475–482, 1992.

[228] G. Kalai and D.J. Kleitman. A quasi-polynomial bound for the diameter of graphs of polyhedra. *Bulletin of the AMS*, 26:315–316, April 1992.

[229] A. Kamath, R. Motwani, K. Palem, and P. Sprirakis. Tail bounds for occupancy and the satisfiability threshold conjecture. In *Proceedings of the 35th Annual IEEE Symposium on Foundations of Computer Science*, 1994.

[230] D. Karger, R. Motwani, and M. Sudan. Approximate graph coloring by semidefinite programming. In *Proceedings of the 35th Annual IEEE Symposium on Foundations of Computer Science*, 1994.

[231] D.R. Karger. Global min-cuts in $\mathcal{RNC}$, and other ramifications of a simple min-cut algorithm. In *Proceedings of the 4th Annual ACM-SIAM Symposium on Discrete Algorithms*, 1993.

[232] D.R. Karger, P.N. Klein, and R.E. Tarjan. A randomized linear-time algorithm for finding minimum spanning trees. To appear in the Journal of the ACM, 1994.

[233] D.R. Karger and R. Motwani. Derandomization through approximation: An $\mathcal{NC}$ algorithm for minimum cuts. In *Proceedings of the 26th Annual ACM Symposium on Theory of Computing*, pages 497–506, 1994.

[234] D.R. Karger and C. Stein. An $O(n^2)$ algorithm for minimum cuts. In *Proceedings of the 25th Annual ACM Symposium on Theory of Computing*, pages 757–765, 1993.

[235] A. R. Karlin, M. S. Manasse, L. Rudolph, and D.D. Sleator. Competitive snoopy caching. *Algorithmica*, 3(1):70–119, 1988.

[236] A.R. Karlin, M.S. Manasse, L.A. McGeoch, and S. Owicki. Competitive randomized algorithms for non-uniform problems. In *Proceedings of the 1st ACM-SIAM Symposium on Discrete Algorithms*, pages 301–309, 1990.

[237] H.J. Karloff. A Las Vegas $\mathcal{RNC}$ algorithm for maximum matching. *Combinatorica*, 6:387–391, 1986.

[238] H.J. Karloff, Y. Rabani, and Y. Ravid. Lower bounds for randomized server algorithms. In *Proceedings of the 23rd Annual ACM Symposium on Theory of Computing*, pages 278–288, 1991.

[239] N. Karmarkar, R.M. Karp, R. Lipton, L. Lovász, and M. Luby. A Monte Carlo algorithm for estimating the permanent. In preparation.

[240] R. M. Karp, M. Luby, and N. Madras. Monte-Carlo approximation algorithms for enumeration problems. *Journal of Algorithms*, 10:429–448, 1989.

[241] R. M. Karp and V. Ramachandran. Parallel algorithms for shared memory machines. In J. van Leeuwen, editor, *Handbook of Theoretical Computer Science*, pages 869–941. Elsevier/The MIT Press, Amsterdam, 1990.

[242] R. M. Karp, E. Upfal, and A. Wigderson. Constructing a perfect matching is in random $\mathcal{NC}$. *Combinatorica*, 6:35–48, 1986.

[243] R.M. Karp. An introduction to randomized algorithms. *Discrete Applied Mathematics*, 34:165–201, 1991.

[244] R.M. Karp. Probabilistic recurrence relations. In *Proceedings of the 23rd Annual ACM Symposium on Theory of Computing*, pages 190–197, 1991.

[245] R.M. Karp and R. Lipton. Turing machines that take advice. *L'enseignment Mathematique*, 28:191–209, 1982.

[246] R.M. Karp and M. Luby. Monte-Carlo algorithms for enumeration and reliability problems. In *Proceedings of the 24th Annual IEEE Symposium on Foundations of Computer Science*, pages 56–64, 1983.

[247] R.M. Karp and M. Luby. Monte Carlo algorithms for the planar multiterminal network reliability problem. *Journal of Complexity*, 1:45–64, 1985.

[248] R.M. Karp, N. Pippenger, and M. Sipser. A time randomness tradeoff. In *AMS Conference on Probabilistic Computational Complexity*, 1985.

