

Classical and Quantum Computation

A. Yu. Kitaev

A. H. Shen

M. N. Vyalyi

Physikalische Bibliothek
Fachbereich 5
Technische Universität Darmstadt
Hochschulstraße 4
D-64289 Darmstadt

pb 2850

Graduate Studies
in Mathematics

Volume 47



American Mathematical Society
Providence, Rhode Island

Contents

Foreword	vii
Notation	xi
Introduction	1
Part 1. Classical Computation	9
1. Turing machines	9
1.1. Definition of a Turing machine	10
1.2. Computable functions and decidable predicates	11
1.3. Turing's thesis and universal machines	12
1.4. Complexity classes	14
2. Boolean circuits	17
2.1. Definitions. Complete bases	17
2.2. Circuits versus Turing machines	20
2.3. Basic algorithms. Depth, space and width	23
3. The class NP: Reducibility and completeness	27
3.1. Nondeterministic Turing machines	27
3.2. Reducibility and NP-completeness	30
4. Probabilistic algorithms and the class BPP	36
4.1. Definitions. Amplification of probability	36
4.2. Primality testing	38
4.3. BPP and circuit complexity	42

5.	The hierarchy of complexity classes	44
5.1.	Games machines play	44
5.2.	The class PSPACE	48
Part 2.	Quantum Computation	53
6.	Definitions and notation	54
6.1.	The tensor product	54
6.2.	Linear algebra in Dirac's notation	55
6.3.	Quantum gates and circuits	58
7.	Correspondence between classical and quantum computation	60
8.	Bases for quantum circuits	65
8.1.	Exact realization	65
8.2.	Approximate realization	71
8.3.	Efficient approximation over a complete basis	75
9.	Definition of Quantum Computation. Examples	82
9.1.	Computation by quantum circuits	82
9.2.	Quantum search: Grover's algorithm	83
9.3.	A universal quantum circuit	88
9.4.	Quantum algorithms and the class BQP	89
10.	Quantum probability	92
10.1.	Probability for state vectors	92
10.2.	Mixed states (density matrices)	94
10.3.	Distance functions for density matrices	98
11.	Physically realizable transformations of density matrices	100
11.1.	Physically realizable superoperators: characterization	100
11.2.	Calculation of the probability for quantum computation	102
11.3.	Decoherence	102
11.4.	Measurements	105
11.5.	The superoperator norm	108
12.	Measuring operators	112
12.1.	Definition and examples	112
12.2.	General properties	114
12.3.	Garbage removal and composition of measurements	115
13.	Quantum algorithms for Abelian groups	116

13.1.	The problem of hidden subgroup in $(\mathbb{Z}_2)^k$; Simon's algorithm	117
13.2.	Factoring and finding the period for raising to a power	119
13.3.	Reduction of factoring to period finding	120
13.4.	Quantum algorithm for finding the period: the basic idea	122
13.5.	The phase estimation procedure	125
13.6.	Discussion of the algorithm	130
13.7.	Parallelized version of phase estimation. Applications	131
13.8.	The hidden subgroup problem for \mathbb{Z}^k	135
14.	The quantum analogue of NP: the class BQNP	138
14.1.	Modification of classical definitions	138
14.2.	Quantum definition by analogy	139
14.3.	Complete problems	141
14.4.	Local Hamiltonian is BQNP-complete	144
14.5.	The place of BQNP among other complexity classes	150
15.	Classical and quantum codes	151
15.1.	Classical codes	153
15.2.	Examples of classical codes	154
15.3.	Linear codes	155
15.4.	Error models for quantum codes	156
15.5.	Definition of quantum error correction	158
15.6.	Shor's code	161
15.7.	The Pauli operators and symplectic transformations	163
15.8.	Symplectic (stabilizer) codes	167
15.9.	Toric code	170
15.10.	Error correction for symplectic codes	172
15.11.	Anyons (an example based on the toric code)	173
Part 3.	Solutions	177
S1.	Problems of Section 1	177
S2.	Problems of Section 2	183
S3.	Problems of Section 3	195
S5.	Problems of Section 5	202
S6.	Problems of Section 6	203

S7. Problems of Section 7	204
S8. Problems of Section 8	204
S9. Problems of Section 9	216
S10. Problems of Section 10	221
S11. Problems of Section 11	224
S12. Problems of Section 12	230
S13. Problems of Section 13	230
S15. Problems of Section 15	234
Appendix A. Elementary Number Theory	237
A.1. Modular arithmetic and rings	237
A.2. Greatest common divisor and unique factorization	239
A.3. Chinese remainder theorem	241
A.4. The structure of finite Abelian groups	243
A.5. The structure of the group $(\mathbb{Z}/q\mathbb{Z})^*$	245
A.6. Euclid's algorithm	247
A.7. Continued fractions	248
Bibliography	251
Index	255