Classical and Quantum Computation

A. Yu. Kitaev
A. H. Shen
M. N. Vyalyi

Graduate Studies in Mathematics
Volume 47

American Mathematical Society

http://dx.doi.org/10.1090/gsm/047

Classical and Quantum Computation

A. Yu. Kitaev
A. H. Shen
M. N. Vyalyi

Graduate Studies
in Mathematics
Volume 47

American Mathematical Society
Providence, Rhode Island

А. Китаев, А. Шень, М. Вялый

КЛАССИЧЕСКИЕ И КВАНТОВЫЕ ВЫЧИСЛЕНИЯ

МЦНМО–ЧеРо, Москва, 1999

Translated from the Russian by Lester J. Senechal

2000 *Mathematics Subject Classification*. Primary 81–02, 68–02;
Secondary 68Qxx, 81P68.

Abstract. The book is an introduction to a new rapidly developing topic: theory of quantum computing. The authors begin with a brief description of complexity theory for classical computations. Then they give a detailed presentation of the basics of quantum computing, including all known efficient quantum algorithms.

The book can be used by graduate and advanced undergraduate students and by researchers working in mathematics, quantum physics, and communication.

For additional information and updates on this book, visit
www.ams.org/bookpages/gsm-47

Library of Congress Cataloging-in-Publication Data

Kitaev, A. Yu. (Alexei Yu.), 1963–
Classical and quantum computation / A. Yu. Kitaev, A. H. Shen, M. N. Vyalyi ; [translated from the Russian by Lester J. Senechal].
p. cm. — (Graduate studies in mathematics, ISSN 1065-7339 ; v. 47)
Includes bibliographical references and index.
ISBN 0-8218-2161-X (acid-free paper) ISBN 0-8218-3229-8 (softcover)
1. Machine theory. 2. Computational complexity. 3. Quantum computers. I. Shen, A. (Alexander), 1958– II. Vyalyi, M. N. (Mikhail N.), 1961– III. Title. IV. Series.
QA267.K57 2002
530.12—dc21 2002016686

---

10 9 8 7 6 5 4 3 2 18 17 16 15 14 13

Contents

Foreword

In recent years interest in what is called "quantum computers" has grown extraordinarily. The idea of using the possibilities of quantum mechanics in organizing computation looks all the more attractive now that experimental work has begun in this area.

However, the prospects for physical realization of quantum computers are presently entirely unclear. Most likely this will be a matter of several decades. The fundamental achievements in this area bear at present a purely mathematical character.

This book is intended for a first acquaintance with the mathematical theory of quantum computation. For the convenience of the reader, we give at the outset a brief introduction to the classical theory of computational complexity. The second part includes the descriptions of basic effective quantum algorithms and an introduction to quantum codes.

The book is based on material from the course "Classical and quantum computations", given by A. Shen (classical computations) and A. Kitaev (quantum computations) at the Independent Moscow University in Spring of 1998. In preparing the book we also used materials from the course Physics 229 — Advanced Mathematical Methods of Physics (Quantum Computation) given by John Preskill and A. Kitaev at the California Institute of Technology in 1998–99 (solutions to some problems included in the course were proposed by Andrew Landahl). The original version of this book was published in Russian [**37**], but the present edition extends it in many ways.

The prerequisites for reading this book are modest. In essence, it is enough to know the basics of linear algebra (as studied in a standard university course), elementary probability, basic notions of group theory, and a

few concepts from the theory of algorithms (some computer programming experience may do as well as the formal knowledge). Some topics require an acquaintance with Lie groups and homology of manifolds — but only at the level of definitions.

To reduce the amount of information the reader needs to digest at the first reading, part of the material is given in the form of *problems* and *solutions*. Each problem is assigned a grade according to its difficulty: 1 for an exercise in use of definitions, 2 for a problem that requires some work, 3 for a difficult problem which requires a nontrivial idea. (Of course, the difficulty of a problem is a subjective thing. Also, if several problems are based on the same idea, only the first of them is marked as difficult). The grade appears in square brackets before the problem number. Some problems are marked with an exclamation sign, which indicates that they are almost as important as the main text. Thus, [1!] means an easy but important exercise, whereas [3] is a difficult problem which is safe to skip.

