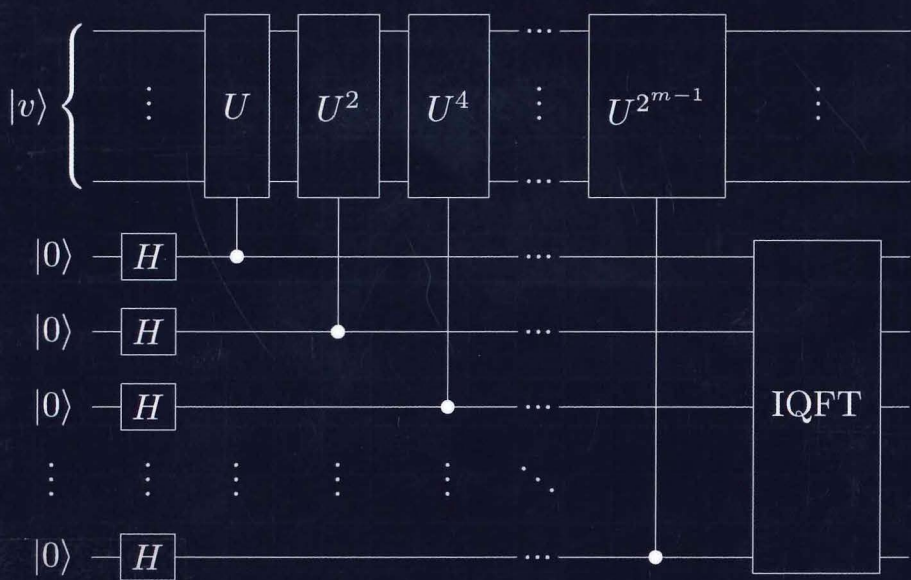


Introduction to Classical and Quantum Computing



Thomas G. Wong

สำนักหอสมุด มหาวิทยาลัยเชียงใหม่

61๖705701

O 12577467

i 22685935

Thomas G. Wong

Introduction to Classical and Quantum Computing



Contents

| | | |
|----------|--|----------|
| 1 | Classical Information and Computation | 1 |
| 1.1 | Bits | 2 |
| 1.1.1 | Coins | 2 |
| 1.1.2 | Dice | 3 |
| 1.1.3 | Encoding Information | 4 |
| 1.1.4 | Physical Bits | 5 |
| 1.1.5 | Binary | 6 |
| 1.1.6 | ASCII | 9 |
| 1.2 | Logic Gates | 11 |
| 1.2.1 | Single-Bit Gates | 11 |
| 1.2.2 | Two-Bit Gates | 13 |
| 1.2.3 | Logic Gates as Physical Circuits | 15 |
| 1.2.4 | Multiple Gates | 21 |
| 1.2.5 | Universal Gates | 23 |
| 1.3 | Adders and Verilog | 27 |
| 1.3.1 | Adding Binary Numbers by Hand | 27 |
| 1.3.2 | Half Adder | 28 |
| 1.3.3 | Full Adder | 32 |
| 1.3.4 | Ripple-Carry Adder | 34 |
| 1.3.5 | Ripple-Carry with Full Adders | 36 |
| 1.3.6 | Circuit Complexity | 37 |
| 1.4 | Circuit Simplification and Boolean Algebra | 37 |
| 1.4.1 | Order of Operations | 38 |
| 1.4.2 | Association, Commutativity, and Distribution | 38 |
| 1.4.3 | Identities Involving Zero and One | 39 |
| 1.4.4 | Single-Variable Identities | 39 |
| 1.4.5 | Two-Variable Identities and De Morgan's Laws | 40 |
| 1.4.6 | Circuit Simplification | 42 |
| 1.5 | Reversible Logic Gates | 44 |
| 1.5.1 | Reversible Gates | 44 |
| 1.5.2 | Irreversible Gates | 45 |

