
Inhaltsverzeichnis

1	Einführung	1
1.1	Historisches	1
1.2	Motivation und Inhalt	4
1.3	Was in diesem Buch nicht behandelt wird	7
1.4	Anmerkungen zur Notation und Literatur	8
2	Grundbegriffe der Quantenmechanik	9
2.1	Allgemeines	9
2.2	Mathematisches: Hilbert-Raum und Operatoren	11
2.3	Physikalisches: Zustände und Observable	20
2.3.1	Reine Zustände	20
2.3.2	Gemischte Zustände	31
2.4	Qbits	40
2.5	Operatoren auf Qbits	46
3	Zusammengesetzte Systeme und Tensorprodukte	57
3.1	Auf dem Weg zum Qbyte	57
3.2	Tensorprodukte von Hilbert-Räumen	58
3.2.1	Definition	58
3.2.2	Die Rechenbasis	63
3.3	Zustände und Observable für zusammengesetzte Systeme	67
3.4	Schmidt-Zerlegung	76
4	Verschränkung	79
4.1	Allgemeines	79
4.2	Definition und Charakterisierung	81
4.3	Erzeugung verschränkter Zustände ohne Wechselwirkung	84
4.4	Das Einstein-Podolsky-Rosen-Paradoxon	86
4.5	Bell'sche Ungleichungen	91
4.5.1	Die ursprüngliche Bell'sche Ungleichung	91
4.5.2	Die CHSH-Verallgemeinerung der Bell'schen Ungleichung	97

4.6	Zwei unmögliche Apparate	104
4.6.1	Bell'sches Telefon	104
4.6.2	Der perfekte Quantenkopierer	107
5	Quantengatter und Schaltkreise für elementare Rechenoperationen	111
5.1	Klassische Gatter	111
5.2	Quantengatter	116
5.2.1	Unäre Quantengatter	117
5.2.2	Binäre Quantengatter	122
5.2.3	Allgemeine Quantengatter	123
5.3	Zum Ablauf von Quantenalgorithmen	147
5.3.1	Vorbereitung des Input- und Nutzung des Arbeitsregisters .	148
5.3.2	Implementierung von Funktionen und Quantenparallelismus	151
5.3.3	Auslesen des Outputregisters	155
5.4	Schaltkreise für elementare Rechenoperationen	156
5.4.1	Quantenaddierer	156
5.4.2	Quantenaddierer modulo N	168
5.4.3	Quantenmultiplikator modulo N	172
5.4.4	Quantenschaltkreis für Exponentiation modulo N	176
5.4.5	Quanten-Fourier-Transformation	180
6	Vom Nutzen der Verschränkung	189
6.1	Dichte Quantenkodierung	189
6.2	Teleportation	191
6.3	Quantenkryptografie	193
6.3.1	Allgemeines zur Kryptografie	193
6.3.2	Schlüsselverteilung ohne Verschränkung	195
6.3.3	Schlüsselverteilung mit verschränkten Zuständen	198
6.3.4	Öffentliche Schlüsselverteilung nach RSA	201
6.4	Shors Algorithmus zur Faktorisierung großer Zahlen	206
6.4.1	Allgemeines	206
6.4.2	Der Algorithmus	207
6.4.3	Schritt 1: Auswahl von b und Berechnung von $ggT(b, N)$.	210
6.4.4	Schritt 2: Periodenbestimmung mit Quantencomputern . . .	211
6.4.5	Schritt 3: Wahrscheinlichkeit der Auswahl eines geeigneten b	224
6.4.6	Bilanzierung der Schritte	230
6.5	Grovers Suchalgorithmus	235
6.5.1	Suchalgorithmus bei bekannter Anzahl von gesuchten Objekten	235
6.5.2	Suchalgorithmus bei unbekannter Anzahl von gesuchten Objekten	246
7	Nachwort	253

8	Anhang A – Elementare Wahrscheinlichkeitstheorie	255
9	Anhang B – Elementare Rechenoperationen	259
10	Anhang C – Landau-Symbole	267
11	Anhang D – Modulare Arithmetik	269
12	Anhang E – Kettenbrüche	297
13	Anhang F – Lösungen	309
	13.1 Lösungen zu Übungen aus Kap. 2	309
	13.2 Lösungen zu Übungen aus Kap. 3	322
	13.3 Lösungen zu Übungen aus Kap. 4	324
	13.4 Lösungen zu Übungen aus Kap. 5	329
	13.5 Lösungen zu Übungen aus Kap. 6	335
	13.6 Lösungen zu Übungen aus Kap. 9	341
	13.7 Lösungen zu Übungen aus Kap. 10	341
	13.8 Lösungen zu Übungen aus Kap. 11	342
	Literatur	345
	Sachverzeichnis	349