Further reading

In this book we focus on algorithm complexity (in particular, for quantum algorithms), while many related things are not covered. As a general reference on quantum information theory we recommend the book by Michael Nielsen and Isaac Chuang [**51**], which includes such topics as the von Neumann entropy, quantum communication channels, quantum cryptography, fault-tolerant computation, and various proposed schemes for the realization of a quantum computer. Another book on quantum computation and information was written by Josef Gruska [**30**]. Most original papers on the subject can be found in the electronic archive at `http://arXiv.org`, section "Quantum Physics" (`quant-ph`).

Acknowledgements

A. K. thanks Michael Freedman and John Preskill for many inspiring discussions on the topics included in this book. We are grateful to Andrew Landahl for providing the solution to Problem 3.6 and pointing to some inconsistencies in the original manuscript. Among other people who have helped us to improve the book are David DiVincenzo and Barbara Terhal.

Thanks to the people at AMS, and especially to our patient editor Sergei Gelfand and the copy-editor Natalya Pluzhnikov, for their help in bringing this book into reality.

The book was written while A. K. was a member of Microsoft Research and Caltech, and while A. S. and M. V. were members of Independent Moscow University. The preparation of the original Russian version was started

while all three of us were working at IMU, and A. K. was a member of L. D. Landau Institute for Theoretical Physics.

A. K. gratefully acknowledges the support from the National Science Foundation through Caltech's Institute for Quantum Informaiton. M. V. acknowledges the support from the Russian Foundation for Basic Research under grant 02–01–00547.

Notation

$\vee$	disjunction (logical OR)
$\wedge$	conjunction (logical AND)
$\neg$	negation
$\oplus$	addition modulo 2 (and also the direct sum of linear subspaces)
$\textcircled{\oplus}$	controlled NOT gate (p. 62)
$\sqcup$	blank symbol in the alphabet of a Turing machine
$\delta(\cdot,\cdot)$	transition function of a Turing machine
δ_{jk}	Kronecker symbol
$\chi_S(\cdot)$	characteristic function of the set S
$f_\oplus$	invertible function corresponding to the Boolean function f (p. 61)
$\overline{x_{n-1}\cdots x_0}$	number represented by binary digits $x_{n-1},\ldots,x_0$
$\gcd(x,y)$	greatest common divisor of x and y
$a \bmod q$	residue of a modulo q
$\boxed{\begin{array}{c}a\\b\end{array}}$	representation of the rational number a/b in the form of an irreducible fraction
$a \mid b$	a divides b
$a \equiv b \pmod q$	a is congruent to b modulo q
$A \Rightarrow B$	A implies B
$A \Leftrightarrow B$	A is logically equivalent to B
$L_1 \propto L_2$	Karp reduction of predicates (L_1 can be reduced to L_2 (p. 30))
$\lfloor x \rfloor$	the greatest integer not exceeding x
$\lceil x \rceil$	the least integer not greater than x