| | | |
|----------|---|------------|
| 1.5.3 | Toffoli Gate: A Reversible AND Gate | 46 |
| 1.5.4 | Making Irreversible Gates Reversible | 48 |
| 1.6 | Error Correction | 52 |
| 1.6.1 | Errors in Physical Devices | 52 |
| 1.6.2 | Error Detection | 54 |
| 1.6.3 | Error Correction | 55 |
| 1.7 | Computational Complexity | 58 |
| 1.7.1 | Asymptotic Notation | 58 |
| 1.7.2 | Complexity Classes | 60 |
| 1.8 | Turing Machines | 63 |
| 1.8.1 | Components | 63 |
| 1.8.2 | Incrementing Binary Numbers | 64 |
| 1.8.3 | Church-Turing Thesis | 67 |
| 1.9 | Summary | 71 |
| 2 | One Quantum Bit | 73 |
| 2.1 | Qubit Touchdown: A Quantum Computing Board Game | 73 |
| 2.2 | Superposition | 74 |
| 2.2.1 | Zero or One | 74 |
| 2.2.2 | Superposition | 76 |
| 2.2.3 | Review of Complex Numbers | 80 |
| 2.3 | Measurement | 83 |
| 2.3.1 | Measurement in the Z-Basis | 83 |
| 2.3.2 | Normalization | 85 |
| 2.3.3 | Measurement in Other Bases | 86 |
| 2.3.4 | Consecutive Measurements | 90 |
| 2.4 | Bloch Sphere Mapping | 90 |
| 2.4.1 | Global and Relative Phases | 91 |
| 2.4.2 | Spherical Coordinates | 92 |
| 2.4.3 | Cartesian Coordinates | 95 |
| 2.5 | Physical Qubits | 97 |
| 2.6 | Quantum Gates | 98 |
| 2.6.1 | Linear Maps | 98 |
| 2.6.2 | Classical Reversible Gates | 100 |
| 2.6.3 | Common One-Qubit Quantum Gates | 102 |
| 2.6.4 | General One-Qubit Gates | 108 |
| 2.7 | Quantum Circuits | 111 |
| 2.7.1 | Circuit Diagrams | 111 |
| 2.7.2 | Quirk | 111 |
| 2.8 | Summary | 112 |
| 3 | Linear Algebra | 115 |
| 3.1 | Quantum States | 115 |
| 3.1.1 | Column Vectors | 115 |
| 3.1.2 | Row Vectors | 116 |

| | | |
|----------|--|------------|
| 3.2 | Inner Products | 118 |
| 3.2.1 | Inner Products Are Scalars | 118 |
| 3.2.2 | Orthonormality | 119 |
| 3.2.3 | Projection, Measurement, and Change of Basis | 120 |
| 3.3 | Quantum Gates | 124 |
| 3.3.1 | Gates as Matrices | 124 |
| 3.3.2 | Common One-Qubit Gates as Matrices | 127 |
| 3.3.3 | Sequential Quantum Gates | 128 |
| 3.3.4 | Circuit Identities | 129 |
| 3.3.5 | Unitarity | 131 |
| 3.3.6 | Reversibility | 132 |
| 3.4 | Outer Products | 133 |
| 3.4.1 | Outer Products Are Matrices | 133 |
| 3.4.2 | Completeness Relation | 135 |
| 3.5 | Summary | 136 |
| 4 | Multiple Quantum Bits | 137 |
| 4.1 | Entanglion: A Quantum Computing Board Game | 137 |
| 4.1.1 | Mechanics | 137 |
| 4.1.2 | Connection to Quantum Computing | 139 |
| 4.2 | States and Measurement | 140 |
| 4.2.1 | Tensor Product | 140 |
| 4.2.2 | Kronecker Product | 142 |
| 4.2.3 | Measuring Individual Qubits | 144 |
| 4.2.4 | Sequential Single-Qubit Measurements | 146 |
| 4.3 | Entanglement | 147 |
| 4.3.1 | Product States | 147 |
| 4.3.2 | Entangled States | 149 |
| 4.4 | Quantum Gates | 150 |
| 4.4.1 | One-Qubit Quantum Gates | 150 |
| 4.4.2 | Two-Qubit Quantum Gates | 153 |
| 4.4.3 | Toffoli Gate | 163 |
| 4.4.4 | No-Cloning Theorem | 165 |
| 4.5 | Quantum Adders | 166 |
| 4.5.1 | Classical Adder | 166 |
| 4.5.2 | Making the Classical Adder a Quantum Gate | 168 |
| 4.5.3 | Quantum Setup | 172 |
| 4.5.4 | Quantum Sum | 172 |
| 4.5.5 | Quantum Carry | 174 |
| 4.5.6 | Quantum Ripple-Carry Adder | 175 |
| 4.5.7 | Circuit Complexity | 183 |
| 4.5.8 | Adding in Superposition | 184 |
| 4.6 | Universal Quantum Gates | 185 |
| 4.6.1 | Definition | 185 |
| 4.6.2 | Components of a Universal Gate Set | 185 |

