

Extended references on quantum computing

By various people – gathered here by
Tom Carter

<http://cogs.csustan.edu/~tom/quantum>

. . .

...

May, 1999

Our general topics: ←

- ⊙ Extended references
- ⊙ Selected on-line references

This is an unedited collection of references on quantum computation and related topics that I gathered in 1999 from a variety of sources. I claim no originality for this compilation, and, unfortunately, I didn't keep good notes about where I found many of these references. I apologize to those to whom credit should go.

I hope it is all right to make this large list available purely to assist researchers in the field . . .

[To top ←](#)

References

- [1] Abrams D S and Lloyd S, Simulation of Many-Body Fermi Systems on a Universal Quantum Computer, *Phys.Rev.Lett.* **79** 2586–2589, 1997
- [2] Abrams D S and Lloyd S, Non-Linear Quantum Mechanics implies Polynomial Time solution for NP-complete and $\#P$ problems,
<http://xxx.lanl.gov/abs/quant-ph/9801041>
- [3] Adleman L, Demarrais J and Huang M-D, Quantum Computability, *SIAM Journal of Computation* **26** 5 pp 1524–1540 October, 1997
- [4] Adleman L, Molecular computation of solutions to combinatorial problems, *Science*, 266, 1021–1024, Nov. 11, 1994
- [5] Aharonov D and Ben-Or M, Fault-Tolerant Quantum Computation with Constant Error, *Proc. of the 29th Annual ACM Symposium on Theory of Computing (STOC)* 1997

- [6] Aharonov D and Ben-Or M, Polynomial Simulations of Decohered Quantum Computers *37th Annual Symposium on Foundations of Computer Science (FOCS)* pp 46–55, 1996
- [7] Aharonov D, Kitaev A Yu and Nisan N, Quantum Circuits with Mixed States, *Proc. of the 30th Annual ACM Symposium on Theory of Computing (STOC)* 1998
- [8] Aharonov D, Ben-Or M, Impagliazzo R and Nisan N, Limitations of Noisy Reversible Computation, in *LANL e-print* quant-ph/9611028, <http://xxx.lanl.gov> (1996)
- [9] Aharonov D, Beckman D, Chuang I and Nielsen M, What Makes Quantum Computers Powerful? <http://wwwcas.phys.unm.edu/~mnielsen/science.html>
- [10] Anderson P W, More Is Different, *Science*, **177**, 4047, 393–396, 1972
- [11] Aharonov, D., Quantum Computation, Annual Reviews of Computational Physics VI, Edited by Dietrich Stauffer, World Scientific, 1998
- [12] Aspect A, Dalibard J and Roger G, Experimental test of Bell's inequalities using time-varying analyzers, *Phys. Rev. Lett.* **49**, 1804–1807, 1982

- [13] Aspect A, Testing Bell's inequalities, *Europhys. News.* **22**, 73–75, 1991
- [14] Barahona F, in *J. Phys. A* vol. 15, (1982) 3241
- [15] Barenco A A universal two-bit gate for quantum computation, *Proc. R. Soc. Lond. A* **449** 679–683, 1995
- [16] Barenco A and Ekert A K Dense coding based on quantum entanglement, *J. Mod. Opt.* **42** 1253–1259, 1995
- [17] Barenco A, Deutsch D, Ekert E and Jozsa R, Conditional quantum dynamics and quantum gates, *Phys. Rev. Lett.* **74** 4083–4086, 1995
- [18] Barenco A, Bennett C H, Cleve R, DiVincenzo D P, Margolus N, Shor P, Sleator T, Smolin J A and Weinfurter H, Elementary gates for quantum computation, *Phys. Rev. A* **52**, 3457–3467, 1995
- [19] Barenco A 1996 Quantum physics and computers, *Contemp. Phys.* **37** 375–389 1996
- [20] Barenco A, Ekert A, Suominen K A and Torma P, Approximate quantum Fourier transform and decoherence, *Phys. Rev. A* **54**, 139–146, 1996

- [21] Barenco A, Berthiaume A, Deutsch D, Ekert A, Jozsa R, and Macchiavello C, Stabilization of Quantum Computations by Symmetrization, *SIAM J. Comp.***26**,5, 1541–1557, 1997
- [22] Barenco A, Brun T A, Schak R and Spiller T P, Effects of noise on quantum error correction algorithms, *Phys. Rev. A* **56** 1177–1188, 1997
- [23] Barnum H, Fuchs C A, Jozsa R and Schumacher B 1996 A general fidelity limit for quantum channels, *Phys. Rev. A* **54** 4707-4711
- [24] Barnum H, Caves C, Fuchs C A, Jozsa R and Schumacher B, Non commuting mixed states cannot be broadcast, *Phys. Rev. Lett.***76** 2818–2822, 1996
- [25] Barnum H, Nielsen M and Schumacher B, in *Phys. Rev. A*, **57**,6, 1998, pp. 4153–4175
- [26] Beals R, Quantum computation of Fourier transform over symmetric groups *Proc. of the 29th Annual ACM Symposium on Theory of Computing (STOC)* 1997
- [27] Beals R, Buhrman H, Cleve R, Mosca M and de Wolf R, Quantum Lower Bounds by Polynomials, in *39th Annual Symposium on Foundations of Computer Science(FOCS)*, (1998)

- [28] Beckman D, Chari A, Devabhaktuni S and Preskill J Efficient networks for quantum factoring, *Phys. Rev. A* **54**, 1034–1063, 1996
- [29] Bell J S On the Einstein-Podolsky-Rosen paradox, *Physics* **1** 195–200, 1964
- [30] Bell J S On the problem of hidden variables in quantum theory, *Rev. Mod. Phys.* **38** 447-52, 1966 *Speakable and unspeakable in quantum mechanics* 1987 (Cambridge University Press)
- [31] Benioff P, The Computer as a Physical Systems: A Microscopic Quantum Mechanical Hamiltonian Model of Computers as Represented by Turing Machines, *J. Stat. Phys.* **22** 563–591, 1980
- [32] Benioff P Quantum mechanical Hamiltonian models of Turing machines, *J. Stat. Phys.* **29** 515-546 1982
- [33] Bennett C H, Logical reversibility of computation, *IBM J. Res. Develop.* **17** 525–532, 1973
- [34] Bennett C H, The Thermodynamics of Computation - a Review, *International Journal of Theoretical Physics*, **21**, No. 12, p 905, 1982
- [35] Bennett C H and Landauer R, The fundamental physical limits of computation, *Scientific American*, July 38–46, 1985

