

7 Wie baut man einen Quantencomputer?	72
7.1 Quantengatter	73
7.2 Ionenfallen	76
7.3 Kernspinresonanz	79
7.4 Quantenpunkte	81

VERTIEFUNGEN

Superdichte Kodierung	84
Fälschungssichere Banknoten	86
Quantenkryptographie mit Verschränkung	87
Dekohärenz	90
Quantenfehlerkorrektur	92
Einfache Quantennetzwerke	95
Verschränkungstheorie	100
Destillation und Reinigung	105
Zahlentheoretische Grundlagen zum Shor-Algorithmus	109
Präzisionsmessungen als Quantentechnologie	112
Quantenspiele	115

ANHANG

Glossar	120
Literaturhinweise	127

1 WAS IST INFORMATION?

Der Begriff »Information« – der lateinische Wortstamm *informatio* bedeutet »Nachricht, Auskunft« – ist in unserem Alltagsleben allgegenwärtig und gehört, im Gegensatz zu vielen anderen Fachausdrücken der Physik, zum allgemeinen Wortschatz. In der heutigen »Informationsgesellschaft« werden tagtäglich riesige Datenmengen verschiedenster Art verarbeitet und vom jeweiligen Sender zum jeweiligen Empfänger übermittelt.

Ein zentrales Thema in der klassischen Informationstheorie ist das Lösen von mathematischen Problemen mittels Algorithmen (methodische Rechenverfahren); ein weiteres die sichere Übermittlung geheimer Daten (etwa Kreditkartennummern im Internet), d. h. die Verschlüsselung, Übertragung und Entschlüsselung einer so genannten »Nachricht«. Eine Nachricht ist eine Kette von so genannten »Buchstaben«, die wiederum aus einem »Alphabet« gewählt werden. Dies kommt Ihnen sicher selbstverständlich vor, denn Sie lesen ja gerade eine solche Folge von Buchstaben aus dem deutschen Alphabet. Die in der Botschaft enthaltene Information hängt dabei nicht von der Wahl des Alphabets ab: Es wäre beispielsweise denkbar, denselben Text (der daher auch denselben Informationsgehalt trägt) mit Hilfe von griechischen Buchstaben zu schreiben, also α statt a und β statt b und so fort. Die Wahl des Alphabets hängt natürlich von der Zielsetzung und von der geplanten Anwendung ab.

Die Verarbeitung, Speicherung und Übertragung von Information beruht heutzutage hauptsächlich auf dem Computer. Das Alphabet, das für die Anwendung mit dem Computer sinnvoll ist, und daher im Folgenden benutzt werden wird, ist das einfachste denkbare. Es besteht nur aus den zwei Zeichen 0 und 1. Ein solches *binäres* Alphabet lässt sich physikalisch einfach verwirklichen, z. B. durch eine hohe

bzw. niedrige Spannung. Jedes andere Alphabet kann man durch eine einfache Vorschrift in das binäre Alphabet übersetzen: Jedem Buchstaben des Alphabets wird eine Zahl im Dezimalsystem zugeordnet, also dem ersten eine 1, dem zweiten eine 2 usw. Diese Zahl wird vom Dezimalsystem ins Binärsystem übersetzt – da man im Binärsystem nur die beiden Ziffern 0 und 1 zur Verfügung hat, zählt man dort wie folgt: auf »001« folgt »010«, darauf »011«, danach »100« und so fort. Der Buchstabe »D« ist beispielsweise der 4. Buchstabe in unserem Alphabet, und die »4« des Dezimalsystems wird im Binärsystem zu »100«. – Im Folgenden wird, wenn nicht anders angegeben, stets von binären Alphabeten die Rede sein.

Die Einheit der klassischen Information wird auch als »Bit« (Abkürzung für *binary digit*) bezeichnet: Hat man einen elementaren Informationsträger zur Verfügung, z. B. eine Kiste, die einen Ball enthält (entspricht 1) oder nicht (entspricht 0), so kann man damit ein Bit an Information übertragen. Sprachlich etwas ungenau wird oft keine Unterscheidung zwischen dem Informationsgehalt und dem Binärzeichen selbst (dem Träger der Information) gemacht, da beide als Bit bezeichnet werden.

Der Empfänger erhält die Information, indem er eine Messung am Informationsträger durchführt: im Fall der Kiste öffnet er sie und sieht nach, ob ein Ball darin ist (Ereignis »1«) oder nicht (Ereignis »0«). Das Auftreten der Ereignisse »0« bzw. »1« geschehe dabei mit den Wahrscheinlichkeiten p_0 bzw. p_1 , wobei $p_0 + p_1 = 1$. Man kann Information auch als Mangel an (Vor-)Wissen interpretieren: Ist z. B. $p_0 = 1$, so ist klar, dass in jedem Fall die Kiste leer ist. Man lernt also nichts dazu, wenn man sie öffnet. Ist das Unwissen maximal, d. h. $p_0 = p_1 = 1/2$, so gewinnt man am meisten Information bei der Messung. Claude Shannon entwickelte die Theorie der mathematischen Quantifizierung des intuitiven Konzepts der Information und zeigte die Äquivalenz zwischen Information und Entropie.