[249] R.M. Karp and M.O. Rabin. Efficient randomized pattern-matching algorithms. *IBM Journal of Research and Development*, 31:249–260, March 1987.

[250] R.M. Karp, E. Upfal, and A. Wigderson. The complexity of parallel search. *Journal of Computer and System Sciences*, 36:225–253, 1988.

[251] R.M. Karp and A. Wigderson. A fast parallel algorithm for the maximal independent set problem. *Journal of the ACM*, 32:762–773, 1985.

[252] A. V. Karzanov and E. A. Timofeev. Efficient algorithm for finding all minimal edge cuts of a non-oriented graph. *Kibernetika*, 22:156–162, 1986. Translation in *Cybernetics 22*.

[253] J.G. Kemeny, J. L. Snell, and A.W. Knapp. *Denumerable Markov Chains*. The University Series in Higher Mathematics. Van Nostrand, Princeton, NJ, 1966.

[254] T. Kimbrel and R. Sinha. A probabilistic algorithm for verifying matrix products using $O(n^2)$ time and $\log_2 n + O(1)$ random bits. *Information Processing Letters*, 45:107–110, 1993.

[255] V. King. A simpler minimum spanning tree verification algorithm. Unpublished manuscript, 1993.

[256] V. King, S. Rao, and R.E.Tarjan. A faster deterministic maximum flow algorithm. In *Proceedings of the 3rd Annual ACM-SIAM Symposium on Discrete Algorithms*, pages 157–164, 1993.

[257] P.N. Klein and R.E. Tarjan. A randomized linear-time algorithm for finding minimum spanning trees. In *Proceedings of the 26th Annual ACM Symposium on Theory of Computing*, pages 9–15, 1994.

[258] D. E. Knuth. *Fundamental Algorithms*, volume 1 of *The Art of Computer Programming*. Addison-Wesley, Reading, MA, 1969.

[259] D. E. Knuth. *Seminumerical Algorithms*, volume 2 of *The Art of Computer Programming*. Addison-Wesley, Reading, MA, 1971.

[260] D. E. Knuth. *Sorting and Searching*, volume 3 of *The Art of Computer Programming*. Addison-Wesley, Reading, MA, 1973.

[261] D. E. Knuth. Big omicron and big omega and big theta. *SIGACT News*, 8(2):18–24, 1976.

[262] D. E. Knuth, J. H. Morris, Jr., and V. R. Pratt. Fast pattern matching in strings. *SIAM Journal on Computing*, 6(2):240–267, 1977.

[263] D.E. Knuth. *Mariages stables* (in French). Les Presses de l'Université de Montréal, Montreal, 1976.

[264] D.E. Knuth and A. C-C. Yao. The complexity of nonuniform random number generation. In J. F. Traub, editor, *Algorithms and Complexity, Recent Results and New Directions*, pages 375–428. Academic Press, New York, 1976.

[265] K-I. Ko. Some observations on probabilistic algorithms and $\mathcal{NP}$-hard problems. *Information Processing Letters*, 14:39–43, 1981.

[266] V.F. Kolchin, V.P. Chistiakov, and B.A. Sevastianov. *Random Allocations*. V.H. Winston, New York, 1978.

[267] A. Kolmogorov. *Grundbegriffe der Wahrscheinlichkeitsrechnung*. Springer, 1933.

[268] J. Komlós. Linear verification for spanning trees. *Combinatorica*, 5:57–65, 1985.

[269] E. Koutsoupias and C.H. Papadimitriou. On the k-server conjecture. In *Proceedings of the 26th Annual ACM Symposium on Theory of Computing*, pages 507–511, 1994.

[270] J. B. Kruskal. On the shortest spanning subtree of a graph and the traveling salesman problem. *Proceedings of the American Mathematical Society*, 7:48–50, 1956.

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

[272] F.T. Leighton, B. Maggs, and S. Rao. Universal packet routing algorithms. In *Proceedings of the 29th Annual IEEE Symposium on Foundations of Computer Science*, pages 256–269, 1988.