- [36] Bennett C H, Demons, engines and the second law, *Scientific American* **257** no. 5 (November) pp 88–96, 1987
- [37] Bennett C H, Brassard G, Briedbart S and Wiesner S, Quantum cryptography, or unforgeable subway tokens, *Advances in Cryptology: Proceedings of Crypto '82* (Plenum, New York) pp 267–275, 1982
- [38] Bennett C H and Brassard G, Quantum cryptography: public key distribution and coin tossing, in *Proc. IEEE Conf. on Computers, Syst. and Signal Process.* pp 175–179, 1984
- [39] Bennett C H and Wiesner S J, Communication via one- and two-particle operations on Einstein-Podolsky-Rosen states, *Phys. Rev. Lett.* **69**, 2881–2884, 1992
- [40] Bennett C H, Quantum information and computation, *Phys. Today* **48 10** 24–30, 1995
- [41] C.H. Bennett, Time/Space Trade-offs for Reversible Computation, *SIAM Journal of Computation*, **18**, 4, pp 766–776, 1989
- [42] Bennett C H and Brassard G 1989, SIGACT News **20**, 78–82

- [43] Bennett C H, Bessette F, Brassard G, Savail L and Smolin J Experimental quantum cryptography, *J. Cryptology* **5**, pp 3–28, 1992
- [44] Bennett C H Quantum Computers: Certainty from Uncertainty, *Nature*, 362, 1993
- [45] Bennett C H, Brassard G, Crépeau C, Jozsa R, Peres A and Wootters W K Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels, *Phys. Rev. Lett.* **70** 1895–1898, 1993
- [46] Bennett C H, Progress towards quantum computation 1995
- [47] Bennett C H, Brassard G, Popescu S, Schumacher B, Smolin J A and Wootters W K 1996a Purification of noisy entanglement and faithful teleportation via noisy channels, *Phys. Rev. Lett.* **76** 722-725
- [48] Bennett C H, DiVincenzo D P, Smolin J A and Wootters W K Mixed state entanglement and quantum error correction, *Phys. Rev. A* **54** 3825, 1996
- [49] Bennett C H, Bernstein E, Brassard G and Vazirani U Strengths and Weaknesses of quantum computing, *SIAM Journal of Computation* **26** 5 pp 1510–1523 October, 1997

- [50] Berman G P, Doolen G D, Holm D D, Tsifrinovich V I Quantum computer on a class of one-dimensional Ising systems, *Phys. Lett.* **193** 444-450 1994
- [51] Bernstein E and Vazirani U, 1993, Quantum complexity theory, *SIAM Journal of Computation* **26** 5 pp 1411–1473 October, 1997
- [52] Berthiaume A, Deutsch D and Jozsa R, The stabilization of quantum computation, in *Proceedings of the Workshop on Physics and Computation, PhysComp 94* 60-62 Los Alamitos: IEEE Computer Society Press, 1994
- [53] Berthiaume A and Brassard G, The quantum challenge to structural complexity theory, in *Proc. of the Seventh Annual Structure in Complexity Theory Conference* 1992 (IEEE Computer Society Press, Los Alamitos, CA) 132–137
- [54] Berthiaume A and Brassard G, Oracle quantum computing, in *Proc. of the Workshop on Physics of Computation: PhysComp '92* (IEEE Computer Society Press, Los Alamitos, CA) 60–62, 1992
- [55] Boghosian B M and Taylor W, Simulating quantum mechanics on a quantum computer in *Physica D*, 120 (1998) pp. 30-42

- [56] Bohm D 1951 *Quantum Theory* (Englewood Cliffs, N. J.)
- [57] Bohm D and Aharonov Y 1957 *Phys. Rev.* **108** 1070
- [58] Bollinger J J, Heinzen D J, Itano W M, Gilbert S L and Wineland D J, *Phys Rev Lett* 63 1031, 1989
- [59] D. Boneh, R. Lipton, Quantum Cryptoanalysis Of Hidden Linear Functions, *Proceedings of CRYPTO'95*
- [60] Bouwmeester D, Pan J-W, Mattle K, Weinfurter H, Zeilinger A, Experimental quantum teleportation *Nature* **390**, 575-579 1997
- [61] Boyer M, Brassard G, Hoyer P and Tapp A, Tight bounds on quantum searching, in *Fortsch.Phys.* 46, (1998) pp. 493-506
- [62] Brassard G, Searching a quantum phone book, **Science** **275** 627-628 1997
- [63] Brassard G and Crepeau C, *SIGACT News* **27** 13-24 1996
- [64] Brassard G, Hoyer P and Tapp A, Quantum Algorithm for the Collision Problem in *LANL e-print* quant-ph/9705002, <http://xxx.lanl.gov> (1997)

- [65] Brassard G and Hoyer P, An Exact Quantum-Polynomial Algorithm for Simon's Problem *Proceedings of the 5th Israeli Symposium on Theory of Computing and Systems (ISTCS)*, 1997
- [66] Brassard G, Teleportation as Quantum Computation, in *Physica D*, 120 (1998) 43-47
- [67] Brassard G, The dawn of a new era for quantum cryptography: The experimental prototype is working!, *Sigact News*, **20**(4), 78–82, 1989
- [68] Braunstein S L, Mann A and Revzen M 1992 Maximal violation of Bell inequalities for mixed states, *Phys. Rev. Lett.* **68**, 3259-3261
- [69] Braunstein S L and Mann A 1995 Measurement of the Bell operator and quantum teleportation, *Phys. Rev. A* **51**, R1727-R1730
- [70] Brillouin L 1956, *Science and information theory* (Academic Press, New York)
- [71] Brune M, Nussenzveig P, Schmidt-Kaler F, Bernardot F, Maali A, Raimond J M and Haroche S, From Lamb shift to light shifts: vacuum and subphoton cavity fields measured by atomic phase sensitive detection, *Phys. Rev. Lett.* **72**, 3339-3342 1994

