Bibliography

[1] Miklós Ajtai and Cynthia Dwork. A public-key cryptosystem with worst-case/average-case equivalence. In *Proceedings of the Twenty-Ninth Annual ACM Symposium on Theory of Computing*, pages 284–293, El Paso, Texas, 4–6 May 1997.

[2] Noga Alon and Joel H. Spencer. *The Probabilistic Method.* John Wiley & Sons, Inc., 1992.

[3] Eric Bach and Jeffrey Shallit. *Algorithmic Number Theory, Volume 1: Efficient Algorithms.* MIT Press, 1998.

[4] Robert Beals. Quantum computation of Fourier transforms over symmetric groups. In *Proceedings of the Twenty-Ninth Annual ACM Symposium on Theory of Computing*, pages 48–53, El Paso, Texas, 4–6 May 1997.

[5] P. Benioff. Quantum mechanical hamiltonian models of turning machines. *J. Stat. Phys.*, 29:515–546, 1982.

[6] C. H. Bennett. Logical reversibility of computation. *IBM J. of Research and Development*, 17:525–532, 1973.

[7] Charles H. Bennett, Ethan Bernstein, Gilles Brassard, and Umesh Vazirani. Strengths and weaknesses of quantum computing. *SIAM Journal on Computing*, 26(5):1510–1523, October 1997.

[8] Ethan Bernstein and Umesh Vazirani. Quantum complexity theory. *SIAM Journal on Computing*, 26(5):1411–1473, October 1997.

[9] A. Berthiaume and G. Brassard. The quantum challenge to structural complexity theory. In Osamu Barrington, David Mix; Brassard, Gilles; Hemachandra, Lane; Leivant, Daniel; Chair, Tim Long; Nisan, Noam; Royer, James; Watanabe, editor, *Proceedings of the 7th Annual Conference on Structure in Complexity Theory (SCTC '92)*, pages 132–137, Boston, MA, USA, June 1992. IEEE Computer Society Press.

[10] A. Berthiaume and G. Brassard. Oracle quantum computing. *Journal of Modern Optics*, 41:2521–2535, 1994.

[11] Dan Boneh and Richard J. Lipton. Quantum cryptanalysis of hidden linear functions (extended abstract). In Don Coppersmith, editor, *Advances in Cryptology—CRYPTO '95*, volume 963 of *Lecture Notes in Computer Science*, pages 424–437. Springer-Verlag, 27–31 August 1995.

[12] B. H. Bransden and C. J. Joachain. *Introduction to Quantum Mechanics*. Longman Scientific & Technical, 1995.

[13] Ronald J. Evans Bruce C. Berndt and Kenneth S. Williams. *Gauss and Jacobi Sums*. John Wiley & Sons, 1998.

[14] R. Cleve, E. Ekert, C. Macchiavello, and M. Mosca. Quantum algorithms revisited. *Proc. Roy. Soc. Lond. A*, 454:339–354, 1998.

[15] John B. Conway. *A Course in Functional Analysis.* Number 96 in Graduate Texts in Mathematics. Springer-Verlag, New York, NY, 2nd edition, 1990.

[16] D. Coppersmith. An approximate fourier transform useful in quantum factoring. Technical Report RC19642, IBM, 1994.

[17] T. H. Cormen, C. E. Leiserson, and R. L. Rivest. *Introduction to Algorithms.* MIT Press and McGraw-Hill Book Company, 6th edition, 1992.

[18] Ivan Bjerre Damgård. On the randomness of Legendre and Jacobi sequences. In *Advances in Cryptology—CRYPTO '88*, volume 403, pages 163–172. Springer-Verlag, 1990, 21–25 August 1988.

[19] David Deutsch. Quantum theory, the church-turing principle and the universal quantum computer. *Proc. Roy. Soc. Lond. A*, 400:97–117, 1985.

[20] David Deutsch and Richard Jozsa. Rapid solution of problems by quantum computation. *Proc. Roy. Soc. Lond. A*, 439:553–558, 1992.

[21] Persi Diaconis and Daniel Rockmore. Efficient computation of the Fourier transform on finite groups. *J. Amer. Math. Soc.*, 3(2):297–332, 1990.

[22] Mark Ettinger and Peter Høyer. A quantum observable for the graph isomorphism problem. Technical report, quant-ph/9901029, 1999.

[23] Mark Ettinger and Peter Høyer. Quantum state detection via elimination. Technical report, quant-ph/9905099, 1999.