[273] A. K. Lenstra and Jr. H. W. Lenstra. Algorithms in number theory. In J. van Leeuwen, editor, *Handbook of Theoretical Computer Science*, pages 675–715. Elsevier Science Publishers, 1990.

[274] A. Lev, N. Pippenger, and L.G. Valiant. A fast parallel algorithm for routing in permutation networks. *IEEE Transactions on Computers*, C-30:93–100, 1981.

[275] W.J. LeVeque. *Fundamentals of Number Theory*. Addison-Wesley, Reading, MA, 1977.

[276] H. R. Lewis and C. H. Papadimitriou. Symmetric space-bounded computation. *Theoretical Computer Science*, 19:161–187, 1982.

[277] R.J. Lipton. New directions in testing. In *Distributed Computing and Cryptography*, DIMACS Series in Discrete Mathematics and Theoretical Computer Science, Volume 2, pages 191–202. American Mathematical Society, Providence, 1991.

[278] R.J. Lipton and N. Young. Simple strategies for large zero-sum games with applications to complexity theory. In *Proceedings of the 26th Annual ACM Symposium on Theory of Computing*, pages 734–740, 1994.

[279] L.H. Loomis. On a theorem of von Neumann. *Proceedings of the National Academy of Sciences of the U.S.A.*, 32:213–215, 1946.

[280] L. Lovász. On determinants, matchings and random algorithms. In L. Budach, editor, *Fundamentals of Computing Theory*. Akademia-Verlag, Berlin, 1979.

[281] L. Lovász and M.D. Plummer. *Matching Theory*. Academic Press, 1986.

[282] M. Luby. A simple parallel algorithm for the maximal independent set. *SIAM Journal on Computing*, 15:1036–1053, 1986.

[283] M. Luby. Removing randomness in parallel computation without a processor penalty. In *Proceedings 29th Annual IEEE Symposium on Foundations of Computer Science*, pages 162–173, October 1988.

[284] M. Luby. Removing randomness in parallel computation without a processor penalty. *Journal of Computer and System Sciences*, 47:250–86, 1993.

[285] M. Luby, J. Naor, and M. Naor. On removing randomness from a parallel algorithm for minimum cuts. Technical Report TR-093-007, International Computer Science Institute, Berkeley, 1993.

[286] M. Luby, A. Sinclair, and D. Zuckerman. Optimal speedup of Las Vegas algorithms. *Information Processing Letters*, 47:173–180, 1993.

[287] R. Luce and H. Raiffa. *Games and Decisions.* John Wiley, New York, 1957.

[288] C. Lund, L. Fortnow, H.J. Karloff, and N. Nisan. Algebraic methods for interactive proof systems. In *Proceedings of the 31st Annual IEEE Symposium on Foundations of Computer Science*, pages 2–10, 1990.

[289] F. Maffioli, M.G. Speranza, and C. Vercellis. Randomized algorithms. In M. O'hEigertaigh, J.K. Lenstra, and A.H.G. Rinooy Kan, editors, *Combinatorial Optimization: Annotated Bibliographies*, pages 89–105. John Wiley and Sons, New York, 1985.

[290] M.S. Manasse, L.A. McGeoch, and D.D. Sleator. Competitive algorithms for server problems. *Journal of Algorithms*, 11:208–230, 1990.

[291] K. Manders and L. Adleman. $\mathcal{NP}$-complete decision problems for quadratic polynomials. In *Proceedings of the 8th ACM Symposium on Theory of Computing*, pages 23–29, 1976.

[292] G.A. Margulis. Explicit constructions of concentrators. *Problemy Peredachi Informatsii*, pages 71–80, 1973. English translation in *Problems of Information Transmisiion*, 9 325–332.

[293] A.A. Markov. *Ischislenie veroi͡atnosteĭ, 2 ed.* 1912.

[294] J. Matoušek. Derandomization in computational geometry. Submitted for publication., 1994.

[295] J. Matoušek, M. Sharir, and E. Welzl. A subexponential bound for linear programming. In *Proceedings of the 8th Annual ACM Symposium on Computational Geometry*, pages 1–8, 1992.

[296] P.C. Matthews. Covering problems for Brownian motion on spheres. *Annals of Probability*, 16:189–199, 1988.