- [72] Buhrman H, Cleve R and van Dam W, Quantum Entanglement and Communication Complexity, in *LANL e-print* quant-ph/9705033, <http://xxx.lanl.gov> (1997)
- [73] Buhrman H, Cleve R and Wigderson A, Quantum vs. Classical Communication and Computation, in *Proc. of the 30th Annual ACM Symposium on Theory of Computing (STOC)* (1998)
- [74] Calderbank A R and Shor P W, Good quantum error-correcting codes exist, *Phys. Rev. A* **54** 1098-1105, 1996
- [75] Calderbank A R, Rains E M, Shor P W and Sloane N J A Quantum error correction and orthogonal geometry, *Phys. Rev. Lett.* **78** 405–408, 1997
- [76] Calderbank A R, Rains E M, Shor P W and Sloane N J A, Quantum error correction via codes over $GF(4)$ in *LANL e-print* quant-ph/9608006, <http://xxx.lanl.gov> (1996), To appear in *IEEE Transactions on Information Theory*.
- [77] Caves C M 1990 Quantitative limits on the ability of a Maxwell Demon to extract work from heat, *Phys. Rev. Lett.* **64** 2111-2114
- [78] Caves C M, Unruh W G and Zurek W H 1990 comment, *Phys. Rev. Lett.* **65** 1387

- [79] Chernoff. See Feller W, An Introduction to Probability Theory and Its Applications, Wiley, New York,1957
- [80] Chuang I L, Laflamme R, Shor P W and Zurek W H, Quantum computers, factoring, and decoherence, *Science* **270** 1633–1635, 1995
- [81] Chuang I L, Laflamme R and Paz J P, Effects of Loss and Decoherence on a Simple Quantum Computer,
<http://xxx.lanl.gov/abs/quant-ph/9602018>
- [82] I.Chuang and W.C.D. Leung and Y. Yamamoto, Bosonic Quantum Codes for Amplitude Damping, in *Phys. Rev. A*, **56**, 2, (1997) pp. 1114-1125
- [83] Chuang I L and Yamamoto Creation of a persistent qubit using error correction *Phys. Rev. A* **55**, 114–127, 1997
- [84] Chuang I L ,Vandersypen L M K, Zhou X, Leung D W and Lloyd S, Experimental realization of a quantum algorithm, in *Nature*, 393, 143-146 (1998)
- [85] Church A An unsolvable problem of elementary number theory, *Amer. J. Math.* **58** 345–363, 1936
- [86] Cirac I J and Zoller P Quantum computations with cold trapped ions, *Phys. Rev. Let.*, 74: 4091-4094, 1995.

- [87] Cirac J I, Pellizari T and Zoller P, Enforcing coherent evolution in dissipative quantum dynamics, *Science* **273**, 1207, 1996
- [88] Cirac J I, Zoller P, Kimble H J and Mabuchi H Quantum state transfer and entanglement distribution among distant nodes of a quantum network, *Phys. Rev. Lett.* **78**, 3221, 1997
- [89] Cirel'son (Tsirelson) B, Reliable storage of information in a system of unreliable components with local interactions. *Lecture notes in Mathematics* **653** 15–30 ,1978
- [90] Clausen M, Fast Generalized Fourier transforms, *Theoret. Comput. Sci.* **56** 55–63 1989
- [91] Clauser J F, Holt R A, Horne M A and Shimony A Proposed experiment to test local hidden-variable theories, *Phys. Rev. Lett.* **23** 880–884, 1969
- [92] Clauser J F and Shimony A, Bell's theorem: experimental tests and implications, *Rep. Prog. Phys.* **41** 1881–1927, 1978
- [93] Cleve R and DiVincenzo D P, Schumacher's quantum data compression as a quantum computation, *Phys. Rev. A* **54** 2636, 1996
- [94] Cleve R and Buhrman H, Substituting Quantum Entanglement for Communication in *Phys rev A*, **56** 2, (1997) pp. 1201-1204

- [95] Cleve R, van Dam W, Nielsen M and Tapp A, Quantum Entanglement and the Communication Complexity of the Inner Product Function, in *LANL e-print* quant-ph/9708019, <http://xxx.lanl.gov> (1997)
- [96] C. Cohen-Tanoudji, *Quantum Mechanics*, Wiley press, New York (1977)
- [97] Coppersmith D, An approximate Fourier transform useful in quantum factoring, IBM Research Report RC 19642, 1994
- [98] Cormen T, Leiserson C and Rivest R, *Introduction to Algorithms*, (pp 776–800 for FFT, 837–844 for primality test, 812 for extended Euclid algorithm, 834–836 for RSA cryptosystem) MIT press, 1990
- [99] Cory D G, Fahmy A F, and Havel T F, Nuclear magnetic resonance spectroscopy: an experimentally accessible paradigm for quantum computing, in *Proc. of the 4th Workshop on Physics and Computation* (Complex Systems Institute, Boston, New England) 1996
- [100] D. G. Cory, M. P. Price, and Havel T F, *Physica D*, 1998. In press (quant-ph/9709001).
- [101] Cory D. G, Fahmy A F, and Havel T F *Proc. Nat. Acad. of Sciences of the U. S.*, 94:1634–1639, 1997.

- [102] Cory D G, Mass W, Price M, Knill E, Laflamme R, Zurek W H, and Havel T F and Somaroo S S, Experimental quantum error correction in *Phys. Rev. Lett.***81** 10, (1998) pp. 2152-2155
- [103] Cover T M and Thomas J A, *Elements of Information Theory*, John Wiley and Sons, New York, 1991
- [104] R. E. Crandall The challenge of large numbers, In *Scientific American* February 59-62, 1997
- [105] Chupp T.E and Hoare R.J, *Phys Rev Lett* 64 2261 1990
- [106] van Dam W, A Universal Quantum Cellular Automaton, *Proceedings of the Fourth Workshop on Physics and Computation*, 1996
- [107] Deutsch D, Quantum theory, the Church-Turing principle and the universal quantum computer, In *Proc. Roy. Soc. Lond. A* **400** 97-117, 1985
- [108] Deutsch D, Quantum computational networks, In *Proc. Roy. Soc. Lond. A* **425** 73-90, 1989
- [109] Deutsch D and Jozsa R, Rapid solution of problems by quantum computation, In *Proc. Roy. Soc. Lond A* **439** 553-558, 1992