1.1 Information ist physikalisch

Der Duden gibt folgende Definition für Information: »als räumliche oder zeitliche Folge physikalischer Signale, die mit bestimmten Wahrscheinlichkeiten oder Häufigkeiten auftreten, sich zusammensetzende Mitteilung, die beim Empfänger ein bestimmtes (Denk)verhalten bewirkt.« Wesentliche Beachtung verdient hier das Wort »physikalisch«. Information ist nicht nur ein abstrakter Begriff: Bei der Übertragung von Information erfolgt immer die Umsetzung einer Nachricht in ein physikalisches Medium. Beispielsweise benutzen Winnetou und Old Shatterhand u. a. optische Mittel (Rauch- oder Feuerzeichen) zur Informationsübertragung. Wenn man eine Nachricht spricht, so wird sie in akustische Wellen umgewandelt, die wiederum beim Zuhörer empfangen und über Ohr und Gehirn in ein Signal verwandelt und interpretiert werden. Bei der digitalen Informationsverarbeitung in einem Computer werden 0 und 1 durch eine hohe bzw. niedrige Spannung kodiert. Diese drei Beispiele betreffen drei wichtige Teilbereiche der Physik: Optik, Akustik und Elektrodynamik. Jede der beschriebenen Methoden hat Vor- und Nachteile, die durch die physikalische Implementation bedingt sind: z. B. ist die optische Informationsübertragung nur dann möglich, wenn kein Hindernis im Weg steht, die akustische nur dann, wenn nicht zu viel Hintergrundrauschen vorhanden ist.

Die bedeutsamste klassische Methode der Informationsverarbeitung ist sicherlich der Computer. Hier hat die Weiterentwicklung der Halbleitertechnologie zu immer kleineren Bauteilen und immer höheren Geschwindigkeiten geführt. In absehbarer Zeit wird man durch die Miniaturisierung der Bauteile an die Quantengrenze stoßen. Welche Neuerungen ergeben sich, wenn die Gesetze der Quantenphysik eine dominante Rolle bei der Informationsverarbeitung spielen?

Die weitreichenden Konsequenzen und vielfältigen neuen Möglichkeiten, die sich aus der Symbiose von klassischer Informations-

theorie und Quantenphysik – der Quanteninformation – ergeben, werden erst seit den 60er Jahren des 20. Jahrhunderts intensiv erforscht. Da es sich um einen jungen Forschungsbereich handelt, der sich weiterhin rasant entwickelt, kann dieses Buch nur auf die grundlegenden Prinzipien der Quanteninformation eingehen und eine Momentaufnahme des derzeitigen Wissensstands liefern.

Bevor wir dazu kommen, jedoch zunächst eine Einführung in wichtige Konzepte der klassischen Informationstheorie.

1.2 Die Turingmaschine

Alan Turing entwickelte 1936 ein abstraktes Konzept eines Computers, die so genannte Turingmaschine. Sie kann alle Funktionen berechnen, die berechenbar sind. Die Elemente, aus denen sie besteht, sind die folgenden (siehe Abb. 1):

1. Eine endliche Menge von internen Zuständen der Maschine (einschließlich eines Anfangs- und eines Endzustands).
2. Ein unendlich langes Band, das in Segmente unterteilt ist, die »0« oder »1« oder »leer« enthalten. Der Startpunkt ist vorgegeben.
3. Ein Schreib- und Lesekopf, der jeweils auf ein Segment des Bandes zeigt.
4. Ein Programm aus endlich vielen Zeilen.

Eine Programmzeile gibt eine Vorschrift für einen gegebenen internen Zustand der Maschine und einen gegebenen Eintrag auf dem Band an. Diese Vorschrift besagt, ob der interne Zustand der Maschine geändert wird oder nicht, ob der Eintrag auf dem Band überschrieben wird oder nicht, und ob sich der Schreib- und Lesekopf danach einen Schritt nach rechts oder links bewegt.

Ein einfaches Beispiel für ein solches Programm ist das Auffinden der Parität einer gegebenen Folge von Nullen und Einsen. (Bei einer

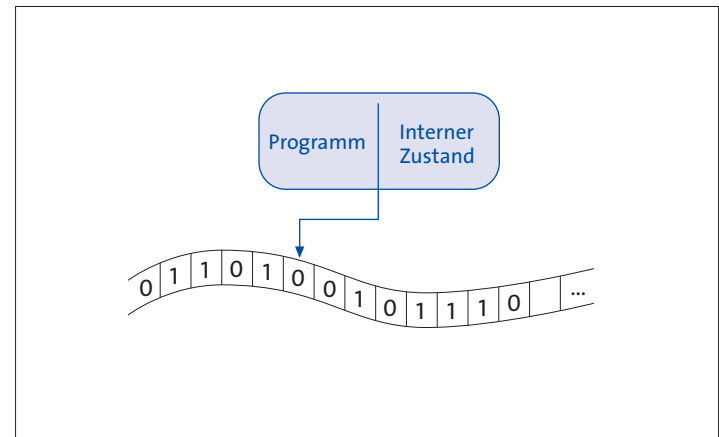


Abb. 1: Die Elemente einer Turingmaschine.

geraden Anzahl von Einsen spricht man von gerader, ansonsten von ungerader Parität.) Hierzu sei der interne Zustand der Maschine anfänglich 0. Der Lese- und Schreibkopf liest den jeweiligen Eintrag auf dem Band. Ist der Eintrag 1, so wird der interne Zustand der Maschine geändert, d. h. wenn er 0 war, wird er zu 1 und umgekehrt. Ist der Eintrag auf dem Band aber gleich 0, so bleibt der interne Zustand ungeändert. Danach rückt der Kopf einen Schritt nach rechts. Das Auftreten eines leeren Segments des Bandes bedeutet das Anhalten der Turingmaschine: Ist nun ihr interner Zustand 0, so hat die getestete Folge von Nullen und Einsen gerade, ansonsten ungerade Parität.

Über dieses abstrakte Konzept eines Computers kann die Komplexität von mathematischen Problemen definiert werden, wie im nächsten Kapitel erläutert. Das Modell der klassischen Turingmaschine kann ferner auf das Modell eines Computers erweitert werden, der auf quantenphysikalischen Prinzipien beruht – die Quanten-Turingmaschine.