[297] P.C. Matthews. Covering problems for Markov chains. *Annals of Probability*, 16:1215–1228, 1988.

[298] R.L. Mattison, J. Gecsei, D.R. Slutz, and I.L. Traiger. Evaluation techniques for storage hierarchies. *IBM Systems Journal*, 9(2), 1990.

[299] D. W. Matula. Determining edge connectivity in O(nm). In *Proceedings of the 28th Annual IEEE Symposium on Foundations of Computer Science*, pages 249–251, 1987.

[300] B. Maurey. Construction de suites symétriques. *Compt. Rend. Acad. Sci. Paris*, 288:679–681, 1979.

[301] J. C. Maxwell. *A Treatise on Electricity and Magnetism.* Clarendon, 1918.

[302] C.J.H. McDiarmid. On the method of bounded differences. In J. Siemons, editor, *Surveys in Combinatorics: Invited Papers at the 12th British Combinatorial Conference*, pages 148–188. Cambridge University Press, 1989.

[303] C.J.H. McDiarmid. On a random recolouring method for graphs and hypergraphs. *Combinatorics, Probability and Computing*, 2:363–365, 1993.

[304] C.J.H. McDiarmid and R. Hayward. Strong concentration for quicksort. In *Proceedings of the 3rd Annual ACM-SIAM Symposium on Discrete Algorithms*, pages 414–421, 1992.

[305] C.J.H. McDiarmid and B.A. Reed. Building heaps fast (data structures). *Journal of Algorithms*, 10:352–365, 1989.

[306] L.A. McGeoch and D.D. Sleator. A strongly competitive randomized paging algorithm. *Algorithmica*, 6:816–825, 1991.

[307] N. Megiddo. Linear programming in linear time when the dimension is fixed. *Journal of the ACM*, 31:114–127, 1984.

[308] S. Micali and V.V. Vazirani. An $O(\sqrt{|V|}|e|)$ algorithm for finding maximum matching in general graphs. In *Proceedings of the 21st Annual IEEE Symposium on Foundations of Computer Science*, pages 17–27, 1980.

[309] M. Mihail. The approximation of the permanent is still open. Manuscript, Harvard University, 1987.

[310] G.L. Miller. Riemann's hypothesis and tests for primality. *Journal of Computer and System Sciences*, 13:300–317, 1976.

[311] D. S. Mitrinović. *Analytic Inequalities*. Springer-Verlag, New York, 1970.

[312] R. Motwani. Expanding graphs and the average-case analysis of algorithms for matchings and related problems. In *Proceedings of the 21st Annual ACM Symposium on Theory of Computing*, pages 550–561, 1989.

[313] R. Motwani, J. Naor, and M. Naor. The probabilistic method yields deterministic parallel algorithms. In *Proceedings of the 30th Annual IEEE Symposium on Foundations of Computer Science*, pages 8–13, October 1989.

[314] R. Motwani, J. Naor, and P. Raghavan. Randomization in approximation algorithms. In D. Hochbaum, editor, *Approximation Algorithms*. To Appear, 1995.

[315] K. Mulmuley. A fast planar partition algorithm, I. In *Proceedings 29th IEEE Symposium on Foundations of Computer Science*, pages 580–589, October 1988.

[316] K. Mulmuley. A fast planar partition algorithm, I. In *Proceedings of the 29th Annual IEEE Symposium on Foundations of Computer Science*, pages 580–589, 1988.

[317] K. Mulmuley. *Computational Geometry: An Introduction Through Randomized Algorithms*. Prentice Hall, New York, 1993.

[318] K. Mulmuley, U.V. Vazirani, and V.V. Vazirani. Matching is as easy as matrix inversion. *Combinatorica*, 7:105–113, 1987.

[319] H. Nagamochi and T. Ibaraki. Computing edge connectivity in multigraphs and capacitated graphs. *SIAM Journal on Discrete Mathematics*, 5:54–66, 1992.

[320] J. Naor and M. Naor. Small-bias probability spaces: efficient constructions and applications. *SIAM Journal on Computing*, 22:838–56, 1993.