[24] Mark Ettinger and Peter Høyer. On quantum algorithms for noncommutative hidden subgroups. *Advances in Applied Mathematics*, (25):239–251, 2000.

[25] Mark Ettinger, Peter Høyer, and Emanuel Knill. Hidden subgroup states are almost orthogonal. Technical report, quant-ph/9901034, 1999.

[26] R. Feynman. Simulating physics with computers. *International Journal of Theoretical Physics*, 21:467–488, 1982.

[27] Mikael Goldmann and Alexander Russell. The computational complexity of solving systems of equations over finite groups. In *Fourteenth Annual IEEE Conference on Computational Complexity*, Atlanta, Georgia, 4–6 May 1999.

[28] Michaelangelo Grigni, Leonard Schulman, and Umesh Vazirani. Quantum mechanical algorithms for the non-abelian hidden subgroup problem. Manuscript, 1997.

[29] D.Y. Grigoriev. Testing the shift-equivalence of polynomials using quantum machines. *Theoretical Computer Science*, (180):217–228, 1997.

[30] Lov K. Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of the Twenty-Eighth Annual ACM Symposium on the Theory of Computing*, pages 212–219, Philadelphia, Pennsylvania, 22–24 May 1996.

[31] Lisa Hales and Sean Hallgren. Quantum fourier sampling simplified. In *Proceedings*

of the Thirty-First Annual ACM Symposium on Theory of Computing, pages 330–338, Atlanta, Georgia, 1–4 May 1999.

[32] Lisa Hales and Sean Hallgren. An improved quantum fourier transform algorithm and applications. In *Proceedings of the 41st Annual Symposium on Foundations of Computer Science*, Redondo Beach, California, 12–14 November 2000.

[33] Sean Hallgren, Alexander Russell, and Amnon Ta-Shma. Normal subgroup reconstruction and quantum computation using group representations. In *Proceedings of the Thirty-Second Annual ACM Symposium on Theory of Computing*, pages 627–635, Portland, Oregon, 21–23 May 2000.

[34] Joe Harris and William Fulton. *Representation Theory.* Number 129 in Graduate Texts in Mathematics. Springer-Verlag, New York, NY, 1991.

[35] Peter Høyer. Simplified proof of the fourier sampling theorem. *Information Processing Letters*, 75:139–143, 2000.

[36] Alexey Yu. Kitaev. Quantum measurements and the abelian stabilizer problem. Technical report, quant-ph/9511026, 1995.

[37] Johannes Köbler, Uwe Schöning, and Jacobo Torán. *The Graph Isomorphism Problem: Its Structural Complexity.* Birkhäuser Boston Inc., Boston, MA, 1993.

[38] G. L. Miller. Riemann's hypothesis and tests for primality. *J. Comput. System Sci*, 13:300–317, 1976.

[39] Michele Mosca and Artur Ekert. The hidden subgroup problem and eigenvalue estima-

tion on a quantum computer. In *QCQS: NASA International Conference on Quantum Computing and Quantum Communications, QCQS*. LNCS, 1998.

[40] Rajeev Motwani and Prabhakar Raghavan. *Randomized Algorithms*. Cambridge University Press, Cambridge, England, June 1995.

[41] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.

[42] R. Peralta. On the distribution of quadratic residues and non-residues modulo a prime number. *Mathematics of Computation*, 58:433 – 440, 1992.

[43] John Preskill. Lecture notes on quantum information and quantum computation. Technical report, Web address: www.theory.caltech.edu/people/preskill/ph229.

[44] Martin Rötteler and Thomas Beth. Polynomial-time solution to the hidden subgroup problem for a class of non-abelian groups. Technical report, quant-ph/9812070, 1998.

[45] Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5):1484–1509, October 1997.

[46] Daniel R. Simon. On the power of quantum computation. *SIAM Journal on Computing*, 26(5):1474–1483, October 1997.

[47] Audrey Terras. *Fourier Analysis on Finite Groups and Applications*. Number 43 in London Mathematical Society Student Texts. Cambridge University Press, 1999.

[48] Wim van Dam. Quantum algorithms for weighing matrices and quadratic residues. Technical report, quant-ph archive no. 0008059, 2000.

[49] Wim van Dam and Sean Hallgren. Efficient quantum algorithms for shifted quadratic character problems. Technical report, quant-ph archive no. 0011067, 2000.

[50] U. V. Vazirani. Personal Communication, 2000.

[51] Christof Zalka. On a particular non-abelian hidden subgroup problem.