A^*	set of all finite words in the alphabet A
E^*	group of characters on the Abelian group E, i.e., $\mathrm{Hom}(E, \mathbf{U}(1))$
z^*	complex conjugate of z
$\mathcal{M}^*$	space of linear functionals on the space $\mathcal{M}$
$\langle\xi\|$	bra-vector (p. 56)
$\|\xi\rangle$	ket-vector (p. 56)
$\langle\xi\|\eta\rangle$	inner product
$A^\dagger$	Hermitian adjoint operator
$\widehat{G}$	unitary operator corresponding to the permutation G (p. 61)
$I_{\mathcal{L}}$	identity operator on the space $\mathcal{L}$
$\Pi_{\mathcal{M}}$	projection (the operator of projecting onto the subspace $\mathcal{M}$)
$\mathrm{Tr}_{\mathcal{F}} A$	partial trace of the operator A over the space (tensor factor) $\mathcal{F}$ (p. 96)
$A \cdot B$	superoperator $\rho \mapsto A\rho B$ (p. 108)
$\mathcal{M}^{\otimes n}$	n-th tensor degree of $\mathcal{M}$
$\mathbb{C}(a, b, \dots)$	space generated by the vectors $a, b, \dots$
$\Lambda(U)$	operator U with quantum control (p. 65)
$U[A]$	application of the operator U to a quantum register (set of qubits) A (p. 58)
$\mathcal{E}[A]$, $\mathcal{E}(n, k)$	error spaces (p. 156)
$\sigma(\alpha_1, \beta_1, \dots, \alpha_n, \beta_n)$	basis operators on the space $\mathcal{B}^{\otimes n}$ (p. 162)
$\mathrm{SympCode}(F, \mu)$	symplectic code (p. 168)
$\|\cdot\|$	cardinality of a set or modulus of a number
$\|\cdot\|$	norm of a vector (p. 71)
	or operator norm (p. 71)
$\|\cdot\|_{\mathrm{tr}}$	trace norm (p. 98)
$\|\cdot\|_{\diamondsuit}$	superoperator norm (p. 110)
$\mathbf{Pr}[A]$	probability of the event A
$\mathbf{P}(\cdot\,\|\,\cdot)$	conditional probability (in various contexts)
$\mathbf{P}(\rho, \mathcal{M})$	quantum probability (p. 95)
$f(n) = O(g(n))$	there exist numbers C and n_0 such that $f(n) \le Cg(n)$ for all $n \ge n_0$
$f(n) = \Omega(g(n))$	there exist numbers C and n_0 such that $f(n) \ge Cg(n)$ for all $n \ge n_0$
$f(n) = \Theta(g(n))$	$f(n) = O(g(n))$ and $f(n) = \Omega(g(n))$ at the same time
$f(n) = \mathrm{poly}(n)$	means the same as $f(n) = n^{O(1)}$
$\mathrm{poly}(n, m)$	abbreviation for $\mathrm{poly}(n + m)$

$\mathbb{N}$	set of natural numbers, i.e., $\{0, 1, 2, \dots\}$
$\mathbb{Z}$	set of integers
$\mathbb{R}$	set of real numbers
$\mathbb{C}$	set of complex numbers
$\mathbb{B}$	classical bit (set $\{0, 1\}$)
$\mathcal{B}$	quantum bit (qubit, space $\mathbb{C}^2$ — p. 53)
$\mathbb{F}_q$	finite field of q elements
$\mathbb{Z}/n\mathbb{Z}$	ring of residues modulo n
$\mathbb{Z}_n$	additive group of the ring $\mathbb{Z}/n\mathbb{Z}$
$(\mathbb{Z}/n\mathbb{Z})^*$	multiplicative group of invertible elements of $\mathbb{Z}/n\mathbb{Z}$
$\mathrm{Sp}_2(n)$	symplectic group of order n over the field $\mathbb{F}_2$ (p. 165)
$\mathrm{ESp}_2(n)$	extended symplectic group of order n over the field $\mathbb{F}_2$ (p. 164)
$\mathbf{L}(\mathcal{N})$	space of linear operators on $\mathcal{M}$
$\mathbf{L}(\mathcal{N}, \mathcal{M})$	space of linear operators from $\mathcal{N}$ to $\mathcal{M}$
$\mathbf{U}(\mathcal{M})$	group of unitary operators in the space $\mathcal{M}$
$\mathbf{SU}(\mathcal{M})$	special unitary group in the space $\mathcal{M}$
$\mathbf{SO}(\mathcal{M})$	special orthogonal group in the Euclidean space $\mathcal{M}$

Notation for matrices:

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \qquad K = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix},$$

Pauli matrices: $\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $\sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$, $\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

Notation for complexity classes:

NC	(p. 23)	NP	(p. 28)	BQP	(p. 91)
P	(p. 14)	MA	(p. 138)	BQNP	(p. 139)
BPP	(p. 36)	Π_k	(p. 46)	PSPACE	(p. 15)
PP	(p. 91)	Σ_k	(p. 46)	EXPTIME	(p. 22)
P/poly	(p. 20)				

Bibliography

[1] J. F. Adams, *Lectures on Lie groups*, W. A. Benjamin, Inc., New York–Amsterdam, 1969.