- [110] Deutsch D, Barenco A and Ekert A, Universality in quantum computation, In *Proc. R. Soc. Lond. A* **449** 669-677, 1995
- [111] D. Deutsch D and A. Ekert and R. Jozsa and C. Macchiavello and S. Popescu and A. Sanpera Quantum privacy amplification and the security of quantum cryptography over noisy channels, In *Phys. Rev. Lett.* **77** 2818, 1996
- [112] Diaconis P and Rockmore D, Efficient Computation of the Fourier transform on finite groups, *J. AMS* **3** No. 2, 297–332, 1990
- [113] Dieks D, Communication by EPR Devices, *Phys Lett A*, 92(6) 271–272 1982
- [114] Diedrich F, Bergquist J C, Itano W M and Wineland D J 1989 Laser cooling to the zero-point energy of motion, *Phys. Rev. Lett.* **62** 403
- [115] Dieks D 1982 Communication by electron-paramagnetic-resonance devices, *Phys. Lett. A* **92** 271
- [116] DiVincenzo D P, Two-bit gates are universal for quantum computation, *Phys. Rev. A* **51** 1015-1022 1995

- [117] DiVincenzo D P, Quantum computation, *Science* **270** 255-261 1995
- [118] DiVincenzo D P and Shor P W, Fault-tolerant error correction with efficient quantum codes, *Phys. Rev. Lett.* **77** 3260-3263, 1996
- [119] DiVincenzo D P, Quantum Gates and Circuits, in *Proceedings of the ITP Conference on Quantum Coherence and Decoherence*, December, (1996), Proc. R. Soc. London A
- [120] Durr C and Hoyer P, A Quantum Algorithm for Finding the Minimum, in *LANL e-print* quant-ph/9607014, <http://xxx.lanl.gov> (1996)
- [121] Durr C, LeThanh H and Santha M, A decision procedure for well formed linear quantum cellular automata, *Proceeding of the 37th IEEE Symposium on Foundations of Computer Science*, 38–45, 1996, and *Random Structures & Algorithms*, 1997
- [122] Einstein A, Rosen N and Podolsky B, *Phys. Rev.* **47**, 777 1935
- [123] Ekert A, Quantum cryptography based on Bell's theorem *Phys. Rev. Lett.* **67**, 661–663, 1996
- [124] Ekert A and Jozsa R Quantum computation and Shor's factoring algorithm, *Rev. Mod. Phys.* **68** 733 1996

- [125] Ekert A and Macchiavello C 1996 Quantum error correction for communication, *Phys. Rev. Lett.* **77** 2585-2588
- [126] Ekert A 1997 From quantum code-making to quantum code-breaking, (preprint quant-ph/9703035)
- [127] van Enk S J, Cirac J I and Zoller P 1997 Ideal communication over noisy channels: a quantum optical implementation, *Phys. Rev. Lett.* **78**, 4293-4296
- [128] Another proof of the parity lower bound, using interesting techniques, was found recently by E. Farhi, J. Goldstone, S. Gutmann, M. Sipser A Limit on the Speed of Quantum Computation in Determining Parity in *LANL e-print* quant-ph/9802045, <http://xxx.lanl.gov> (1998)
- [129] Feynman R P Simulating physics with computers, In *Int. J. Theor. Phys.* **21** 467-488, 1982
- [130] Feynman R P, Quantum mechanical computers, In *Found. of Phys.* **16** 507-531, 1986 see also *Optics News* February 1985, 11-20.
- [131] R. Feynman, Feynman lectures on computation, 1996.

- [132] Fortnow L and Rogers J, Complexity Limitations on quantum computation Technical report 97-003, DePaul University, School of Computer science, 1997
- [133] Fredkin E and Toffoli T 1982 Conservative logic, Int. J. Theor. Phys. **21** 219-253
- [134] Freedman M, Logic, P/NP and the quantum field computer, preprint, 1997
- [135] P. Ga'cs, Self Correcting Two Dimensional Arrays, in *Randomness and Computation*, 1989, edited by S. Micali, vol 5, in series "Advances in Computing Research", pages 240-241, 246-248, series editor: F.P.Preparata
- [136] P. Ga'cs, one dimensional self correcting array.
- [137] Gardiner C W, Quantum Noise, Springer-Verlag, Berlin, 1991
- [138] Garey M R and Johnson D S, Computers and Intractability, published by Freeman and Company, New York, 1979
- [139] A. Gaudí. The set of ropes is presented in *la sagrada familia* in Barcelona, Spain. Pictures of *la sagrada familia* can be found in:
<http://futures.wharton.upenn.edu/~jonath22/Gaudi/eltemple.html>

- [140] R. Geroch and G. Hartle Computability and Physical theories in *Between Quantum and Cosmos* edited by Zurek and Van der Merwe and Miller, Princeton University Press, 1988, 549-566
- [141] Gershenfeld N A and Chuang I L Bulk spin-resonance quantum computation, *Science*, 275:350–356, 1997.
- [142] Glauber R J 1986, in *Frontiers in Quantum Optics*, Pike E R and Sarker S, eds (Adam Hilger, Bristol)
- [143] Golay M J E 1949 Notes on digital coding, *Proc. IEEE* **37** 657
- [144] Gottesman D 1996 Class of quantum error-correcting codes saturating the quantum Hamming bound, *Phys. Rev. A* **54**, 1862-1868
- [145] Gottesman D A theory of fault-tolerant quantum computation, in *Phys. Rev. A*, **57** 127–137
- [146] Gottesman D, Evslin J, Kakade D and Preskill J, preprint (1996)
- [147] Greenberger D M, Horne M A and Zeilinger A 1989 Going beyond Bell's theorem, in *Bell's theorem, quantum theory and conceptions of the universe*, Kafatos M, ed, (Kluwer Academic, Dordrecht) 73-76

