Quantum-Computing

SS 2002

Claudius Gros
Institut für Theoretische Physik
Universität des Saarlandes

überarbeitetes Skript, mit freundlicher Genehmigung von Prof. Dr. J. Stolze
und von Prof. Dr. H. Suter,
Fachbereich Physik, Universität Dortmund

Contents

1 Introduction and Survey **4**
- 1.1 Motivation: why quantum computers . . . 4
- 1.2 History of quantum information processing . . . 5
- 1.3 Quantum communication . . . 7
- 1.4 Quantum computer: principle of operation . . . 8
- 1.5 Some quantum mechanics . . . 10
  - 1.5.1 Vectors in Hilbert space . . . 10
  - 1.5.2 Operators in Hilbert space . . . 11
  - 1.5.3 Dynamics: The Schrödinger equation . . . 12
  - 1.5.4 The two-dimensional Hilbert space: Qubits and Spins . . . 14
  - 1.5.5 Two qubits and the density matrix . . . 17
  - 1.5.6 No cloning theorem . . . 19

2 Elements of classical computer science **21**
- 2.1 Bits of History . . . 21
- 2.2 Boolean algebra and logic gates . . . 21
  - 2.2.1 Minimum set of irreversible gates . . . 23
  - 2.2.2 Minimum set of reversible gates . . . 25
- 2.3 The Turing machine as a universal computer . . . 27
- 2.4 The von Neumann machine . . . 28
- 2.5 Complexity and complexity classes . . . 29

3 Physical limitations to computations **32**
- 3.1 Information and Thermodynamics . . . 32
- 3.2 Reversible Logic . . . 36
- 3.3 The ultimate Laptop . . . 37

4 Elements of quantum information theory **40**
- 4.1 Elementary quantum logical gates . . . 41
  - 4.1.1 Unary qubit gates . . . 42
  - 4.1.2 Binary qubit gates . . . 42
  - 4.1.3 3-Qubit Gates . . . 44
- 4.2 The generic single-qubit gate . . . 45
  - 4.2.1 SU-rotations . . . 46
  - 4.2.2 Representation of the generic single-qubit operator . . . 47
- 4.3 Controlled gates . . . 48
- 4.4 Universal quantum gates . . . 48
  - 4.4.1 (i) Two-level gates are universal . . . 49
  - 4.4.2 (ii) Single-qubit and CNOT gates are universal . . . 50
  - 4.4.3 (iii) Hadamard, phase and $\frac{\pi}{8}$ are (approximately) universal single-qubit gates . . . 50

5 The quantum computer: principles **52**
5.1 Quantum parallelism 52
5.2 Quantum software vs. quantum hardware 53
5.2.1 Time-dependent activation of quantum gates. 54
5.2.2 Fixed-wired quantum circuits 55
5.3 Quantum hardware 56
5.3.1 Creation and anhilation operators 56
5.3.2 Hamiltonians do not commute gnerally 57
5.3.3 Full time evolution 59

References

[1] Michael Brooks. *Quantum Computing and Communications*. Springer, New York, 1999. 152 pp.

[2] Jozef Gruska. *Quantum computing*. McGraw-Hill, London, 2000. 439 pp.

[3] Michael A. Nielsen and Isaac L. Chuang. *Quantum computation and quantum information*. Cambridge Univ. Press, Cambridge, 2001. 676 pp.

[4] Colin P. Williams and Scott H. Clearwater. *Explorations in quantum computing*. Springer, New York, 1998. 307 pp, CD-ROM, DM 98.00.

[5] A. Steane. Quantum computing. *Rep. Prog. Phys.*, 61:117–173, 1998.

[6] Dorit Aharonov. Quantum computation. In Dietrich Stauffer, editor, *Annual Reviews of Computational Physics VI*, pages 259–346. World Scientific, 1999. Preprint quant-ph/9812037.

[7] A. Galindo and M. A. Martin-Delgado. Information and computation: Classical and quantum aspects, 2002. Rev. Mod. Phys., to appear. Preprint quant-ph/0112105.

[8] John Preskill. Quantum computation. http://theory.caltech.edu/ preskill/ph229/, 1997. 413 pp.

[9] Paul Benioff. Quantum mechanical Hamiltonian models of Turing machines. *J. Stat. Phys.*, 29:515, 1982.

[10] Y. Lecerf. Machines de Turing reversibles. Compters Rendus **257**, 1597, 1963.

[11] Richard P. Feynman. Simulating physics with computers. *Int. J. Theor. Phys.*, 21:467–488, 1982.

[12] Peter Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. In *Proceedings, 35th Annual Symposium on Foundations of Computer Science*, Piscataway, NJ, 1994. IEEE Press.

[13] Stephan Mertens. Computational complexity for physicists. Lecture given at the DPG school on "Quantum Computing", 2000. Preprint cond-mat/0012185.

[14] Barenco, A., C.H. Bennett, R. Cleve, D.P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J.A. Smolin, H. Weinfurter. *"Elementary gates for quantum computation"*, Phys. Rev. A **52**, 3457-3467 (1995).

[15] Barenco, A., D. Deutsch, A. Ekert and R. Jozsa. *"Conditional quantum dynamics and logic gates"*, Phys. Rev. Lett. **74**, 4083-6 (1995).

[16] Alonzo Church. An unsolvable problem of elementary number theory. *Am. J. Math.*, 58:345–363, 1936.

[17] Alan M. Turing. On computable numbers, with an application to the Entscheidungsproblem. *Proc. Lond. Math. Soc. Ser.*, 42:230, 1936. See also ibidem 43, 544.

