

Yorick Hardy
Willi-Hans Steeb

Classical and Quantum Computing

with C++ and Java Simulations

Springer Basel AG

Authors:

Yorick Hardy and Willi-Hans Steeb
International School for Scientific Computing
Rand Afrikaans University
P.O. Box 524
Auckland Park 2006
South Africa

2000 Mathematical Subject Classification 68Q01; 81P68

A CIP catalogue record for this book is available from the
Library of Congress, Washington D.C., USA

Deutsche Bibliothek Cataloging-in-Publication Data

Hardy, Yorick:

Classical and quantum computing with C++ and Java simulations /
Yorick Hardy ; Willi-Hans Steeb. - Basel ; Boston ; Berlin : Birkhäuser,
2001

ISBN 978-3-7643-6610-0 ISBN 978-3-0348-8366-5 (eBook)

DOI 10.1007/978-3-0348-8366-5

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, re-use of illustrations, recitation, broadcasting, reproduction on microfilms or in other ways, and storage in data banks. For any kind of use permission of the copyright owner must be obtained.

© 2001 Springer Basel AG

Originally published by Birkhäuser Verlag in 2001

Cover design: Micha Lotrovsky, 4106 Therwil, Switzerland

Printed on acid-free paper produced from chlorine-free pulp. TCF ∞

Contents

List of Tables	xiii
List of Figures	xv
List of Symbols	xix
Preface	xxi

I Classical Computing

1 Algorithms

1.1 Algorithms	3
1.2 Algorithm Verification	6
1.3 Random Algorithms	10
1.4 Total and Partial Functions	15
1.5 Alphabets and Words	18

2 Boolean Algebra

2.1 Introduction	23
2.2 Definitions	24
2.3 Rules and Laws of Boolean Algebra	26
2.4 DeMorgan's Theorem	27
2.5 Further Definitions	27
2.6 Boolean Function Implementation	32
2.6.1 Karnaugh Maps	35
2.6.2 Quine-McKluskey Method	38
2.7 Example Programs	41
2.7.1 Efficient Set Operations Using Boolean Algebra	41
2.7.2 Quine-McKluskey Implementation	46

3	Number Representation	
3.1	Binary, Decimal and Hexadecimal Numbers	51
3.1.1	Conversion	53
3.1.2	Arithmetic	58
3.1.3	Signed Integers	60
3.1.4	Overflow	67
3.1.5	Binary-Coded Decimal Form	70
3.2	Floating Point Representation	72
3.2.1	Introduction	72
3.2.2	Representation	74
4	Logic Gates	
4.1	Introduction	79
4.2	Gates	80
4.2.1	AND Gate	80
4.2.2	OR Gate	81
4.2.3	XOR Gate	82
4.2.4	NOT Gate (Inverter)	83
4.2.5	NAND Gate	84
4.2.6	NOR Gate	85
4.2.7	XNOR Gate	86
4.3	Buffer	87
4.4	Tri-State Logic	88
4.5	Feedback and Gates	89
5	Combinational Circuits	
5.1	Introduction	91
5.2	Decoder	92
5.3	Encoder	93
5.4	Demultiplexer	96
5.5	Multiplexer	97
5.6	Binary Adder	98
5.6.1	Binary Half Adder	98
5.6.2	Binary Full Adder	99
5.6.3	Binary Four-Bit Adder	100
5.6.4	Faster Addition	101
5.7	Binary Subtraction	102
5.8	Binary Multiplication	103
5.8.1	Unsigned Integer Multiplication	103
5.8.2	Fast Multiplication	105
5.8.3	Signed Integer Multiplication	106
5.9	Binary Division	107

5.10	Magnitude Comparator	108
5.11	4-Bit ALU	110
5.12	Read Only Memory (ROM)	112
5.13	Combinational Programmable Logic Devices	113
5.14	Programmable Gate Arrays	117
5.15	VHDL	118
6	Latches and Registers	
6.1	Introduction	119
6.2	SR Latch	120
6.3	D Latch	121
6.4	JK Latch	122
6.5	D Register	123
6.6	JK Register	124
7	Synchronous Circuits	
7.1	Introduction	125
7.2	Shift Registers	127
7.3	Binary Counter	129
7.4	Example Program	133
8	Recursion	
8.1	Introduction	135
8.2	Example Programs	140
8.3	Mutual Recursion	152
8.4	Wavelets and Recursion	156
8.5	Primitive Recursive Functions	162
8.6	Backtracking	165
8.7	Stacks and Recursion Mechanisms	168
	8.7.1 Recursion Using Stacks	168
	8.7.2 Stack Free Recursion	169
9	Abstract Data Types	
9.1	Introduction	171
9.2	Linked List	172
9.3	Stack	187
9.4	Tree	190