[2] L. M. Adleman, J. DeMarrais and M. A. Huang, *Quantum computability*, SIAM J. Comput. **26** (1997), 1524–1540.

[3] D. Aharonov and M. Ben-Or, *Fault tolerant quantum computation with constant error*, e-print `quant-ph/9611025`; extended version, e-print `quant-ph/9906129`.

[4] D. Aharonov, A. Kitaev, and N. Nisan, *Quantum circuits with mixed states*, STOC'29, 1997; e-print `quant-ph/9806029`.

[5] A. V. Aho and J. D. Ullman, *Principles of compiler design*, Addison-Wesley, Reading, MA, 1977.

[6] L. Babai and S. Moran, *Arthur–Merlin games: A randomized proof system and a hierarchy of complexity classes*, J. Comput. System Sci. **36** (1988), 254–276.

[7] A. Barenco, C. H. Bennett, R. Cleve, D. P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. Smolin, and H. Weinfurter, *Elementary gates for quantum computation*, Phys. Rev. Ser. **A52** (1995), 3457–3467; e-print `quant-ph/9503016`.

[8] D. A. Barrington, *Bounded-width polynomial-size branching programs recognize exactly those languages in* NC^1, J. Comput. System Sci. **38** (1989), 150–164.

[9] P. Beame, S. Cook, and H. J. Hoover, *Log depth curcuits for division and related problems*, SIAM J. Comput. **15** (1986), 994–1003.

[10] C. H. Bennett, *Logical reversibility of computations*, IBM J. Res. Develop. **17** (1973), 525–532.

[11] C. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. Wootters, *Teleporting an unknown quantum state via dual classical and Einstein–Podolsky–Rosen channel*, Phys. Rev. Lett. **70** (1993), 1895–1899.

[12] C. Bennett, D. DiVincenzo, J. Smolin, and W. Wootters, *Mixed state entanglement and quantum error correction*, Phys. Rev. **A54** (1996), 3824–3851; e-print `quant-ph/9604024`.

[13] D. Boneh and R. Lipton, *Quantum cryptoanalysis of hidden linear functions*, Proc. of Advances in Cryptology—CRYPTO-95, Lecture Notes Computer Science, vol. 963, Springer-Verlag, Berlin, 1995, pp. 424–437.

[14] R. Boppana and M. Sipser, *The complexity of finite functions*, Handbook of Theoretical Computer Science. Volume A, Algorithms and Complexity, Ch. 14. J. van Leeuwen (ed.), Elsevier, Amsterdam; MIT Press, Cambridge, MA, 1990, pp. 757–804.

[15] N. Bourbaki, *Lie Groups and Lie Algebras*, Hermann, Paris, 1971.

[16] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane *Quantum error correction and orthogonal Geometry*, Phys. Rev. Lett. **78** (1997), 405–408; e-print `quant-ph/9605005`.

[17] A. R. Calderbank and P. W. Shor, *Good quantum error-correcting codes exist*, Phys. Rev. **A54** (1996), 1098–1106; e-print `quant-ph/9512032`.

[18] R. Cleve and J. Watrous, *Fast parallel circuits for the quantum Fourier transform*, FOCS'41, 2000, pp. 526–536; e-print `quant-ph/0006004`.

[19] D. Coppersmith, *An approximate Fourier transform useful in quantum factoring*, Technical Report RC19642, IBM, 1994; e-print `quant-ph/0201067`.

[20] D. Deutsch, *Quantum theory, the Church–Turing principle and the universal quantum computer*, Proc. Roy. Soc. London **A400** (1985), 97–117.

[21] ———, *Quantum computational networks*, Proc. Roy. Soc. London. **A425** (1989), 73–90.

[22] P. Erdös and J. Spencer, *Probabilistic methods in combinatorics*, Academic Press, New York, 1974.

[23] R. P. Feynman, *Simulating physics with computers*, Internat. J. Theoret. Phys. **21**(6/7) (1982), 467–488.

[24] ———, *Quantum mechanical computers*, Optics News, **11**, February 1985, p. 11.