[321] N. Nisan. Pseudorandom generators for space-bounded computation. *Combinatorica*, 12:449–461, 1992.

[322] I. Niven and H. S. Zuckerman. *An Introduction to the Theory of Numbers*. John Wiley & Sons, 1960.

[323] V. Pan. How to multiply matrices faster. In *Springer-Verlag Lecture Notes in Computer Science 179*. Springer Verlag, New York, 1984.

[324] V. Pan. Fast and efficient algorithms for the exact inversion of integer matrices. In *Proceedings of the Fifth Annual Conference on the Foundations of Software Technology and Theoretical Computer Science*. Springer-Verlag LNCS 206, 1985.

[325] C.H. Papadimitriou. Games against nature. *Journal of Computer and System Sciences*, 31:288–301, 1985.

[326] C.H. Papadimitriou. On selecting a satisfying truth assignment. In *Proceedings of the 32nd Annual IEEE Symposium on Foundations of Computer Science*, pages 163–169, 1991.

[327] C.H. Papadimitriou. *Complexity Theory*. Addison-Wesley, Reading, MA, 1994.

[328] C.H. Papadimitriou and M. Yanakakis. Shortest paths without a map. *Theoretical Computer Science*, 84:127–150, 1991.

[329] M.S. Paterson. Improved sorting networks with $o(\log n)$ depth. *Algorithmica*, 5:75–92, 1990.

[330] M.S. Paterson and F.F. Yao. Efficient binary space partitions for hidden surface removal and solid modeling. *Discrete and Computational Geometry*, 5:485–503, 1990.

[331] M. Pease, R. Shostak, and L. Lamport. Reaching agreement in the presence of faults. *Journal of the ACM*, 27:228–234, 1980.

[332] D. Peleg and E. Upfal. A time-randomness tradeoff for oblivious routing. *SIAM Journal on Computing*, 19:256–266, 1990.

[333] S. Phillips and J. Westbrook. Online load balancing and network flow. In *Proceedings of the 25th Annual ACM Symposium on Theory of Computing*, pages 402–411, 1991.

[334] M. Pinsker. On the complexity of a concentrator. In *7th International Teletraffic Conference*, pages 318/1–318/4, 1973.

[335] V. D. Podderyugin. An algorithm for finding the edge connectivity of graphs. *Vopr. Kibernetika*, 2:136, 1973.

[336] V. Pratt. Every prime has a succinct certificate. *SIAM Journal on Computing*, 4:214–220, 1975.

[337] F. P. Preparata and M. I. Shamos. *Computational Geometry: an Introduction*. Springer-Verlag, New York, NY, 1985.

[338] R.C. Prim. Shortest connection networks and some generalizations. *Bell Systems Technical Journal*, 36:1389–1401, 1957.

[339] K. Pruhs and U. Manber. The complexity of controlled selection. *Information and Computation*, 91:103–127, 1991.

[340] W. Pugh. Skip lists: A probabilistic alternative to balanced trees. *Communications of the ACM*, 33(6):668–676, 1990.

[341] M. O. Rabin. Probabilistic automata. *Information and Control*, 6:230–245, 1963.

[342] M. O. Rabin. Probabilistic algorithms. In J. F. Traub, editor, *Algorithms and Complexity, Recent Results and New Directions*, pages 21–39. Academic Press, New York, 1976.

[343] M. O. Rabin. Probabilistic algorithm for testing primality. *Journal of Number Theory*, 12:128–138, 1980.

[344] M. O. Rabin. Probabilistic algorithms in finite fields. *SIAM Journal on Computing*, 9:273–280, 1980.

[345] M. O. Rabin. The choice coordination problem. *Acta Informatica*, 17:121–134, 1982.

[346] M. O. Rabin and J. O. Shallit. Randomized algorithms in number theory. *Communications in Pure and Applied Mathematics*, 39:239–256, 1986.

[347] M.O. Rabin. Digitalized signatures and public-key functions as intractable as factorization. Technical Report MIT/LCS/TR-212, M.I.T., January 1979.

[348] M.O. Rabin. Randomized Byzantine generals. In *Proceedings of the 24th Annual Symposium on Foundations of Computer Science*, pages 403–409, 1983.