[18] Douglas R. Hofstadter. *Gdel, Escher, Bach: An Eternal Golden Braid.* Basic Books, New York, 1979. 777 pp.

[19] Leo Szilard. ber die Entropieverminderung in einem thermodynamischen System bei Eingriffen intelligenter Wesen. *Z. Physik*, 53:840–856, 1929.

[20] R. Landauer. Irreversibility and heat generation in the computing process. *IBM Journal Res Dev*, 5:183–191, 1961.

[21] Seth Lloyd. Ultimate physical limits to computation. *Nature*, 406:1047–1054, 2000.

[22] N. Margolus and L.B. Levitin. title. In T. Toffoli, M. Biafore, and J. Le?o, editors, *Proceedings of the Fourth Workshop on Physics and Computation PhysComp96 (New England Complex Systems Institute, Boston, MA, 1996).* North-Holland, 1998. Physica D Vol. 120.

[23] Richard P. Feynman. *Feynman Lectures on Computing*, chapter 6, Quantum Mechanical Computers. Addison-Wesley, 1996. Originally published in Optics News, February 1985, pp. 11-20; see also Found. Phys. **16**, 507-532 (1986).

[24] P. Jordan and E. Wigner. Über das Paulische Äquivalenzverbot. *Z. Physik*, 47:631–651, 1928.

[25] Jian-Wei Pan, Dik Bouwmeester, Matthew Daniell, Harald Weinfurter, and Anton Zeilinger. Experimental test of quantum nonlocality in three-photon Greenberger-Horne-Zeilinger entanglement. *Nature*, 403:515–519, 2000.

[26] C. A. Sackett, D. Kielpinski, B. E. King, C. Langer, V. Meyer, C. J. Myatt, M. Rowe, Q. A. Turchette, W. M. Itano, D. J. Wineland, and C. Monroe. Experimental entanglement of four particles. *Nature*, 404:256–259, 2001.

[27] Rainer Blatt. Push-button entanglement. *Nature*, 404:231–232, 2001.

[28] Brian Julsgaard, Alexander Kozhekin, and Eugene S. Polzik. Experimental long-lived entanglement of two macroscopic objects. *Nature*, 413:400–403, 2001.

[29] J. Ignacio Cirac. Quantum physics: Entangled atomic samples. *Nature*, 413:375–377, 2001.

[30] L. Grover. (title). In *Proc. 28th Annual ACM Symposium on the Theory of Computation*, pages 212–219, New York, 1996. ACM Press.

[31] L.K. Grover. Quantum mechanics helps in searching for a needle in a haystack. *Phys. Rev. Lett.*, 79:325–328, 1997. Preprint quant-ph/9706033.

[32] P. Oscar Boykin, Tal Mor, Matthew Pulver, Vwani Roychowdhury, and Farrokh Vatan. On universal and fault-tolerant quantum computing, 1999. Preprint quant-ph/9906054.

[33] D.P. DiVincenzo. The physical implementation of quantum computation. *Fortschr. Phys.*, 48:771–783, 2000. Preprint quant-ph/0002077.

[34] C.E. Hughes and S. Wimperis. Bounds on spin dynamics and the design of multiple-pulse NMR experiments. *J. Chem. Phys.*, 106:2105–2117, 1997.

[35] J. Stoustrup, O. Schedletzky, S.J. Glaser, C. Griesinger, N.C. Nielsen, and O.W. Sorensen. Generalized bound on quantum dynamics: efficiency of unitary transformations between non-hermitian states. *Phys. Rev. Lett.*, 74:2921–2924, 1995.

[36] J. H. Smet, R. A. Deutschmann, F. Ertl, W. Wegscheider, G. Abstreiter, and K. von Klitzing. Gate-voltage control of spin interactions between electrons and nuclei in a semiconductor. *Nature*, 415:281–286, 2002.

[37] J. Kikkawa. Eavesdropping on spin talk. *Nature*, 415:273–274, 2002.

[38] W.K. Wootters and W.H. Zurek. A single quantum cannot be cloned. *Nature*, 299:802–803, 1982.

[39] D. Dieks. Communication by EPR devices. *Phys. Lett. A*, 92:271–271, 1982.

[40] C.H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. Wootters. Teleporting an unknown quantum state via dual classical and EPR channels. *Phys. Rev. Lett.*, 70:1895–1899, 1993.

[41] C.H. Bennettr. Logical reversability of computation. *IBM J. Res. Dev.* **17**, 525-532, 1973.

[42] C.H. Bennett and S.J. Wiesner. Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states. *Phys. Rev. Lett.*, 69:2881–2884, 1992.

[43] C.H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing (Bangalore, India, December 1984)*, pages 175–179, New York, 1984. IEEE.

[44] H. Zbinden, J.D. Gautier, N. Gisin, B. Huttner, A. Muller, and W. Tittle. Interferometry with Faraday mirrors and quantum cryptography. *Electron. Lett.*, 33:586–588, 1997.

[45] C.H. Bennett, G. Brassard, and N.D. Mermin. Quantum cryptography without Bell's theorem. *Phys. Rev. Lett.*, 68:557–559, 1992.

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

[47] D.A. Lidar, I.L. Chuang, and K.B. Whaley. Decoherence-free subspaces for quantum computation. *Phys. Rev. Lett.*, 81:2594–2597, 1998.

[48] E. Knill, R. Laflamme, and L. Viola. Theory of quantum error correction for general noise. *Phys. Rev. Lett.*, 84:2525–2528, 2000.

[49] L. Viola, E.M. Fortunato, M.A. Pravia, E. Knill, R. Laflamme, and D.G. Cory. Experimental realization of noiseless subsystems for quantum information processing. *Science*, 293:2059–2063, 2001.