- [148] Greenberger D M, Horne M A, Shimony A and Zeilinger A 1990 Bell's theorem without inequalities, *Am. J. Phys.* **58**, 1131-1143
- [149] R. B. Griffiths and C. S. Niu 1996 Semi classical Fourier transform for quantum computation in *Phys. Rev. Lett.* ,76, pp. 3228–3231
- [150] Grover L K, Quantum mechanics helps in searching for a needle in a haystack, *Phys. Rev. Lett.* **79**, 325-328 1997 and the original STOC paper: A fast quantum mechanical algorithm for database search *Proc. of the 28th Annual ACM Symposium on Theory of Computing (STOC)* 212–221, 1996
- [151] Grover L K, A framework for fast quantum mechanical algorithms,
<http://xxx.lanl.gov/abs/quant-ph/9711043>
- [152] Grover L K, Quantum computers can search arbitrarily large databases by a single query in *Phys. Rev. Lett.* **79** 23, 4709–4712, 1997
- [153] Grover L K, A fast quantum mechanical algorithm for estimating the median,
<http://xxx.lanl.gov/abs/quant-ph/9607024>
- [154] Hagley E et. al, Generation of Einstein Podolsky Rosen pairs of atoms, *Phys. Rev. Lett*, **79**, 1–5, 1997

- [155] Hamming R W 1950 Error detecting and error correcting codes, Bell Syst. Tech. J. **29** 147
- [156] Hamming R W 1986 *Coding and information theory*, 2nd ed, (Prentice-Hall, Englewood Cliffs)
- [157] Hardy G H and Wright E M 1979 *An introduction to the theory of numbers* (Clarendon Press, Oxford)
- [158] Haroche S and Raimond J-M 1996 Quantum computing: dream or nightmare? Phys. Today August 51-52
- [159] Hellman M E 1979 The mathematics of public-key cryptography, Scientific American **241** August 130-139
- [160] Hill R 1986 *A first course in coding theory* (Clarendon Press, Oxford)
- [161] Hodges A 1983 *Alan Turing: the enigma* (Vintage, London)
- [162] Hughes R J, Alde D M, Dyer P, Luther G G, Morgan G L and Schauer M 1995 Quantum cryptography, Contemp. Phys. **36** 149-163
- [163] Hungerford T W, 1974 *Algebra* (Springer-Verlag, New York)

- [164] Jones D S 1979 *Elementary information theory* (Clarendon Press, Oxford)
- [165] A. J. Jones, M. Mosca and R. H. Hansen, Implementation of a Quantum Search Algorithm on a Nuclear Magnetic Resonance Quantum Computer, in *Nature* 393 (1998) 344-346, and see also A. J. Jones and M. Mosca, Implementation of a Quantum Algorithm to Solve Deutsch's Problem on a Nuclear Magnetic Resonance Quantum Computer, in *J. Chem. Phys.* 109 (1998) 1648-1653
- [166] Jozsa R and Schumacher B 1994 A new proof of the quantum noiseless coding theorem, *J. Mod. Optics* **41** 2343
- [167] Jozsa R 1997 Entanglement and quantum computation, appearing in *Geometric issues in the foundations of science*, Huggett S *et. al.*, eds, (Oxford University Press)
- [168] Jozsa R 1997 Quantum algorithms and the Fourier transform, submitted to *Proc. Santa Barbara conference on quantum coherence and decoherence* (preprint quant-ph/9707033)
- [169] Khalfin L A and Tsirelson B S, Quantum/Classical Correspondence in the Light of Bell's Inequalities. *Foundations of physics*, **22** No. 7, 879–948 July 1992

- [170] Lord Kelvin, differential analyzer (1870),
presented in the Science Museum of Aarhus,
Denmark (1998)
- [171] Keyes R W and Landauer R 1970 IBM J. Res.
Develop. **14**, 152
- [172] Keyes R W Science **168**, 796, 1970
- [173] Kholevo A S 1973 Probl. Peredachi Inf **9**, 3;
Probl. Inf. Transm. (USSR) **9**, 177
- [174] Kitaev A Yu, Quantum Computations:
Algorithms and Error Corrections, in *Russian
Math. Surveys*, **52**:6, 1191-1249
- [175] Kitaev A Yu, Quantum measurements and the
Abelian stablizer problem, in *LANL e-print*
quant-ph/9511026, <http://xxx.lanl.gov> (1995)
- [176] Kitaev. A. Yu Quantum error correction with
imperfect gates, *Quantum Communication,
Computing, and Measurement*, eds: Hirota,
Holevo and Caves, 181–188, Plenum Press, New
York, 1997.
- [177] Kitaev A Yu 1997 Fault-tolerant quantum
computation by anyons, in *LANL e-print*
quant-ph/9707021, <http://xxx.lanl.gov> (1997)
- [178] A. Yu. Kitaev, private communication

- [179] Knill E and Laflamme R, Concatenated quantum codes, in *LANL e-print* quant-ph/9608012, <http://xxx.lanl.gov> (1996)
- [180] Knill E, Laflamme R, and Zurek W, Resilient quantum computation, *Science*, vol 279, p.342, 1998.
- [181] Knill E and Laflamme R 1997 A theory of quantum error-correcting codes, *Phys. Rev. A* **55** 900-911
- [182] Knill E, Laflamme R and Zurek W H 1997 Resilient quantum computation: error models and thresholds
<http://xxx.lanl.gov/abs/quant-ph/9702058>
- [183] E. Knill, Non-Binary Unitary Error Bases and Quantum Codes, in *LANL e-print* quant-ph/9608048, <http://xxx.lanl.gov> (1996)
- [184] Knuth D E 1981 *The Art of Computer Programming, Vol. 2: Seminumerical Algorithms*, 2nd ed (Addison-Wesley).
- [185] Kondacs A and Watrous J On the power of Quantum Finite State Automata *38th Annual Symposium on Foundations of Computer Science*,(FOCS) 1997

- [186] Kwiat P G, Mattle K, Weinfurter H, Zeilinger A, Sergienko A and Shih Y 1995 New high-intensity source of polarization-entangled photon pairs Phys. Rev. Lett. **75**, 4337-4341
- [187] R. Laflamme, E. Knill, W.H. Zurek, P. Catasti and S. Marathan. quant-ph/9709025, 1997.
- [188] Laflamme R, Miquel C, Paz J P and Zurek W H 1996 Perfect quantum error correcting code, Phys. Rev. Lett. **77**, 198-201
- [189] Landauer R. Is quantum mechanics useful? *Phil. Trans. Roy. Soc. of London*, 353:367–376, 1995.
- [190] Landauer R 1961 IBM J. Res. Dev. **5** 183, and 1970 IBM J. Res. Dev, volume 14, page 152.
- [191] Landauer R 1991 Information is physical, Phys. Today May 1991 23-29
- [192] Landauer R 1996 The physical nature of information, Phys. Lett. A **217** 188
- [193] Lecerf Y 1963 Machines de Turing réversibles . Réursive insolubilité en $n \in N$ de l'équation $u = \theta^n u$, où θ est un isomorphisme de codes, C. R. Acad. Francaise Sci. **257**, 2597-2600