[349] M.O. Rabin and V.V. Vazirani. Maximum matchings in general graphs through randomization. Technical Report TR-15-84, Aiken Computation Laboratory, Harvard University, 1984.

[350] M.O. Rabin and V.V. Vazirani. Maximum matchings in general graphs through randomization. *Journal of Algorithms*, 10:557–567, 1989.

[351] P. Raghavan. *Randomized Rounding and Discrete Ham-Sandwich Theorems*. PhD thesis, University of California, Berkeley, July 1986.

[352] P. Raghavan. Probabilistic construction of deterministic algorithms: Approximating packing integer programs. *Journal of Computer and System Sciences*, 37:130–143, October 1988.

[353] P. Raghavan and M. Snir. Memory versus randomization in on-line algorithms. In *16th International Colloquium on Automata, Languages, and Programming*, volume 372 of *Lecture Notes in Computer Science*, pages 687–703. Springer-Verlag, July 1989. Revised version to appear in the IBM Journal of Research and Development, 1995.

[354] P. Raghavan and C.D. Thompson. Randomized rounding. *Combinatorica*, 7:365–374, 1987.

[355] J.H. Reif. *Synthesis of Parallel Algorithms*. Morgan-Kauffman Publishers, 1993.

[356] N. Reingold, D.D. Sleator, and J. Westbrook. Randomized competitive algorithms for the list update problem. *Algorithmica*, 11(1):15–32, 1994.

[357] R. Reischuk. Probabilistic parallel algorithms for sorting and selection. *SIAM Journal on Computing*, 14(2):396–409, 1985.

[358] A. Rényi. *Probability Theory*. North-Holland, Amsterdam, 1970.

[359] R. L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21:120–126, 1978.

[360] F. Romani. Shortest-path problem is not harder than matrix multiplication. *Information Processing Letters*, 11:134–136, 1980.

[361] R. Rubinfeld. *A Mathematical Theory of Self-Checking, Self-Testing and Self-Correcting Programs*. PhD thesis, Computer Science Department, University of California, Berkeley, 1990.

[362] H. Ryser. *Combinatorial Mathematics*. The Mathematical Association of America, 1963.

[363] M. Saks and A. Wigderson. Probabilistic Boolean decision trees and the complexity of evaluating game trees. In *Proceedings of the 27th Annual IEEE Symposium on Foundations of Computer Science*, pages 29–38, Toronto, Ontario, 1986.

[364] J.P. Schmidt, A. Siegel, and A. Srinivasan. Chernoff-Hoeffding bounds for applications with limited independence. In *Proceedings of the 4th Annual ACM-SIAM Symposium on Discrete Algorithms*, pages 331–340, 1993.

[365] A. Schönhage, M. Paterson, and N. Pippenger. Finding the median. *Journal of Computer and System Sciences*, 13:184–199, 1976.

[366] U. Schöning. Graph isomorphism is in the low hierarchy. *Journal of Computer and System Sciences*, 37:312–323, 1988.

[367] A. Schrijver. *Theory of Linear and Integer Programming*. John Wiley, New York, 1986.

[368] J. T. Schwartz. Fast probabilistic algorithms for verification of polynomial identities. *Journal of the ACM*, 27(4):701–717, October 1980.

[369] R.G. Seidel. A simple and fast incremental randomized algorithm for computing trapezoidal decompositions and for triangulating polygons. *Computational Geometry: Theory and Applications*, 1:51–64, 1991.

[370] R.G. Seidel. Small-dimensional linear programming and convex hulls made easy. *Discrete and Computational Geometry*, 6:423–434, 1991.

[371] R.G. Seidel. On the all-pairs-shortest-path problem. In *Proceedings of the 24th Annual ACM Symposium on Theory of Computing*, pages 745–749, 1992.

[372] R.G. Seidel. Backwards analysis of randomized geometric algorithms. In J. Pach, editor, *New Trends in Discrete and Computational Geometry*, volume 10 of *Algorithms and Combinatorics*, pages 37–68. Springer-Verlag, 1993.

