# References


1. Andris Ambainis: *A note on quantum black-box complexity of almost all Boolean functions*, Information Processing Letters 71, 5–7 (1999). Electronically available at quant-ph/9811080.[9]
2. E. Bach and J. Shallit: *Computational number theory*, MIT Press (1996).
3. Adriano Barenco, Charles H. Bennett, Richard Cleve, David P. DiVincenzo, Norman Margolus, Peter Shor, Tycho Sleator, John Smolin, and Harald Weinfurter: *Elementary gates for quantum computation*, Physical Review A 52:5, 3457–3467 (1995). Electronically available at quant-ph/9503016.
4. R. Beals, H. Buhrman, R. Cleve, M. Mosca, and R. de Wolf: *Quantum lower bounds by polynomials*, Proceedings of the 39th Annual IEEE Symposium on Foundations of Computer Science – FOCS, 352–361 (1998). Electronically available at quant-ph/9802049.
5. P. A. Benioff: *Quantum mechanical Hamiltonian models of discrete processes that erase their own histories: application to Turing machines*, International Journal of Theoretical Physics 21:3/4, 177–202, (1982).
6. Charles H. Bennett: *Logical reversibility of computation*, IBM Journal of Research and Development 17, 525–532 (1973).
7. Charles H. Bennett: *Time/space trade-offs for reversible computation*, SIAM Journal of Computing 18, 766–776 (1989).
8. Charles H. Bennett, Ethan Bernstein, Gilles Brassard, and Umesh V. Vazirani: *Strengths and weaknesses of quantum computation*, SIAM Journal of Computing 26:5, 1510–1523 (1997). Electronically available at quant-ph/9701001.
9. Ethan Bernstein and Umesh Vazirani: *Quantum complexity theory*, SIAM Journal of Computing 26:5, 1411–1473 (1997).
10. André Berthiaume and Gilles Brassard: *Oracle quantum computing*, Proceedings of the Workshop on Physics and Computation – PhysComp'92, IEEE Press, 195–199 (1992).
11. Michel Boyer, Gilles Brassard, Peter Hoyer, and Alain Tapp: *Tight bound on quantum searching*, Fourth Workshop on Physics and Computation – PhysComp'96, Ed.: T. Toffoli, M. Biaford, J. Lean, New England Complex Systems Institute, 36–43 (1996). Electronically available at quant-ph/9605034.
12. Gilles Brassard and Peter Hoyer: *An exact quantum polynomial-time algorithm for Simon's problem*, Proceedings of the 1997 Israeli Symposium on Theory of Computing and Systems – ISTCS'97, 12–23 (1997). Electronically available at quant-ph/9704027.
13. Gilles Brassard, Peter Hoyer, and Alain Tapp: *Quantum counting*, Automata, Languages and Programming, Proceedings of the 25th International Colloquium, ICALP'98, Lecture Notes in Computer Science 1443, 820–831, Springer (1998). Electronically available at quant-ph/9805082.


[9] Code "quant-ph/9811080" refers to http://xxx.lanl.gov/abs/quant-ph/9811080 at Los Alamos preprint archive.