10 Error Detection and Correction	
10.1 Introduction	197
10.2 Parity Function	198
10.3 Hamming Codes	199
10.4 Weighted Checksum	204
10.5 Noiseless Coding Theorem	205
10.6 Example Programs	208
11 Cryptography	
11.1 Introduction	215
11.2 Classical Cypher Systems	216
11.3 Public Key Cryptography	221
12 Finite State Machines	
12.1 Introduction	229
12.2 Finite Automata	230
12.3 Finite Automata with Output	233
12.4 Turing Machines	238
12.5 Example Programs	244
13 Computability and Complexity	
13.1 Introduction	251
13.2 Computability	252
13.2.1 Church's Thesis	252
13.2.2 The Halting Problem	253
13.3 Gödel's Incompleteness Theorem	254
13.3.1 Gödel Numbering	254
13.3.2 Gödel's Incompleteness Theorem	256
13.4 Complexity	256
13.4.1 Complexity of Bit Strings	256
13.4.2 NP-class of Problems	259
14 Neural Networks	
14.1 Introduction	261
14.2 Hyperplanes	266
14.3 Perceptron	268
14.3.1 Introduction	268
14.3.2 Boolean Functions	272
14.3.3 Perceptron Learning	275
14.3.4 Quadratic Threshold Gates	279
14.3.5 One and Two Layered Networks	282

14.3.6 Perceptron Learning Algorithm 283

14.3.7 The XOR Problem and Two-Layered Networks 289

14.4 Multilayer Perceptrons 294

14.4.1 Introduction 294

14.4.2 Cybenko's Theorem 295

14.4.3 Back-Propagation Algorithm 296

15 Genetic Algorithms

15.1 Introduction 313

15.2 The Sequential Genetic Algorithm 315

15.3 Gray Code 320

15.4 Schemata Theorem 323

15.5 Markov Chain Analysis 326

15.6 Bit Set Classes in C++ and Java 328

15.7 A Bit Vector Class 333

15.8 Maximum of One-Dimensional Maps 337

15.9 Maximum of Two-Dimensional Maps 346

15.10 The Four Colour Problem 356

15.11 Problems with Constraints 360

15.11.1 Introduction 360

15.11.2 Knapsack Problem 362

15.11.3 Traveling Salesman Problem 368

15.12 Other Applications for Genetic Algorithms 380

15.13 Distributed Global Optimization 381

15.14 Genetic Programming 384

15.15 Gene Expression Programming 392

II Quantum Computing

16 Quantum Mechanics

16.1 Hilbert Spaces 403

16.2 Linear Operators in Hilbert Spaces 417

16.3 Schmidt Decomposition 431

16.4 Spin Matrices and Kronecker Product 434

16.5 Postulates of Quantum Mechanics 442

17 Quantum Bits and Quantum Computation

17.1	Introduction	451
17.2	Quantum Bits and Quantum Registers	452
	17.2.1 Quantum Bits	452
	17.2.2 Quantum Registers	453
17.3	Entangled States	455
17.4	Quantum Gates	463
	17.4.1 Introduction	463
	17.4.2 NOT Gate	464
	17.4.3 Walsh-Hadamard Gate	465
	17.4.4 XOR and the Controlled NOT Gate	467
	17.4.5 Other Quantum Gates	468
	17.4.6 Universal Sets of Quantum Gates	471
	17.4.7 Functions	472
17.5	Garbage Disposal	476
17.6	Quantum Copying	477
17.7	Example Programs	480

18 Measurement and Quantum States

18.1	Introduction	491
18.2	Measurement Problem	492
18.3	Copenhagen Interpretation	493
18.4	Hidden Variable Theories	495
18.5	Everett Interpretation	496
18.6	Basis Degeneracy Problem	498
18.7	Information Theoretic Viewpoint	500

19 Quantum State Machines

19.1	Introduction	501
19.2	Quantum Automata	501
19.3	Quantum Turing Machines	504

20 Teleportation

20.1	Introduction	507
20.2	Teleportation Algorithm	508
20.3	Example Program	511

21 Quantum Algorithms	
21.1 Deutsch's Problem	515
21.2 Simon's Problem	519
21.3 Quantum Fourier Transform	522
21.4 Factoring (Shor's Algorithm)	524
21.5 The Hidden Subgroup Problem	528
21.6 Unstructured Search (Grover's Algorithm)	530
21.7 Quantum Key Distribution	537
21.8 Dense Coding	539
22 Quantum Information Theory	
22.1 Introduction	541
22.2 Von Neumann Entropy	542
22.3 Measures of Entanglement	543
22.3.1 Bell's Inequality	543
22.3.2 Entanglement of Formation	545
22.3.3 Conditions on Entanglement Measures	546
22.4 Quantum Coding	548
22.5 Holevo Bound	554
23 Quantum Error Detection and Correction	
23.1 Introduction	555
23.2 The Nine-qubit Code	556
23.3 The Seven-qubit Code	558
23.4 Efficiency and the Five-qubit Code	559
23.5 Stabilizer Codes	561
24 Quantum Hardware	
24.1 Introduction	563
24.2 Trapped Ions	564
24.3 Cavity Quantum Electrodynamics	565
24.4 Quantum Dots	566
24.5 Nuclear Magnetic Resonance Spectroscopy	569
25 Internet Resources	571
Bibliography	573
Index	585