

# Quantum Algorithms via Linear Algebra

computer science/mathematics

A PRIMER | RICHARD J. LIPTON AND KENNETH W. REGAN

This introduction to quantum algorithms is concise but comprehensive, covering many key algorithms. It is mathematically rigorous but requires minimal background and assumes no knowledge of quantum theory or quantum mechanics. The book explains quantum computation in terms of elementary linear algebra; it assumes the reader will have some familiarity with vectors, matrices, and their basic properties, but offers a review of all the relevant material from linear algebra. By emphasizing computation and algorithms rather than physics, this primer makes quantum algorithms accessible to students and researchers in computer science without the complications of quantum mechanical notation, physical concepts, and philosophical issues.

After explaining the development of quantum operations and computations based on linear algebra, the book presents the major quantum algorithms, from seminal algorithms by Deutsch, Jozsa, and Simon through Shor's and Grover's algorithms to recent quantum walks. It covers quantum gates, computational complexity, and some graph theory. Mathematical proofs are generally short and straightforward; quantum circuits and gates are used to illuminate linear algebra; and the discussion of complexity is anchored in computational problems rather than machine models.

*Quantum Algorithms via Linear Algebra* is suitable for classroom use or as a reference for computer scientists and mathematicians.

Richard J. Lipton is Professor and Frederick G. Storey Chair in Computing at Georgia Tech. Kenneth W. Regan is Associate Professor in the Department of Computer Science and Engineering at the University at Buffalo, State University of New York.

"A remarkably large part of quantum algorithms and quantum computing can be described with just the knowledge of multiplying matrices with complex number entries. Lipton and Regan have done a great job presenting all the major quantum algorithms from this easy and accessible point of view. Anyone interested in quantum computing would gain much from this presentation."

—Noson S. Yanofsky, Professor, Department of Computer and Information Sciences, Brooklyn College; coauthor of *Quantum Computing for Computer Scientists*

"This book gives an excellent, rigorous introduction to quantum computing, using only the mathematical background normal for an undergraduate computer science major. Students often ask me how they can get started toward understanding this field, and I can now point them to this book. I will certainly recommend it to all the students in my undergraduate theory of computation class."

—David Mix Barrington, School of Computer Science, University of Massachusetts Amherst

"*Quantum Algorithms via Linear Algebra* provides a great alternative introduction to the fascinating area of quantum computing. While traditional treatments are rooted in quantum mechanics, this quantum way of thinking could be a barrier for entry into this area. This book strips out the 'quantum-ness' from some famous algorithms and keeps it about elementary linear algebra, thus opening up quantum computing to a larger audience."

—Nisheeth Vishnoi, École Polytechnique Fédérale de Lausanne

"*Quantum Algorithms via Linear Algebra* is a marvelous and self-contained account of the algorithms that 'made' quantum computing, presented in a clear and conversational style that is a delight to read. It succeeds in giving a mathematically precise, and complete, exposition that invokes only elementary linear algebra. This style of presentation strips away unnecessary notation and abstraction and brings the beautiful ideas underlying these algorithms into a sharp focus."

—Chris Umans, Professor of Computer Science, Caltech

The MIT Press | Massachusetts Institute of Technology | Cambridge, Massachusetts 02142 | <http://mitpress.mit.edu>

ISBN 9780262028394



9 780262 028394



Preface	xi
Acknowledgements	xiii
<b>1 Introduction</b>	<b>1</b>
1.1 The Model	2
1.2 The Space and the States	3
1.3 The Operations	5
1.4 Where Is the Input?	6
1.5 What Exactly Is the Output?	7
1.6 Summary and Notes	8
<b>2 Numbers and Strings</b>	<b>9</b>
2.1 Asymptotic Notation	11
2.2 Problems	12
2.3 Summary and Notes	13
<b>3 Basic Linear Algebra</b>	<b>15</b>
3.1 Hilbert Spaces	16
3.2 Products and Tensor Products	16
3.3 Matrices	17
3.4 Complex Spaces and Inner Products	19
3.5 Matrices, Graphs, and Sums Over Paths	20
3.6 Problems	23
3.7 Summary and Notes	26
<b>4 Boolean Functions, Quantum Bits, and Feasibility</b>	<b>27</b>
4.1 Feasible Boolean Functions	28
4.2 An Example	30
4.3 Quantum Representation of Boolean Arguments	33
4.4 Quantum Feasibility	35
4.5 Problems	38
4.6 Summary and Notes	40
<b>5 Special Matrices</b>	<b>41</b>
5.1 Hadamard Matrices	41
5.2 Fourier Matrices	42
5.3 Reversible Computation and Permutation Matrices	43
5.4 Feasible Diagonal Matrices	44
5.5 Reflections	45
5.6 Problems	46



