References

[1] I. Abraham, Y. Bartal, and O. Neiman. Advances in metric embedding theory. In *STOC*, 2006.

[2] M. Adams and V. Guillemin. *Measure Theory and Probability*. Birkhäuser, 1996.

[3] R. Ahlswede and D. E. Daykin. An inequality for the weights of two families of sets, their unions and intersections. *Z. Wahrscheinl. V. Geb*, 43:183–185, 1978.

[4] M. Ajtai, V. Chvátal, M. Newborn, and E. Szemerédi. Crossing-free subgraphs. *Annals of Discrete Mathematics*, 12:9–12, 1982.

[5] M. Artin. *Algebra*. Prentice-Hall, 1991.

[6] Y. Azar, A. Broder, A. Karlin, and E. Upfal. Balanced allocations. *SIAM J. Comput.*, 29(1):180–200, 1999.

[7] B. Berger. The fourth moment method. *SIAM J. Comput.*, 26(4):1188–1207, 1997.

[8] Bernstein inequality. In *Encyclopedia of Mathematics*. Kluwer, 1987. Translator: M. Hazewinkel.

[9] S. N. Bernstein. On a modification of Chebyshev's inequality and of the error formula of Laplace. *Ann. Sci. Inst. Sav. Ukraine, Sect. Math. 1*, 1924.

[10] S. N. Bernstein. On certain modifications of Chebyshev's inequality. *Doklady Akademii Nauk SSSR*, 17(6):275–277, 1937.

[11] P. Billingsley. *Probability and Measure*. Wiley, third edition, 1995.

[12] J. Bourgain. On Lipschitz embedding of finite metric spaces in Hilbert space. *Israel J. Math.*, 52:46–52, 1985.

[13] H. Chernoff. A measure of asymptotic efficiency for tests of a hypothesis based on the sum of observations. *Ann. Math. Stat.*, 23:493–507, 1952.

[14] T. M. Cover and J. A. Thomas. *Elements of Information Theory*. Wiley, 1991.

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

[16] D. E. Daykin and L. Lovasz. The number of values of Boolean functions. *J. London Math. Soc.*, 2(12):225–230, 1976.

[17] R. A. DeMillo and R. J. Lipton. A probabilistic remark on algebraic program testing. *Information Processing Letters*, 7(4):193 – 195, 1978.

[18] M. Dietzfelbinger, A. Karlin, K. Mehlhorn, F. Meyer auf der Heide, H. Rohnert, and R. E. Tarjan. Dynamic perfect hashing: Upper and lower bounds. *SIAM J. Comput.*, 23(4):738–761, 1994.

[19] L. Engebretsen, P. Indyk, and R. O'Donnell. Derandomized dimensionality reduction with applications. In *SODA*, 2002.

[20] P. Erdös. Some remarks on the theory of graphs. *Bull. Amer. Math. Soc.*, 53:292–294, 1947.

[21] P. Erdös. Graph theory and probability. *Canad. J. Math.*, 11:34–38, 1959.

[22] P. Erdös and G. Szekeres. A combinatorial problem in geometry. *Compositio Math.*, 2:463–470, 1935.

[23] P.C. Fishburn and N.J.A. Sloane. the solution to Berlekamp's switching game. *Discrete Mathematics*, 74:263–290, 1989.

[24] C. M. Fortuin, P. W. Kasteleyn, and J. Ginibre. Correlation inequalities on some partially ordered sets. *Commun. Math. Phys.*, 22:89–103, 1971.

[25] M. L. Fredman, J. Komlós, and E. Szemerédi. Storing a sparse table with O(1) worst case access time. *J. Assoc. Comput. Mach.*, 31(3):538–544, 1984.

[26] R. Freivalds. Probabilistic machines can use less running time. In *IFIP Congress*, pages 839–842, 1977.

[27] E. Friedgut and G. Kalai. Every monotone graph property has a sharp threshold. *Proc. Amer. Math. Soc.*, 124:2993–3002, 1996.

[28] H. N. Gabow and R. E. Tarjan. Faster scaling algorithms for general graph-matching problems. *J. ACM*, 38(4):815–853, 1991.

[29] F. Le Gall. Powers of tensors and fast matrix multiplication. In *International Symposium on Symbolic and Algebraic Computation, ISSAC '14, Kobe, Japan, July 23-25, 2014*, pages 296–303, 2014.

[30] S. Goldwasser and M. Sipser. Private coins versus public coins in interactive proof systems. pages 58–68, 1986.

[31] G. H. Gonnet. Determining equivalence of expressions in random polynomial time. In *Proceedings of the Sixteenth Annual ACM Symposium on Theory of Computing*, STOC '84, pages 334–341, New York, NY, USA, 1984. ACM.

[32] R. L. Graham, B. L. Rothschild, and J. H. Spencer. *Ramsey Theory*. Wiley, 2nd edition, 1990.

[33] G. Grimmett and D. Stirzaker. *Probability and Random Processes*. Oxford, third edition, 2001.

[34] T. E. Harris. Lower bound for the critical probability in a certain percolation process. *Math. Proc. Cambridge Philos. Soc.*, 56:13–20, 1960.

[35] J. Håstad. Some optimal inapproximability results. *J. ACM*, 48(4):798–859, 2001.

[36] W. E. Hickson. In *Oxford Dictionary of Quotations*, page 251. Oxford University Press, 3rd edition, 1979.