14. Leon Brillouin: *Science and information theory*, 2nd edition, Academic Press (1967).
15. Paul Busch, Pekka J. Lahti, and P. Mittelstaedt: *The quantum theory of measurement*, Springer-Verlag, 1991.
16. A. R. Calderbank, Peter W. Shor: *Good quantum error-correcting codes exist*, Physical Review A 54, 1098–1105 (1996). Electronically available at quant-ph/9512032.
17. Man-Duen Choi: *Completely positive linear maps on complex matrices*, Linear Algebra and its Applications 10, 285–290 (1975).
18. Isaac L. Chuang, Lieven M. K. Vandersypen, Xinlan Zhou, Debbie W. Leung, and Seth Lloyd: *Experimental realization of a quantum algorithm*, Nature 393, 143–146 (1998). Electronically available at quant-ph/9801037.
19. Juan I. Cirac and Peter Zoller: *Quantum computations with cold trapped ions*, Physical Review Letters 74:20, 4091–4094 (1995).
20. Henri Cohen: *A course in computational algebraic number theory*, Graduate Texts in Mathematics 138, Springer (1993), 4th printing 2000.
21. Win van Dam: *Two classical queries versus one quantum query*, electronically available at quant-ph/9806090.
22. David Deutsch: *Uncertainty in quantum measurements*, Physical Review Letters 50:9, 631–633 (1983).
23. David Deutsch: *Quantum theory, the Church-Turing principle and the universal quantum computer*, Proceedings of the Royal Society of London A 400, 97–117 (1985).
24. David Deutsch: *Quantum computational networks*, Proceedings of the Royal Society of London A 425, 73–90 (1989).
25. David Deutsch, Adriano Barenco, and Artur Ekert: *Universality in quantum computation*, Proceedings of the Royal Society of London A 449, 669–677 (1995). Electronically available at quant-ph/9505018.
26. David Deutsch, Richard Jozsa: *Rapid solutions of problems by quantum computation*, Proceedings of the Royal Society of London A 439, 553–558 (1992).
27. Chistoph Dürr and Peter Hoyer: *A quantum algorithm for finding the minimum*, electronically available at quant-ph/9607014.
28. Mark Ettinger and Peter Hoyer: *On quantum algorithms for noncommutative hidden subgroups*, Proceedings of the 16th Annual Symposium on Theoretical Aspects of Computer Science – STACS 99, Lecture Notes in Computer Science 1563, 478–487, Springer (1999). Electronically available at quant-ph/9807029.
29. Edward Farhi, Jeffrey Goldstone, Sam Gutmann, and Michael Sipser: *A limit on the speed of quantum computation in determining parity*, Physical Review Letters 81:5, 5442–5444 (1998). Electronically available at quant-ph/9802045.
30. Richard P. Feynman: *Simulating physics with computers*, International Journal of Theoretical Physics 21:6/7, 467–488 (1982).
31. Lov K. Grover: *A fast quantum-mechanical algorithm for database search*, Proceedings of the 28th Annual ACM Symposium on the Theory of Computing – STOC, 212–219 (1996). Electronically available at quant-ph/9605043.
32. Josef Gruska: *Quantum Computing*, McGraw-Hill (1999).
33. G. H. Hardy and E. M. Wright: *An introduction to the theory of numbers*, 4th ed. with corrections, Clarendon Press, Oxford (1971).
34. Mika Hirvensalo: *On quantum computation*, Ph.Lic. Thesis, University of Turku, 1997.
35. Mika Hirvensalo: *The reversibility in quantum computation theory*, Proceedings of the 3rd International Conference Developments in Language Theory – DLT'97, Ed.: Symeon Bozapalidis, Aristotle University of Thessaloniki, 203–210 (1997).

36. Loo Keng Hua: *Introduction to number theory*, Springer-Verlag, 1982.
37. E. Knill, R. Laflamme, R. Martinez, C.-H. Tseng: *An algorithmic benchmark for quantum information processing*, Nature 404: 368–370 (2000).
38. Rolf Landauer: *Irreversibility and heat generation in the computing process*, IBM Journal of Research and Development 5, 183-191 (1961).
39. M. Y. Lecerf: *Récursive insolubilité de l'équation générale de diagonalisation de deux monomorphismes de monoïdes libres* $\varphi x = \psi x$, Comptes Rendus de l'Académie des Sciences 257, 2940–2943 (1963).
40. Ming Li, John Tromp and Paul Vitányi: *Reversible simulation of irreversible computation*, Physica D 120:1/2, 168-176 (1998). Electronically available at quant-ph/9703009.
41. Seth Lloyd: *A potentially realizable quantum computer*, Science 261, 1569–1571 (1993).
42. Hans Maassen and J. B. M. Uffink: *Generalized entropic uncertainty relations*, Physical Review Letters 60:12, 1103–1106 (1988).
43. F. J. MacWilliams and Neil J. A. Sloane: *The theory of error-correcting codes*, North-Holland (1981).
44. Gary L. Miller: *Riemann's hypothesis and tests for primality*, Journal of Computer and System Sciences 13, 300–317 (1976).
45. Michele Mosca and Artur Ekert: *The hidden subgroup problem and eigenvalue estimation on a quantum computer*, Quantum Computing and Quantum Communications, Proceedings of the 1st NASA International Conference, Lecture Notes in Computer Science 1509, 174–188, Springer (1998). Electronically available at quant-ph/9903071.
46. A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone: *Handbook of applied cryptography*, Series on Discrete and Mathematics and Its Applications, CRC Press (1997).
47. Masanao Ozawa: *Quantum Turing machines: local transitions, preparation, measurement, and halting problem*, electronically available at quant-ph/9809038 (1998).
48. Christos H. Papadimitriou: *Computational complexity*, Addison-Wesley (1994).
49. K. R. Parthasarathy: *An introduction to quantum stochastic calculus*, Birkhäuser, Basel (1992).
50. R. Paturi: *On the degreee of polynomials that approximate symmetric Boolean functions*, Proceedings of the 28th Annual ACM Symposium on the Theory of Computing – STOC, 468-474 (1992).
51. Max Planck: Annalen der Physik 1, 69, 1900; Verhandlg. dtsch. phys. Ges., 2, 202; Verhandlg. dtsch. phys. Ges. 2, 237; Annalen der Physik 4, 553, 1901.
52. M. B. Plenio and P. L. Knight: *Realistic lower bounds for the factorization time of large numbers on a quantum computer*, Physical Review A 53:5, 2986–2990 (1996). Electronically available at quant-ph/9512001.
53. E. L. Post: *The two-valued iterative systems of mathematical logic*, Princeton University Press (1941).
54. E. L. Post: *A variant of a recursively unsolvable problem*, Bulletin of the American Mathematical Society 52, 264–268 (1946).
55. John Preskill: *Robust solutions to hard problems*, Nature 391, 631–632 (1998).
56. Marcel Riesz: *Sur les maxima des formes bilinéaires et sur les fonctionnelles linéaires*, Acta Mathematica 49, 465–497 (1926).
57. Yurii Roghozin *On the notion of universality and small universal Turing machines*, Theoretical Computer Science 168, 215–240 (1996).
58. Sheldon M. Ross: *Introduction to probability models*, 4th edition, Academic Press (1985).