[25] L. Fortnow and M. Sipser, *Are there interactive protocols for Co-NP-languages?*, Inform. Process. Lett. **28** (1988), 249–251.

[26] M. H. Freedman, *P/NP, and the quantum field computer*, Proc. Nat. Acad. Sci. U.S.A. **95** (1998), 98–101.

[27] M. H. Freedman and A. Yu. Kitaev, *Diameter of homogeneous spaces*, unpublished.

[28] M. R. Garey and D. S. Johnson, *Computers and intractability*, Freeman, New York, 1983.

[29] L. Grover, *A fast quantum mechanical algorithm for database search*, STOC'28, 1996, pp. 212–219.

[30] J. Gruska, *Quantum Computing*, McGraw-Hill, London, 1999.

[31] A. W. Harrow, B. Recht and I. L. Chuang, *Tight bounds on discrete approximation of quantum gates*, e-print `quant-ph/0111031`.

[32] R. Impagliazzo and A. Wigderson. P = BPP *if* E *requires exponential circuits: Derandomizing the* XOR *lemma*, STOC'29, 1997.

[33] A. J. Khinchin, *Continued fractions*, Univ. of Chicago Press, 1992.

[34] A. A. Kirillov, *Elements of the theory of representations*, Springer-Verlag, New York, 1976.

[35] A. Yu. Kitaev, *Fault-tolerant quantum computation by anyons*, e-print `quant-ph/9707021`.

[36] A. Yu. Kitaev, *Quantum computations: algorithms and error correction*, Uspehi Mat. Nauk **52** (1997), no. 6, 53–112; English transl., Russian Math. Surveys **52** (1997), no. 6, 1191–1249.

[37] A. Kitaev, A. Shen, M. Vyalyi, *Classical and Quantum Computations*, Moscow, 1999 (in Russian); available at `http://www.mccme.ru/free-books`.

[38] A. Yu. Kitaev and J. Watrous, *Parallelization, amplification, and exponential time simulation of quantum interactive systems*, STOC'32, 2000, pp. 608–617.

[39] S. C. Kleene, *Mathematical logic*, Wiley, New York, 1967.

[40] ———, *Introduction to metamathematics*, Van Nostrand, New York, 1952.

[41] E. Knill and R. Laflamme, *A theory of quantum error-correcting codes*, e-print `quant-ph/9604034`.

[42] E. Knill, R. Laflamme, and W. Zurek, *Threshold accuracy for quantum computation*, e-print `quant-ph/9610011`.

[43] D. E. Knuth, *The art of computer programming*, Addison-Wesley, Reading, MA, 1973.

[44] A. I. Kostrikin and Yu. I. Manin, *Linear algebra and geometry*, Nauka, Moscow, 1986; English transl., Gordon and Breach, New York, 1989.

[45] R. Landauer, *Irreversibility and heat generation in the computing process*, IBM J. Res. Develop. **3** (1961), 183–191.

[46] C. Lautemann, *BPP and the polynomial hierarchy*, Inform. Process. Lett. **17** (1983), 215–217.

[47] F. J. MacWilliams and N. J. A. Sloane, *The theory of error correction codes*, North Holland, New York, 1981.

[48] A. I. Maltsev, *Algorithms and recursive functions*, Wolters-Noordhof, Groningen, 1970.

[49] Yu. I. Manin *Computable and Incomputable*, Moscow, 1980 (in Russian).

[50] M. Marcus and H. Minc. *A survey of matrix theory and matrix inequalities*, Allyn and Bacon, Boston, 1964.

[51] M. A. Nielsen and I. L. Chuang *Quantum computation and quantum information*, Cambridge University Press, 2000.

[52] C. H. Papadimitriou and K. Steiglitz, *Combinatorial optimization: algorithms and complexity*, Prentice-Hall, Englewood Cliffs, NJ, 1982.

[53] V. V. Prasolov, *Problems and theorems in linear algebra*, Amer. Math. Soc., Providence, RI, 1994.

[54] H. Rogers, *Theory of recursive functions and effective computability*, MIT Press, Cambridge, MA, 1987.

[55] A. Schrijver, *Theory of linear and integer programming*, Wiley-Interscience, Chichester, NY, 1986.

