

# Inhaltsverzeichnis

<b>Vorwort</b>	<b>IX</b>
<b>1 Einleitung</b>	<b>1</b>
1.1 Eine neue Art des Rechnens . . . . .	1
1.2 Über dieses Buch . . . . .	8
<b>2 Vom Bit zum Quantenregister</b>	<b>9</b>
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 Com- puting . . . . .	51
2.11 Verschränkung . . . . .	53
2.12 Die Hadamard-Transformation und mehrere Bits . . . . .	59
2.13 Der Algorithmus von Deutsch-Jozsa . . . . .	62
<b>3 Vom Quantenregister zum Quantenschaltkreis</b>	<b>67</b>
3.1 Laufzeit . . . . .	68
3.2 Klassische Schaltkreise und Komplexität . . . . .	75
3.3 Quantengatter und Quantenschaltkreise . . . . .	76
3.4 Quantenbits kopieren: Das No-Cloning-Theorem . . . . .	81
3.5 Umkehrbare Berechnungen . . . . .	84
3.6 Unterscheidbare Zustände . . . . .	93
3.7 Gestörte Berechnungen . . . . .	95
<b>4 Hilfsmittel aus der Theoretischen Informatik</b>	<b>101</b>
4.1 Komplexitätsklassen . . . . .	101
4.2 Randomisierte Algorithmen . . . . .	106
4.2.1 Mit dem Zufall rechnen . . . . .	106

4.2.2	Ein Primzahltest . . . . .	107
4.2.3	Probabilistische Komplexitätsklassen . . . . .	110
4.3	Unlösbare Probleme? NP-Vollständigkeit . . . . .	114
4.4	Quantenkomplexitätstheorie . . . . .	118
4.5	Die Churchsche These . . . . .	121
<b>5</b>	<b>Teleportation und dichte Kodierung</b>	<b>125</b>
5.1	Quantenteleportation . . . . .	127
5.2	Dichte Kodierung . . . . .	131
5.3	Verschänkte Bits . . . . .	133
<b>6</b>	<b>Suchen</b>	<b>137</b>
6.1	Die Nadel im Heuhaufen . . . . .	138
6.2	Die Grover-Iteration . . . . .	140
6.3	Eine geometrische Veranschaulichung . . . . .	146
6.4	Varianten der Quantensuche . . . . .	153
6.4.1	Suche nach einer von mehreren Lösungen . . . . .	153
6.4.2	Suche bei unbekannt vielen Lösungen . . . . .	155
6.4.3	Die Suche nach dem Minimum . . . . .	156
6.4.4	Zählen . . . . .	159
6.5	Anwendungen von Grovers Algorithmus . . . . .	159
6.6	Grovers Algorithmus ist von optimaler Größenordnung . . . . .	161
6.7	Folgen für die Fähigkeiten von Quantencomputern . . . . .	166
<b>7</b>	<b>Geheime Botschaften</b>	<b>169</b>
7.1	Alice, Bob und Eve . . . . .	170
7.2	Quantenverschlüsselung: das BB84-Protokoll . . . . .	175
7.3	Lauschstrategien . . . . .	183
7.4	Quantenverschlüsselung mit Verschränkung . . . . .	188
<b>8</b>	<b>Klassische Verschlüsselungen knacken: Primfaktorzerlegung</b>	<b>193</b>
8.1	Faktorisierung und Verschlüsselung: RSA-Kryptographie . . . . .	194
8.2	Die Suche nach Perioden . . . . .	199
8.3	Die schnelle Fouriertransformation . . . . .	207
8.4	Die Quanten-Fouriertransformation . . . . .	214
8.5	Simons Algorithmus . . . . .	218
8.6	Shors Algorithmus . . . . .	223
8.7	Jenseits von Shor . . . . .	231
<b>9</b>	<b>Quantenhardware</b>	<b>237</b>
9.1	Anforderungen . . . . .	237
9.2	Dekohärenz . . . . .	238
9.3	Photonen . . . . .	241
9.3.1	Mach-Zehnder-Interferometer . . . . .	241
9.3.2	Zufallszahlen . . . . .	244
9.3.3	Kryptographie . . . . .	245
9.4	Kernspinresonanz . . . . .	249
9.5	Ionenfallen . . . . .	251

9.6	Einwegberechnungen mit Clusterzuständen . . . . .	252
9.7	Supraleiter . . . . .	255
9.8	Adiabatische Quantencomputer . . . . .	257
<b>10</b>	<b>Zur Geschichte der Quantenmechanik</b>	<b>263</b>
10.1	Max Planck: das Quantum der Wirkung . . . . .	263
10.2	Albert Einstein: Spukhafte Fernwirkung . . . . .	265
10.3	Niels Bohr: Kopenhagen . . . . .	266
10.4	Werner Heisenberg: Ein großes Quantenei . . . . .	269
10.5	Erwin Schrödinger: Katzen und Wellen . . . . .	271
10.6	Zur Geschichte des Quantencomputers . . . . .	272
<b>A</b>	<b>Mathematische Grundlagen</b>	<b>275</b>
A.1	Komplexe Zahlen . . . . .	275
A.2	Vektorräume . . . . .	277
A.2.1	Was sind Vektorräume? . . . . .	277
A.2.2	Basen und Unterräume . . . . .	279
A.2.3	Winkel und Abstände in einem Vektorraum . . . . .	280
A.2.4	Projektionen . . . . .	282
A.3	Matrizen . . . . .	283
A.4	Kombinatorik und Wahrscheinlichkeit . . . . .	285
A.5	Ganze Zahlen . . . . .	287
A.5.1	Teiler und Vielfache . . . . .	287
A.5.2	Modulares Rechnen . . . . .	287
A.5.3	Zur Division . . . . .	289
<b>B</b>	<b>Lösungen ausgewählter Übungsaufgaben</b>	<b>291</b>
	<b>Literatur</b>	<b>299</b>
	<b>Symbole und Abkürzungen</b>	<b>305</b>
	<b>Quantengatter</b>	<b>306</b>
	<b>Namen- und Sachwortverzeichnis</b>	<b>307</b>