59. J. Barkley Rosser and Lowell Schoenfeld, *Approximate formulas for some functions of prime numbers*, Illinois Journal of Mathematics 6:1, 64–94 (1962).
60. Walter Rudin: *Functional Analysis*, 2nd edition, McGraw-Hill (1991).
61. Keijo Ruohonen: *Reversible machines and Post's correspondence problem for biprefix morphisms*, EIK – Journal of Information Processing and Cybernetics 21:12, 579–595 (1985).
62. Arto Salomaa: *Public-key cryptography*, Texts in Theoretical Computer Science – An EATCS Series, 2nd ed., Springer (1996).
63. Peter W. Shor: *Algorithms for quantum computation: discrete log and factoring*, Proceedings of the 35th Annual IEEE Symposium on Foundations of Computer Science – FOCS, 20–22 (1994).
64. Peter W. Shor: *Scheme for reducing decoherence in quantum computer memory*, Physical Review A 52:4, 2493–2496 (1995).
65. Daniel R. Simon: *On the power of quantum computation*, Proceedings of the 35th Annual IEEE Symposium on Foundations of Computer Science – FOCS, 116–123 (1994).
66. Douglas R. Stinson: *Cryptography - Theory and practice*, Series on Discrete Mathematics and Its Applications, CRC Press, Boca Raton (1995).
67. W. Tittel, J. Brendel, H. Zbinden, N. Gisin: *Violation of Bell inequalities by photons more than 10 km apart*, Physical Review Letters 81:17, 3563–3566, (1998). Electronically available at quant-ph/9806043.
68. Tommaso Toffoli: *Bicontinuous extensions of invertible combinatorial functions*, Mathematical Systems Theory 14, 13–23 (1981).
69. B. L. van der Waerden: *Sources of quantum mechanics*, North-Holland (1967).
70. C. P. Williams and S. H. Clearwater: *Explorations in quantum computing*, Springer (1998).
71. C. P. Williams and S. H. Clearwater: *Ultimate zero and one. Computing at the quantum frontier*, Springer (2000).
72. William K. Wootters, Wojciech H. Zurek: *A single quantum cannot be cloned*, Nature 299, 802–803 (1982).
73. Andrew Chi-Chih Yao: *Quantum circuit complexity*, Proceedings of the 34th Annual IEEE Symposium on Foundations of Computer Science – FOCS, 352–361 (1993).

# Index

## *Natural Computing Series*

W.M. Spears: Evolutionary Algorithms. The Role of Mutation and Recombination. XIV, 222 pages, 55 figs., 23 tables. 2000

H.-G. Beyer: The Theory of Evolution Strategies. XIX, 380 pages, 52 figs., 9 tables. 2001

L. Kallel, B. Naudts, A. Rogers (Eds.): Theoretical Aspects of Evolutionary Computing. X, 497 pages. 2001

M. Hirvensalo: Quantum Computing. XI, 190 pages. 2001

M. Amos: Theoretical and Experimental DNA Computation. Approx. 200 pages. 2001

L.F. Landweber, E. Winfree (Eds.): Evolution as Computation. DIMACS Workshop, Princeton, January 1999. Approx. 300 pages. 2001