[56] J. P. Serr, *Lie algebras and Lie groups*, W. A. Benjamin, Inc., New York–Amsterdam, 1965.

[57] I. R. Shafarevich, *Basic notions of algebra*, Springer-Verlag, New York, 1997.

[58] A. Shamir, *IP=PSPACE*, J. ACM **39** (1992), 869–877.

[59] A. Shen, *IP=PSPACE: simplified proof*, J. ACM **39** (1992), 878–880.

[60] J. R. Shoenfield, *Mathematical logic*, Addison-Wesley, Reading, MA, 1967.

[61] ———, *Degrees of unsolvability*, Elsevier, New York, 1972.

[62] P. W. Shor, *Algorithms for quantum computation: Discrete log and factoring*, FOCS'35, 1994, pp. 124–134.

[63] ———, *Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer*, SIAM J. Comput. **26** (1997), 1484–1509; e-print `quant-ph/9508027`.

[64] ———, *Scheme for reducing decoherence in quantum memory*, Phys. Rev. **A52** (1995), 2493–2496.

[65] ———, *Fault-tolerant quantum computation*, FOCS'37, 1996, pp. 56–65; e-print `quant-ph/9605011`.

[66] D. Simon, *On the power of quantum computation*, FOCS'35, 1994, pp. 116–123.

[67] M. Sipser, *Introduction to the theory of computation*, PWS, Boston, 1997.

[68] A. M. Steane, *Multiple particle interference and quantum error correction*, Proc. Roy. Soc. London **A452** (1996), p. 2551; e-print `quant-ph/9601029`.

[69] C. Umans, *Pseudo-random generators for all hardnesses*, to appear in STOC 2002 and Complexity 2002 joint session; `http://www.research.microsoft.com/~umans/research.htm`.

[70] I. M. Vinogradov, *Elements of number theory*, Dover, New York, 1954.

[71] J. Watrous, *On quantum and classical space-bounded processes with algebraic transition amplitudes*, FOCS'40, 1999, pp. 341–351; e-print `cs.CC/9911008`.

[72] J. Watrous, *PSPACE has constant-round quantum interactive proof systems*, FOCS'40, 1999, pp. 112–119; e-print: `cs.CC/9901015`.

[73] T. Yamakami and A. C. Yao, $\mathrm{NQP}_{\mathbb{C}} = \mathrm{co} - \mathrm{C}_{=}\mathbf{P}$, Inform. Process. Lett. **71** (2) (1999), 63–69; e-print `quant-ph/9812032`.

[74] A. C.-C. Yao, *Quantum circuit complexity*, FOCS'34, 1993, pp. 352–361.

[75] C. Zalka, *Grover's quantum searching algorithm is optimal*, e-print `quant-ph/9711070`.

Index

http://dx.doi.org/10.1090/gsm/047/30

http://dx.doi.org/10.1090/gsm/047/31

This book presents a concise introduction to an emerging and increasingly important topic, the theory of quantum computing. The development of quantum computing exploded in 1994 with the discovery of its use in factoring large numbers—an extremely difficult and time-consuming problem when using a conventional computer. In less than 300 pages, the authors set forth a solid foundation to the theory, including results that have not appeared elsewhere and improvements on existing works.

The book starts with the basics of classical theory of computation, including NP-complete problems and the idea of complexity of an algorithm. Then the authors introduce general principles of quantum computing and pass to the study of main quantum computation algorithms: Grover's algorithm, Shor's factoring algorithm, and the Abelian hidden subgroup problem. In concluding sections, several related topics are discussed (parallel quantum computation, a quantum analog of NP-completeness, and quantum error-correcting codes).

This is a suitable textbook for a graduate course in quantum computing. Prerequisites are very modest and include linear algebra, elements of group theory and probability, and the notion of an algorithm (on a formal or an intuitive level). The book is complete with problems, solutions, and an appendix summarizing the necessary results from number theory.

ISBN 978-0-8218-3229-5

9 780821 832295

GSM/47.S

For additional information
and updates on this book, visit

www.ams.org/bookpages/gsm-47

AMS *on the* Web
www.ams.org