[373] A. Shamir. $\mathcal{IP} = \mathcal{PSPACE}$. *JACM*, 39:869–877, 1992.

[374] E. Shamir and J. Spencer. Sharp concentration of the chromatic number on random graphs $g_{n,p}$. *Combinatorica*, 7:121–129, 1987.

[375] M. Sharir and E. Welzl. A combinatorial bound for linear programming and related problems. In *Proceedings of the 9th Symposium on Theoretical Aspects of Computer Science*, volume 577 of *Lecture Notes in Computer Science*, pages 569–579. Springer-Verlag, 1992.

[376] A. Sinclair. *Algorithms for Random Generation and Counting: A Markov Chain Approach.* Progress in Theoretical Computer Science. Birkhauser, Boston, 1992.

[377] A. Sinclair and M.R. Jerrum. Approximate counting, uniform generation and rapidly mixing Markov chains. *Information and Computation*, 82:93–133, 1989.

[378] A. J. Sinclair. Improved bounds for mixing rates of Markov chains and multicommodity flow. *Combinatorics, Probability and Computing*, 1:351–370, 1992.

[379] M. Sipser. Expanders, randomness or time versus space. In *Proceedings of the ???th Structure in Complexity Theory Conference*, page 325, 1986.

[380] D.D. Sleator and R.E. Tarjan. Amortized efficiency of list update and paging rules. *Communications of the ACM*, 28:202–208, February 1985.

[381] D.D. Sleator and R.E. Tarjan. Self-adjusting binary search trees. *Journal of the ACM*, 32:652–686, July 1985.

[382] M. Snir. Lower bounds on probabilistic linear decision trees. *Theoretical Computer Science*, 38:69–82, 1985.

[383] R. Solovay and V. Strassen. A fast Monte-Carlo test for primality. *SIAM Journal on Computing*, 6(1):84–85, March 1977. See also *SIAM Journal on Computing 7*, 1 February 1978), 118.

[384] J. Spencer. Six standard deviations suffice. *Transactions of the American Mathematical Society*, 289(2):679–706, June 1985.

[385] J. Spencer. *Ten Lectures on the Probabilistic Method.* SIAM, 1987.

[386] R. Sprugnoli. Perfect hashing functions: A single probe retrieving method for static sets. *Communications of the ACM*, 21(11):606–611, 1979.

[387] L.J. Stockmeyer. On approximation algorithms for $\#\mathcal{P}$. *SIAM Journal on Computing*, 14:849–861, 1985.

[388] G. Strang. *Linear Algebra and Its Applications.* Harcourt Brace Jovanovich, San Diego, CA, 1988.

[389] M. Sudan. *Efficient Checking of Polynomials and Proofs and the Hardness of Approximation Problems.* PhD thesis, University of California at Berkeley, 1992.

[390] R.M. Tanner. Explicit construction of concentrators from generalized n-gons. *SIAM Journal on Algebraic and Discrete Methods*, 5:287–293, 1984.

[391] R. E. Tarjan. Applications of path compression on balanced trees. *Journal of the ACM*, 26:690–715, 1979.

[392] R.E. Tarjan. *Data Structures and Network Algorithms.* CBMS-NSF Regional Conference Series in Applied Mathematics. SIAM, Philadelphia, 1983.

[393] R.E. Tarjan and A. Yao. Storing a sparse table. *Communications of the ACM*, 22:606–611, 1979.

[394] M. Tarsi. Optimal search on some game trees. *Journal of the ACM*, 30:389–396, 1983.

[395] P.-L. Tchébyshef. Des valeurs moyennes. *Journal de Mathématiques pures et appliquées, ser. 2*, 12:177–184, 1867.

[396] B. Teia. A lower bound for randomized list update algorithms. *Information Processing Letters*, 47:5–9, 1993.

[397] P. Tetali. Random walks and the effective resistance of networks. *Journal of Theoretical Probability*, pages 101–109, 1991.

[398] A. Treat. Experimental control of ear choice in the moth ear mite. *XI. Internationaler Kongress für Entomologie*, pages 619–621, 1960.

[399] W.T. Tutte. The factorization of linear graphs. *J. of the London Math. Soc.*, 22:107–111, 1947.