- [194] Leung D W, Nielsen M A, Chuang I L and Yamamoto Y, Approximate quantum error correction can lead to better codes in *Phys. Rev. A*, **56**, 1, 2567–2573, 1997
- [195] Levitin L B 1987 in *Information Complexity and Control in Quantum Physics*, Blaquiéve A, Diner S, Lochak G, eds (Springer, New York) 15-47
- [196] Lidar D A and Biham O 1996 Simulating Ising spin glasses on a quantum computer (preprint quant-ph/9611038)
- [197] van Lint J H Coding Theory, Springer-Verlag, 1982
- [198] Lipton R J, Using DNA to solve NP-complete problems. *Science*, **268** 542–545, Apr. 28, 1995
- [199] Lloyd S, Universal quantum simulators, *Science*, 273:1073–1078, 1996.
- [200] Lloyd S 1993 A potentially realisable quantum computer, *Science* **261** 1569; see also *Science* **263** 695 (1994).
- [201] Lloyd S 1995 Almost any quantum logic gate is universal, *Phys. Rev. Lett.* **75**, 346-349
- [202] Lloyd S 1997 The capacity of a noisy quantum channel, *Phys. Rev. A* **55** 1613-1622

- [203] Lo H-K and Chau H F 1997 Is quantum bit commitment really possible?, *Phys. Rev. Lett.* **78** 3410-3413
- [204] Loss D and DiVincenzo D P Quantum Computation with Quantum Dots, in *Phys. Rev. A*, **57**, 1, pp. 120-126, 1997
- [205] MacWilliams F J and Sloane N J A 1977 *The theory of error correcting codes*, (Elsevier Science, Amsterdam)
- [206] Majumder et.al *Phys. rev.lett.* 65 2931 (1990)
- [207] Mattle K, Weinfurter H, Kwiat P G and Zeilinger A 1996 Dense coding in experimental quantum communication, *Phys. Rev. Lett.* **76**, 4656-4659.
- [208] Margolus N 1986 Quantum computation, *Ann. New York Acad. Sci.* **480** 487-497
- [209] Margolus N 1990 Parallel Quantum Computation, in *Complexity, Entropy and the Physics of Information, Santa Fe Institute Studies in the Sciences of Complexity*, vol VIII p. 273 ed Zurek W H (Addison-Wesley)
- [210] Maxwell J C 1871 *Theory of heat* (Longmans, Green and Co, London)

- [211] Mayers D 1997 Unconditionally secure quantum bit commitment is impossible, *Phys. Rev. Lett.* **78** 3414-3417
- [212] Mayers D 1997 secure key distribution
- [213] Menezes A J, van Oorschot P C and Vanstone S A 1997 *Handbook of applied cryptography* (CRC Press, Boca Raton)
- [214] Mermin N D 1990 What's wrong with these elements of reality? *Phys. Today* (June) 9-11
- [215] Meyer D A 1996 Quantum mechanics of lattice gas automata I: one particle plane waves and potentials, (preprint quant-ph/9611005)
- [216] Minsky M L 1967 *Computation: Finite and Infinite Machines* (Prentice-Hall, Inc., Englewood Cliffs, N. J.; also London 1972)
- [217] Miquel C, Paz J P and Perazzo 1996 Factoring in a dissipative quantum computer *Phys. Rev. A* **54** 2605-2613
- Miquel C, Paz J P and Zurek W H 1997 Quantum computation with phase drift errors, *Phys. Rev. Lett.* **78** 3971-3974

- [218] Monroe C, Meekhof D M, King B E, Jefferts S R, Itano W M, Wineland D J and Gould P 1995a Resolved-sideband Raman cooling of a bound atom to the 3D zero-pointenergy, *Phys. Rev. Lett.* **75** 4011-4014
- [219] Monroe C, Meekhof D M, King B E, Itano W M and Wineland D J. Demonstration of a universal quantum logic gate, *Phys. Rev. Lett.*, 75:4714-4717, 1995.
- [220] N. F. Mott, The wave Mechanics of α -Ray Tracks, in *Proc. Roy. Soc. London*, A126, 79-84, (1929), and in *Quantum Theory and Measurement*, edited by Wheeler J A and Zurek W H, Princeton Univ. Press, Princeton, NJ (1983)
- [221] Mukamel D, private communication
- [222] Myers J M 1997. Can a universal quantum computer be fully quantum? *Phys. Rev. Lett.* **78**, 1823-1824
- [223] von Neumann, Probabilistic logic and the synthesis of reliable organisms from unreliable components, in *automata studies*(*Shanon, McCarthy eds*), 1956
- [224] Nisan N and Szegedy M, On the degree of Boolean functions as real polynomials, *Proc. of the 24th Annual ACM Symposium on Theory of Computing (STOC)* 1992

- [225] Nielsen M A and Chuang I L 1997
Programmable quantum gate arrays, *Phys. Rev. Lett.* **79**, 321-324

- [226] Palma G M, Suominen K-A & Ekert A K 1996
Quantum computers and dissipation, *Proc. Roy. Soc. Lond. A* **452** 567-584

- [227] Papadimitriou C H, *Computational Complexity*, Addison-Wesley, 1994

- [228] *J. Mod. Opt.* **41**, no 12 1994 Special issue: quantum communication

- [229] See also in this context: Y. Ozhigov, Quantum computers cannot speed up iterated applications of a black box, in *LANL e-print* quant-ph/9712051, <http://xxx.lanl.gov> (1997)

- [230] Pellizzari T, Gardiner S A, Cirac J I and Zoller P 1995 Decoherence, continuous observation, and quantum computing: A cavity QED model, *Phys. Rev. Lett.* **75** 3788-3791

- [231] Peres A 1993 *Quantum theory: concepts and methods* (Kluwer Academic Press, Dordrecht)

- [232] Phoenix S J D and Townsend P D 1995
Quantum cryptography: how to beat the code breakers using quantum mechanics, *Contemp. Phys.* **36**, 165-195

- [233] , Pippenger and Stamoulis and Tsitsiklis, On a Lower Bound for the Redundancy of Reliable Networks with Noisy Gates, in *IEEE TIT: IEEE Transactions on Information Theory*, volume 37, 1991

- [234] Plenio M B and Knight P L 1996 Realistic lower bounds for the factorization time of large numbers on a quantum computer, *Phys. Rev. A* **53**, 2986-2990.

