# Inhaltsverzeichnis


**Vorwort** **XI**

**1 Einleitung** **1**
1.1 Eine neue Art des Rechnens . . . . . 1
1.2 Über dieses Buch . . . . . 8

**2 Vom Bit zum Quantenregister** **9**
2.1 Was ist eine Berechnung? . . . . . 10
2.1.1 Die Turingmaschine . . . . . 13
2.1.2 Schaltkreise . . . . . 14
2.1.3 Der Sprung in die Quantenwelt: Schrödingers Katze . 17
2.2 Das Quantenbit . . . . . 20
2.3 Rechenschritte auf einem Quantenbit . . . . . 23
2.4 Der erste Algorithmus: Ein Zufallsgenerator . . . . . 26
2.5 Quantenregister . . . . . 28
2.6 Der zweite Algorithmus: Das Problem von Deutsch . . . . . 33
2.7 Die Rolle des Tensorprodukts . . . . . 37
2.8 Das Messen von Quantenregistern . . . . . 44
2.9 Noch einmal das Problem von Deutsch . . . . . 50
2.10 Bestandsaufnahme: Die drei Prinzipien des Quantum Computing 51
2.11 Verschränkung . . . . . 53
2.12 Die Hadamard-Transformation und mehrere Bits . . . . . 59
2.13 Der Algorithmus von Deutsch-Jozsa . . . . . 62

**3 Vom Quantenregister zum Quantenschaltkreis** **67**
3.1 Laufzeit . . . . . 68
3.2 Klassische Schaltkreise und Komplexität . . . . . 74
3.3 Quantengatter und Quantenschaltkreise . . . . . 76
3.4 Quantenbits kopieren: Das No-Cloning-Theorem . . . . . 81
3.5 Umkehrbare Berechnungen . . . . . 83
3.6 Unterscheidbare Zustände . . . . . 92
3.7 Gestörte Berechnungen . . . . . 95

**4 Hilfsmittel aus der Theoretischen Informatik** **99**
4.1 Komplexitätsklassen . . . . . 99
4.2 Randomisierte Algorithmen . . . . . 104
4.2.1 Mit dem Zufall rechnen . . . . . 104
4.2.2 Ein Primzahltest . . . . . 105

4.2.3 Probabilistische Komplexitätsklassen . . . . . 107
4.3 Unlösbare Probleme? NP-Vollständigkeit . . . . . 111
4.4 Quantenkomplexitätstheorie . . . . . 116
4.5 Die Churchsche These . . . . . 119

**5 Teleportation und dichte Kodierung 123**
5.1 Quantenteleportation . . . . . 125
5.2 Dichte Kodierung . . . . . 130
5.3 Verschränkte Bits . . . . . 132

**6 Suchen 135**
6.1 Die Nadel im Heuhaufen . . . . . 136
6.2 Die Grover-Iteration . . . . . 138
6.3 Eine geometrische Veranschaulichung . . . . . 144
6.4 Varianten der Quantensuche . . . . . 151
6.4.1 Suche nach einer von mehreren Lösungen . . . . . 151
6.4.2 Suche bei unbekannt vielen Lösungen . . . . . 153
6.4.3 Die Suche nach dem Minimum . . . . . 154
6.4.4 Zählen . . . . . 157
6.5 Anwendungen von Grovers Algorithmus . . . . . 157
6.6 Grovers Algorithmus ist von optimaler Größenordnung . . . . 159
6.7 Folgen für die Fähigkeiten von Quantencomputern . . . . . 164

**7 Geheime Botschaften 167**
7.1 Alice, Bob und Eve . . . . . 168
7.2 Quantenverschlüsselung: das BB84-Protokoll . . . . . 172
7.3 Lauschstrategien . . . . . 180
7.4 Quantenverschlüsselung mit Verschränkung . . . . . 185

**8 Klassische Verschlüsselungen knacken: Primfaktorzerlegung 191**
8.1 Faktorisierung und Verschlüsselung: RSA-Kryptographie . . . 192
8.2 Die Suche nach Perioden . . . . . 197
8.3 Die schnelle Fouriertransformation . . . . . 204
8.4 Die Quanten-Fouriertransformation . . . . . 212
8.5 Simons Algorithmus . . . . . 216
8.6 Shors Algorithmus . . . . . 221
8.7 Jenseits von Shor . . . . . 229

**9 Fehler korrigieren 235**
9.1 Dekohärenz und Fehler auf Quantenbits . . . . . 235
9.2 Klassische Fehlerkorrektur . . . . . 240
9.3 Herausforderungen bei der Korrektur von Quantenbits . . . . 240
9.4 Qubits gegen Fehler sichern . . . . . 241
9.4.1 Bitflip-Code mit Syndrom: Korrektur des Codewords 241
9.4.2 Der Bitflip-Code: Korrektur des Datenbits . . . . . 243
9.4.3 Korrektur von Phaseflips . . . . . 244
9.5 Shors 9-Qubit-Code . . . . . 245
9.6 Ausblick . . . . . 248

**10 Quantenhardware** **251**
10.1 Anforderungen . . . . . 251
10.2 Photonen . . . . . 253
10.2.1 Mach-Zehnder-Interferometer . . . . . 253
10.2.2 Zufallszahlen . . . . . 256
10.2.3 Kryptographie . . . . . 257
10.3 Kernspinresonanz . . . . . 261
10.4 Ionenfallen . . . . . 263
10.5 Einwegberechnungen mit Clusterzuständen . . . . . 264
10.6 Supraleiter . . . . . 267

**11 Ausblick: Optimieren** **271**
11.1 Adiabatische Quantencomputer . . . . . 271
11.2 Quantum Annealing . . . . . 274

**12 Zur Geschichte der Quantenmechanik** **281**
12.1 Max Planck: das Quantum der Wirkung . . . . . 281
12.2 Albert Einstein: Spukhafte Fernwirkung . . . . . 283
12.3 Niels Bohr: Kopenhagen . . . . . 284
12.4 Werner Heisenberg: Ein großes Quantenei . . . . . 287
12.5 Erwin Schrödinger: Katzen und Wellen . . . . . 289
12.6 Schlaglichter der Geschichte des Quantencomputers . . . . . 290

**A Mathematische Grundlagen** **293**
A.1 Komplexe Zahlen . . . . . 293
A.2 Vektorräume . . . . . 295
A.2.1 Was sind Vektorräume? . . . . . 295
A.2.2 Basen und Unterräume . . . . . 297
A.2.3 Winkel und Abstände in einem Vektorraum . . . . . 298
A.2.4 Projektionen . . . . . 300
A.3 Matrizen . . . . . 301
A.4 Kombinatorik und Wahrscheinlichkeit . . . . . 303
A.5 Ganze Zahlen . . . . . 305
A.5.1 Teiler und Vielfache . . . . . 305
A.5.2 Modulares Rechnen . . . . . 305
A.5.3 Zur Division . . . . . 307

**B Lösungen ausgewählter Übungsaufgaben** **309**

**Literatur** **320**

**Symbole und Abkürzungen** **329**

**Quantengatter** **330**

**Namen- und Sachwortverzeichnis** **331**