[400] E. Upfal. Efficient schemes for parallel communication. *Journal of the ACM*, 31:507–517, 1984.

[401] L. G. Valiant and G. J. Brebner. Universal schemes for parallel communication. In *Proceedings of the 13th Annual ACM Symposium on Theory of Computing*, pages 263–277, Milwaukee, Wisconsin, May 1981.

[402] L.G. Valiant. The complexity of computing the permanent. *Theoretical Computer Science*, 8:189–201, 1979.

[403] L.G. Valiant. The complexity of enumeration and reliability problems. *SIAM Journal on Computing*, 8:410–421, 1979.

[404] L.G. Valiant. A scheme for fast parallel communication. *SIAM Journal on Computing*, 11:350–361, 1982.

[405] B. L. van der Waerden. *Algebra.* Ungar, 1970.

[406] V.V. Vazirani. Parallel graph matching. In J.H. Reif, editor, *Synthesis of Parallel Algorithms*, pages 783–811. Morgan-Kauffman Publishers, 1993.

[407] V.V. Vazirani. A theory of alternating paths and blossoms for proving correctness of $\mathrm{O}\sqrt{V}e$ graph maximum matching algorithms. *Combinatorica*, 14(1):71–109, 1994.

[408] I. M. Vinogradov. *Elements of Number Theory.* Dover, 1954.

[409] J. von Neumann. Zur Theorie der Gesellschaftsspiele. *Mathematische Annalen*, 100:295–320, 1928.

[410] J. von Neumann. Various techniques used in connection with random digits (notes by G.E. Forsythe). *National Bureau of Standards, Applied Math. Series*, 12:36–38, 1951.

[411] J. von Neumann. *Collected Works*, volume 5. Pergamon Press, 1963.

[412] J. von Neumann and O. Morgenstern. *Theory of Games and Economic Behavior.* Princeton University Press, Princeton, NJ, 1953.

[413] J. von zur Gathen. Parallel linear algebra. In J.H. Reif, editor, *Synthesis of Parallel Algorithms*, pages 573–617. Morgan-Kauffman Publishers, 1993.

[414] S. Warshall. A theorem on Boolean matrices. *Journal of the ACM*, 9:11–12, 1962.

[415] M.N. Wegman and J.L. Carter. New hash functions and their use in authentication and set equality. *Journal of Computer and System Sciences*, 22(3):265–279, 1981.

[416] D. J. A. Welsh. Randomised algorithms. *Discrete Applied Mathematics*, 5:133–145, 1983.

[417] D.J.A. Welsh. *Complexity: Knots, Colourings and Counting.* Cambridge University Press, Cambridge, UK, 1994.

[418] E. Welzl. Partition trees for triangle counting and other range searching problems. In *Proceedings of the 4th Annual ACM Symposium on Computational Geometry*, pages 23–33, 1988.

[419] M. Yannakakis. On the approximation of maximum satisfiability. In *Proceedings of the 3rd ACM-SIAM Symposium on Discrete Algorithms*, pages 1–9, 1992.

[420] A. C-C. Yao. Probabilistic computations: Towards a unified measure of complexity. In *Proceedings of the 17th Annual Symposium on Foundations of Computer Science*, pages 222–227, 1977.

[421] A.C.-C. Yao. Should tables be sorted? *Journal of the ACM*, 28(3):615–628, 1981.

[422] G. Yuval. An algorithm for finding all shortest paths using $n^{2.81}$ infinite-precision multiplications. *Information Processing Letters*, 4:155–156, 1976.

[423] R.E. Zippel. Probabilistic algorithms for sparse polynomials. In *Proceedings of EUROSAM 79*, volume 72 of *Lecture Notes in Computer Science*, pages 216–226, Marseille, 1979.

[424] R.E. Zippel. *Efficient Polynomial Computations.* Kluwer Academic Publishers, Boston, 1993.

[425] D. Zuckerman. Simulating $\mathcal{BPP}$ using a general weak random source. In *Proceedings of the 32nd Annual Symposium on Foundations of Computer Science*, pages 79–89, 1991.