- [235] Polkinghorne J 1994 *Quarks, chaos and Christianity* (Triangle, London)

- [236] J. Preskill. *Proc. Roy. Soc. of London A*, in press.

- [237] Preskill J 1997 Fault tolerant quantum computation, to appear in *Introduction to Quantum Computation*, edited by H.-K. Lo, S. Popescu, and T. P. Spiller
<http://xxx.lanl.gov/abs/quant-ph/9712048>

- [238] Preskill J, Kitaev A, Course notes for Physics 229, Fall 1998, Caltech Univ.,
<http://www.theory.caltech.edu/people/preskill/ph229>

- [239] Privman V, Vagner I D and Kventsel G 1997 Quantum computation in quantum-Hall systems, in *Phys. Lett. A*, 239 (1998) 141-146

- [240] Rabin M O, Probabilistic Algorithms *Algorithms and Complexity: New Directions and Recent Results*, pp. 21-39, Academic Press, 1976.
- [241] Rains E, Nonbinary quantum codes, (quant-ph/9703048)
- [242] Rains E, Hardin R H, Shor P W and Sloane N J A, A non additive quantum code, Phys.Rev.Lett. 79 953–954 1997
- [243] Rieffel E, Polak W An Introduction to Quantum Computing for Non-Physicists
<http://xxx.lanl.gov/abs/quant-ph/9809016>
- [244] Rivest R, Shamir A and Adleman L 1979 On digital signatures and public-key cryptosystems, MIT Laboratory for Computer Science, Technical Report, MIT/LCS/TR-212
- [245] J.J.Saqrui Modern Quantum Mechanics, revised edition. Addison Wesley, 1994
- [246] Schroeder M R 1984 *Number theory in science and communication* (Springer-Verlag, Berlin Heidelberg)
- [247] Schumacher B 1995 Quantum coding, Phys. Rev. A **51** 2738-2747

- [248] L. J. Schulman and U. Vazirani in *LANL e-print* quant-ph/9804060, <http://xxx.lanl.gov> (1998),
- [249] Schumacher B W and Nielsen M A 1996
Quantum data processing and error correction
Phys Rev A **54**, 2629
- [250] Shamir A 1979 Factoring Numbers in $O(\log(n))$
Arithmetic Steps, in *Information Processing*
Letters 8(1) 28-31.
- [251] Shankar R 1980 *Principles of quantum*
mechanics (Plenum Press, New York)
- [252] Shannon C E 1948 A mathematical theory of
communication *Bell Syst. Tech. J.* **27** 379; also
p. 623
- [253] Shor P W, Polynomial-time algorithms for prime
factorization and discrete logarithms on a
quantum computer, *SIAM J. Comp.*, **26**, No. 5,
pp 1484–1509, October 1997
- [254] Shor P W, Scheme for reducing decoherence in
quantum computer memory, *Phys. Rev. A*, 52:
2493-2496, 1995.
- [255] Shor P W, Fault tolerant quantum computation,
In *Proceedings of the 37th Symposium on the*
Foundations of Computer Science, pages 56–65,
Los Alamitos, California, 1996. IEEE press.
quant-ph/9605011.

- [256] Shor P W and Laflamme R 1997 Quantum analog of the MacWilliams identities for classical coding theory, *Phys. Rev. Lett.* **78** 1600-1602
- [257] Simon J On feasible numbers, in *Proc. of the 9th Annual ACM Symposium on Theory of Computing (STOC)* 195-207, 1977
- [258] Simon D 1994 On the power of quantum computation, *SIAM J. Comp.*, **26**, No. 5, pp 1474–1483, October 1997
- [259] Simon D 1998, private communication.
- [260] Slepian D 1974 ed, *Key papers in the development of information theory* (IEEE Press, New York)
- [261] R Solovay and A. C-C Yao, preprint, 1996
- [262] Spiller T P 1996 Quantum information processing: cryptography, computation and teleportation, *Proc. IEEE* **84**, 1719-1746
- [263] Steane A, Multiple particle interference and quantum error correction, *Proc. Roy. Soc. of London A*, 452:2551-2577, 1996.

- [264] Steane A M, Error correcting codes in quantum theory, Phys. Rev. Lett. **77** 793-797, 1996, Simple quantum error-correcting codes, Phys. Rev. A **54**, 4741-4751, 1996, Quantum Reed-Muller codes, submitted to IEEE Trans. Inf. Theory (preprint in *LANL e-print* quant-ph/9608026, <http://xxx.lanl.gov>) Active stabilization, quantum computation, and quantum state synthesis, Phys. Rev. Lett. **78**, 2252-2255, 1997
- [265] Steane A, Quantum Computation, Reports on Progress in Physics 61 (1998) 117, preprint in <http://xxx.lanl.gov/abs/quant-ph/9708022>
- [266] Steane A M The ion trap quantum information processor, Appl. Phys. B **64** 623-642 1997
- [267] Steane A M Space, time, parallelism and noise requirements for reliable quantum computing, in *Fortsch. Phys.* **46** (1998) 443-458
- [268] Stern A, Aharonov Y and Imry Y, "Phase uncertainty and loss of interference: a general picture" Phys. Rev. A **41**, 3436 (1990). and "Dephasing of interference by a back reacting environment" in "Quantum coherence" ed. J. Anandan, World Scientific, 1990.
- [269] Szilard L 1929 Z. Phys. **53** 840; translated in Wheeler and Zurek (1983).