| | | |
|----------|---|------------|
| 4.6.3 | Examples of Universal Gate Sets | 186 |
| 4.6.4 | Solovay-Kitaev Theorem | 187 |
| 4.6.5 | Quantum Computing without Complex Numbers | 187 |
| 4.7 | Quantum Error Correction | 189 |
| 4.7.1 | Decoherence | 189 |
| 4.7.2 | Bit-Flip Code | 190 |
| 4.7.3 | Phase-Flip Code | 196 |
| 4.7.4 | Shor Code | 201 |
| 4.8 | Summary | 207 |
| 5 | Quantum Programming | 209 |
| 5.1 | IBM Quantum | 209 |
| 5.1.1 | Services | 209 |
| 5.1.2 | Quantum Composer | 212 |
| 5.1.3 | Quantum Processor | 215 |
| 5.1.4 | Simulator | 218 |
| 5.2 | Quantum Assembly Language | 219 |
| 5.2.1 | OpenQASM | 219 |
| 5.2.2 | Quantum Experience Standard Header | 221 |
| 5.2.3 | OpenQASM in IBM Quantum | 222 |
| 5.2.4 | Quantum Adder | 222 |
| 5.3 | Qiskit | 228 |
| 5.3.1 | Quantum Composer | 228 |
| 5.3.2 | Quantum Lab | 229 |
| 5.3.3 | Simulator | 232 |
| 5.3.4 | Quantum Processor | 234 |
| 5.4 | Other Quantum Programming Languages | 236 |
| 5.5 | Summary | 236 |
| 6 | Entanglement and Quantum Protocols | 237 |
| 6.1 | Measurements | 237 |
| 6.1.1 | Product States | 238 |
| 6.1.2 | Maximally Entangled States | 238 |
| 6.1.3 | Partially Entangled States | 238 |
| 6.2 | Bell Inequalities | 240 |
| 6.2.1 | EPR Paradox and Local Hidden Variables | 240 |
| 6.2.2 | Bell Inequalities and the CHSH Inequality | 241 |
| 6.2.3 | Quantum Processor Experiment | 246 |
| 6.2.4 | Other Experiments | 249 |
| 6.2.5 | No-Signaling Principle | 249 |
| 6.2.6 | Other Theories | 251 |
| 6.3 | Monogamy of Entanglement | 253 |
| 6.3.1 | Classical Correlations | 253 |
| 6.3.2 | Quantum Entanglement | 253 |
| 6.4 | Superdense Coding | 255 |

| | | |
|----------|--|------------|
| 6.4.1 | The Problem | 255 |
| 6.4.2 | Classical Solution | 255 |
| 6.4.3 | Quantum Solution | 255 |
| 6.5 | Quantum Teleportation | 257 |
| 6.5.1 | The Problem | 257 |
| 6.5.2 | Classical Solution | 257 |
| 6.5.3 | Quantum Solution | 258 |
| 6.6 | Quantum Key Distribution | 262 |
| 6.6.1 | Encryption | 262 |
| 6.6.2 | Classical Solution: Public Key Cryptography | 263 |
| 6.6.3 | Quantum Solution: BB84 | 269 |
| 6.7 | Summary | 272 |
| 7 | Quantum Algorithms | 273 |
| 7.1 | Circuit vs Query Complexity | 273 |
| 7.1.1 | Circuit Complexity | 273 |
| 7.1.2 | Query Complexity | 274 |
| 7.1.3 | Quantum Oracles | 275 |
| 7.1.4 | Phase Oracle | 276 |
| 7.2 | Parity | 278 |
| 7.2.1 | The Problem | 278 |
| 7.2.2 | Classical Solution | 278 |
| 7.2.3 | Quantum Solution: Deutsch's Algorithm | 278 |
| 7.2.4 | Generalization to Additional Bits | 280 |
| 7.3 | Constant vs Balanced Functions | 281 |
| 7.3.1 | The Problem | 281 |
| 7.3.2 | Classical Solution | 282 |
| 7.3.3 | Quantum Solution: Deutsch-Jozsa Algorithm | 283 |
| 7.4 | Secret Dot Product String | 287 |
| 7.4.1 | The Problem | 287 |
| 7.4.2 | Classical Solution | 288 |
| 7.4.3 | Quantum Solution: Bernstein-Vazirani Algorithm | 288 |
| 7.4.4 | Recursive Problem | 290 |
| 7.5 | Secret XOR Mask | 291 |
| 7.5.1 | The Problem | 291 |
| 7.5.2 | Classical Solution | 292 |
| 7.5.3 | Quantum Solution: Simon's Algorithm | 294 |
| 7.5.4 | Summary | 297 |
| 7.6 | Brute-Force Searching | 297 |
| 7.6.1 | The Problem | 297 |
| 7.6.2 | Classical Solution | 299 |
| 7.6.3 | Quantum Solution: Grover's Algorithm | 299 |
| 7.6.4 | Reflection About Uniform State | 303 |
| 7.6.5 | Optimality | 306 |
| 7.7 | Discrete Fourier Transform | 306 |

- 7.7.1 Application: Analyzing Music 306
- 7.7.2 Classical Solution: Fast Fourier Transform 311
- 7.7.3 Quantum Solution: Quantum Fourier Transform 314
- 7.7.4 Inverse Quantum Fourier Transform 320
- 7.8 Phase / Eigenvalue Estimation 321
 - 7.8.1 The Problem 321
 - 7.8.2 Classical Solution 322
 - 7.8.3 Quantum Solution 323
 - 7.8.4 Multiple Eigenstates 326
- 7.9 Period of Modular Exponentiation 327
 - 7.9.1 The Problem 327
 - 7.9.2 Classical Solution 329
 - 7.9.3 Quantum Solution 332
- 7.10 Factoring 341
 - 7.10.1 The Problem 341
 - 7.10.2 Classical Solution 341
 - 7.10.3 Quantum Solution: Shor’s Algorithm 341
- 7.11 Summary 344
- 8 Next Steps** 345
 - 8.1 Careers in Quantum Computing 345
 - 8.2 Technical Next Steps 346
 - 8.3 Questions 348
 - 8.4 Parting Words 348
- Answers to Exercises** 349
- Index** 383