5.7	Summary and Notes	49
<b>6</b>	<b>Tricks</b>	51
6.1	Start Vectors	51
6.2	Controlling and Copying Base States	52
6.3	The Copy-Uncompute Trick	54
6.4	Superposition Tricks	55
6.5	Flipping a Switch	56
6.6	Measurement Tricks	58
6.7	Partial Transforms	59
6.8	Problems	60
6.9	Summary and Notes	62
<b>7</b>	<b>Phil's Algorithm</b>	63
7.1	The Algorithm	63
7.2	The Analysis	63
7.3	An Example	64
7.4	A Two-Qubit Example	64
7.5	Phil Measures Up	66
7.6	Quantum Mazes versus Circuits versus Matrices	69
7.7	Problems	71
7.8	Summary and Notes	74
<b>8</b>	<b>Deutsch's Algorithm</b>	77
8.1	The Algorithm	77
8.2	The Analysis	78
8.3	Superdense Coding and Teleportation	82
8.4	Problems	86
8.5	Summary and Notes	87
<b>9</b>	<b>The Deutsch-Jozsa Algorithm</b>	89
9.1	The Algorithm	89
9.2	The Analysis	90
9.3	Problems	92
9.4	Summary and Notes	92
<b>10</b>	<b>Simon's Algorithm</b>	93
10.1	The Algorithm	93
10.2	The Analysis	94



10.3	Problems	95
10.4	Summary and Notes	96
<b>11</b>	<b>Shor's Algorithm</b>	97
11.1	Strategy	97
11.2	Good Numbers	98
11.3	Quantum Part of the Algorithm	99
11.4	Analysis of the Quantum Part	100
11.5	Probability of a Good Number	102
11.6	Using a Good Number	105
11.7	Continued Fractions	106
11.8	Problems	107
11.9	Summary and Notes	108
<b>12</b>	<b>Factoring Integers</b>	109
12.1	Some Basic Number Theory	109
12.2	Periods Give the Order	110
12.3	Factoring	110
12.4	Problems	112
12.5	Summary and Notes	113
<b>13</b>	<b>Grover's Algorithm</b>	115
13.1	Two Vectors	115
13.2	The Algorithm	117
13.3	The Analysis	117
13.4	The General Case, with $k$ Unknown	118
13.5	Grover Approximate Counting	119
13.5.1	The Algorithm	122
13.5.2	The Analysis	122
13.6	Problems	126
13.7	Summary and Notes	128
<b>14</b>	<b>Quantum Walks</b>	129
14.1	Classical Random Walks	129
14.2	Random Walks and Matrices	130
14.3	An Encoding Nicety	132
14.4	Defining Quantum Walks	133
14.5	Interference and Diffusion	134



14.6	The Big Factor	138
14.7	Problems	139
14.8	Summary and Notes	140
<b>15</b>	<b>Quantum Walk Search Algorithms</b>	143
15.1	Search in Big Graphs	143
15.2	General Quantum Walk for Graph Search	145
15.3	Specifying the Generic Walk	147
15.4	Adding the Data	149
15.5	Toolkit Theorem for Quantum Walk Search	150
15.5.1	The Generic Algorithm	151
15.5.2	The Generic Analysis	152
15.6	Grover Search as Generic Walk	152
15.7	Element Distinctness	153
15.8	Subgraph Triangle Incidence	154
15.9	Finding a Triangle	155
15.10	Evaluating Formulas and Playing Chess	156
15.11	Problems	157
15.12	Summary and Notes	158
<b>16</b>	<b>Quantum Computation and BQP</b>	159
16.1	The Class BQP	159
16.2	Equations, Solutions, and Complexity	161
16.3	A Circuit Labeling Algorithm	163
16.4	Sum-Over-Paths and Polynomial Roots	165
16.5	The Additive Polynomial Simulation	168
16.6	Bounding BQP	169
16.7	Problems	170
16.8	Summary and Notes	173
<b>17</b>	<b>Beyond</b>	175
17.1	Reviewing the Algorithms	175
17.2	Some Further Topics	176
17.3	The “Quantum” in the Algorithms	179
	Bibliography	183
	Index	189