- [270] Teich W G, Obermayer K and Mahler G 1988 Structural basis of multistationary quantum systems II. Effective few-particle dynamics, *Phys. Rev. B* **37** 8111-8121
- [271] W. Tittel, J. Brendel, B. Gisin, T. Herzog, H. Zbinden, N. Gisin Experimental demonstration of quantum-correlations over more than 10 kilometers, in *Phys. Rev. A*, **57**, 3229 (1998)
- [272] Toffoli T 1980 Reversible computing, in *Automata, Languages and Programming*, Seventh Colloquium, Lecture Notes in Computer Science, Vol. 84, de Bakker J W and van Leeuwen J, eds, (Springer) 632-644
- [273] Turchette Q A, Hood C J, Lange W, Mabushi H and Kimble H J 1995 Measurement of conditional phase shifts for quantum logic, *Phys. Rev. Lett.* **75** 4710-4713
- [274] Turing A M 1936 On computable numbers, with an application to the Entscheidungsproblem, *Proc. Lond. Math. Soc. Ser. 2* **42**, 230 ; see also *Proc. Lond. Math. Soc. Ser. 2* **43**, 544
- [275] Unruh W G, Maintaining coherence in quantum computers, *Phys. Rev. A*, 51:992–997, 1995.
- [276] Valiant, unpublished

- [277] Valiant L. G, Negation can be exponentially powerful. *Theoretical Computer Science*, 12(3):303-314, November 1980.
- [278] Valiant L G and Vazirani V V. NP is as easy as detecting unique solutions. *Theoretical Computer Science*, 47(1):85-93, 1986
- [279] Vedral V, Barenco A and Ekert A 1996 Quantum networks for elementary arithmetic operations, *Phys. Rev. A* **54** 147-153
- [280] Vergis A, Steiglitz K and Dickinson B , "The Complexity of Analog Computation", *Math. Comput. Simulation* 28, pp. 91-113. 1986
- [281] Walsworth et.al. *Phys rev. lett.* 64,2599, 1990.
- [282] Warren W S, *Science*, 277:1688–1698, 1997.
- [283] Watrous J, On one Dimensional quantum cellular automata, *Complex Systems* **5** (1), pp 19–30, 1991
- [284] Weinfurter H 1994 Experimental Bell-state analysis, *Europhys. Lett.* **25** 559-564
- [285] Wiesner S 1983 Conjugate coding, *SIGACT News* **15** 78-88

- [286] Wiesner S 1996 Simulations of many-body quantum systems by a quantum computer in *LANL e-print* quant-ph/9603028, <http://xxx.lanl.gov> (1996)
- [287] Wheeler J A and Zurek W H, eds, 1983 *Quantum theory and measurement* (Princeton Univ. Press, Princeton, NJ)
- [288] A. Wigderson, private communication
- [289] Wineland D J, Monroe C, Itano W M, Leibfried D, King B, and Meekhof D M 1997 Experimental issues in coherent quantum-state manipulation of trapped atomic ions, preprint, submitted to Rev. Mod. Phys.
- [290] Wootters W K and Zurek W H 1982 A single quantum cannot be cloned, *Nature* **299**, 802
- [291] Wootters W K A Measure of the Distinguishability of Quantum States *Quantum Optics, General Relativity, and Measurement* eds: Marlan O. Scully and Pierre Meystre, 145–154, Plenum Press, New York, 1983
- [292] Yao A C-C, Quantum circuit complexity, in *33th Annual Symposium on Foundations of Computer Science(FOCS)*, (1993) pp. 352–361

- [293] Zalka C, Efficient simulation of quantum systems by quantum computers *Proc. Roy. Soc. of London A*, in press, in *LANL e-print* quant-ph/9603026, <http://xxx.lanl.gov> (1996)
- [294] Zalka C, Grover's quantum searching algorithm is optimal,
<http://xxx.lanl.gov/abs/quant-ph/9711070>
- [295] Zbinden H, Gautier J D, Gisin N, Huttner B, Muller A, Tittle W 1997 Interferometry with Faraday mirrors for quantum cryptography, *Elect. Lett.* **33**, 586-588
- [296] Zurek W H, Decoherence and the transition from quantum to classical, *Physics Today* 44(10), October, 1991 36–44.
- [297] Zurek W H 1989 Thermodynamic cost of computation, algorithmic complexity and the information metric, *Nature* **341** 119-124

[To top ←](#)

Selected on-line references

Some of the references listed above are available on line. A few are listed again here for easy access:

Abrams D S and Lloyd S, Non-Linear Quantum Mechanics implies Polynomial Time solution for NP-complete and #P problems,

<http://xxx.lanl.gov/abs/quant-ph/9801041>

Aharonov D, Beckman D, Chuang I and Nielsen M, What Makes Quantum Computers Powerful?

<http://wwwcas.phys.unm.edu/~nielsen/science.html>

Chuang I L, Laflamme R and Paz J P, Effects of Loss and Decoherence on a Simple Quantum Computer,

<http://xxx.lanl.gov/abs/quant-ph/9602018>

Grover L K, A framework for fast quantum mechanical algorithms, <http://xxx.lanl.gov/abs/quant-ph/9711043>

Grover L K, A fast quantum mechanical algorithm for estimating the median,

<http://xxx.lanl.gov/abs/quant-ph/9607024>

Knill E, Laflamme R and Zurek W H 1997 Resilient quantum computation: error models and thresholds

<http://xxx.lanl.gov/abs/quant-ph/9702058>

Preskill J 1997 Fault tolerant quantum computation, to appear in *Introduction to Quantum Computation*, edited by H.-K. Lo, S. Popescu, and T. P. Spiller

<http://xxx.lanl.gov/abs/quant-ph/9712048>

Preskill J, Kitaev A, Course notes for Physics 229, Fall 1998, Caltech Univ.,

<http://www.theory.caltech.edu/people/preskill/ph229>

Rieffel E, Polak W An Introduction to Quantum Computing for Non-Physicists

<http://xxx.lanl.gov/abs/quant-ph/9809016>

Steane A, Quantum Computation, Reports on Progress in Physics 61 (1998) 117,

<http://xxx.lanl.gov/abs/quant-ph/9708022>

Zalka C, Grover's quantum searching algorithm is optimal, <http://xxx.lanl.gov/abs/quant-ph/9711070>

[To top ←](#)