[37] W. Hoeffding. Probability inequalities for sums of bounded random variables. *J. Am. Stat. Assoc.*, 58:13–30, 1963.

[38] R. Holley. Remarks on the FKG inequalities. *Communications in Mathematical Physics*, 36:227–231, 1974. doi:10.1007/BF01645980.

[39] W. B. Johnson and J. Lindenstrauss. Extensions of Lipschitz mappings into a Hilbert space. *Contemp. Math.*, 26:189–206, 1984.

[40] V. Kabanets and R. Impagliazzo. Derandomizing polynomial identity tests means proving circuit lower bounds. *Comput. Complex.*, 13:1–46, 2004.

[41] A. Kalai. Generating random factored numbers, easily. *J. Cryptology*, 16:287–289, 2003.

[42] R. M. Karp, E. Upfal, and A. Wigderson. Constructing a Maximum Matching is in Random NC. *Combinatorica*, 6(1):35–48, 1986.

[43] D. J. Kleitman. Families of non-disjoint subsets. *J. Combin. Theory*, 1:153–155, 1966.

[44] D. Koller and N. Megiddo. Constructing small sample spaces satisfying given constants. *SIAM J. Discret. Math.*, 7:260–274, May 1994. Previously in 25th STOC pp.268-277, 1993.

[45] E. Kushilevitz and N. Nisan. *Communication Complexity*. Cambridge University Press, New York, NY, USA, 1997.

[46] R. Kutzelnigg. Bipartite random graphs and cuckoo hashing. In *Proceedings of the Fourth Colloquium on Mathematics and Computer Science*, 2006.

[47] F. T. Leighton. *Complexity issues in VLSI*. MIT Press, 1983.

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

[49] R. Lidl and H. Niederreiter. *Finite Fields*. 2nd edition, 1997. (Theorem 6.13).

[50] N. Linial, E. London, and Y. Rabinovich. The geometry of graphs and some of its algorithmic applications. *Combinatorica*, 15(2):215–245, 1995. Also in FOCS '94.

[51] S. Micali and V. V. Vazirani. An $O(\sqrt{|V|} \cdot |E|)$ algorithm for finding maximum matching in general graphs. In *Proc. 21st FOCS*, pages 17–27. IEEE, 1980.

[52] M. Mitzenmacher. Some open questions related to cuckoo hashing. In *Proc. European Symposium on Algorithms (ESA)*, 2009.

[53] R. A. Moser. A constructive proof of the Lovasz local lemma. In *Proceedings of the 41st annual ACM symposium on Theory of computing*, STOC '09, pages 343–350, New York, NY, USA, 2009. ACM.

[54] R. A. Moser and G. Tardos. A constructive proof of the general Lovasz local lemma. *CoRR*, abs/0903.0544, 2009.

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

[56] D. Mumford. The dawning of the age of stochasticity. In V. Arnold, M. Atiyah, P. Lax, and B. Mazur, editors, *Mathematics: Frontiers and Perspectives*. AMS, 2000.

[57] J. Pach and G. Tóth. Graphs drawn with few crossings per edge. *Combinatorica*, 17:427–439, 1997.

[58] A. Pagh and F. Rodler. Cuckoo hashing. *J. Algorithms*, 51(2):122–144, 2004. (Conf. version in 9th ESA pp. 121-133, 2001).

[59] V. Pan. Fast and efficient parallel algorithms for the exact inversion of integer matrices. In S.N. Maheshwari, editor, *Foundations of Software Technology and Theoretical Computer Science*, volume 206 of *Lecture Notes in Computer Science*, pages 504–521. Springer, 1985.

[60] S. Rajagopalan and L. J. Schulman. Verification of identities. *SIAM J. Comput.*, 29(4):1155–1163, 2000.

[61] F. P. Ramsey. On a problem of formal logic. *Proc. London Math. Soc.*, 48:264–286, 1930.

[62] M. Saks and A. Wigderson. Probabilistic boolean decision trees and the complexity of evaluating game trees. In *Proc. 27th IEEE Symp. on Foundations of Computer Science*, pages 29–38, 1986.

[63] I. N. Sanov. On the probability of large deviations of random variables. *Mat. Sbornik*, 42:11–44, 1957.

[64] J. Schwartz. Fast probabilistic algorithms for verification of polynomial identities. *Journal of the ACM*, 27:701–717, 1980.

[65] C. E. Shannon. A mathematical theory of communication. *Bell System Tech. J.*, 27:379–423; 623–656, 1948.

[66] J. B. Shearer. On a problem of Spencer. *Combinatorica*, 5:241–245, 1985.

[67] L. A. Shepp. The XYZ-conjecture and the FKG-inequality. *Ann. Probab.*, 10(3):824–827, 1982.

[68] D. Sivakumar. Algorithmic derandomization via complexity theory. In *STOC*, 2002.

[69] M. Tarsi. Optimal search on some game trees. *J. ACM*, 30(3):389–396, July 1983.

[70] W. T. Tutte. The factorization of linear graphs. *Journal of the London Mathematical Society*, s1-22(2):107–111, 1947.

[71] L. Valiant and V. Vazirani. NP is as easy as detecting unique solutions. *Theoretical Computer Science*, 47:85–93, 1986.

[72] R. Zippel. Probabilistic algorithms for sparse polynomials. In E. W. Ng, editor, *Symbolic and Algebraic Computation*, volume 72 of *Lecture Notes in Computer Science*, pages 216–226. Springer, 1979.