Können Quanten rechnen?

Quanteninformatik – Einführung in die Grundprinzipien

Teil 1: Grundbegriffe der Quantenphysik

von Peter Bussemer

Um die Grundzüge des *Rechnens mithilfe von Quanten* als eine Anwendung der Quantenphysik und die Grundlagen des interdisziplinären Forschungsgebiets *Quanteninformatik* zu verstehen, werden in dieser Artikelserie zunächst die wesentlichen Begriffe der Quantentheorie entwickelt. Anschließend wird das Quantenbit definiert und auf die Besonderheiten des reversiblen Rechnens eingegangen; auch werden einige Ein- und Zweibit-Operationen vorgestellt. Ein einfacher Quantenalgorithmus zeigt (in der Reduktion der Rechenzeit gegenüber klassischen Algorithmen) den Vorteil der Nutzung quantentheoretischer Phänomene wie Überlagerung und Verschränkung. Die neuen Möglichkeiten bei der Chiffrierung (Quantenkryptografie) und der Nachrichtenübertragung (Quantenteleportation) werden diskutiert, ebenso der Entwicklungsstand der Quantenhardware.

Physik und Informatik

Die modernen Computer, die die logischen Operationen mittels Silizium-Chips realisieren, arbeiten auf der Grundlage der Gesetze der klassischen Physik (Mechanik, Elektrodynamik, Thermodynamik). In den letzten Jahrzehnten hat sich ihre Leistungsfähigkeit nach dem sogenannten Moore'schen Gesetz ständig verbessert, mit dem behauptet wird, dass sich die Anzahl der auf einem Chip integrierten Transistoren alle zwei Jahre verdoppelt (inzwischen geht man von anderthalb Jahren aus). Dieses exponentielle Wachstum ist mit einer starken Miniaturisierung der Rechnerkomponenten verbunden, sodass in absehbarer Zeit Strukturen von einer charakteristischen Breite von etwa 10 nm, etwa 100 Atomen entsprechend, notwendig werden. Damit gelangt man in den Bereich der Nanotechnologie, wo bereits die in der Mikrowelt geltenden Gesetze der Quantentheorie zu berücksichtigen sind.

Die in den Zwanzigerjahren des vorigen Jahrhunderts von Werner Heisenberg, Erwin Schrödinger, Paul Dirac und anderen entwickelte Quantenmechanik bedient sich zur Beschreibung des physikalischen Verhaltens der Mikroobjekte (Quanten) einer im Gegensatz zur anschaulichen Newton'schen Mechanik recht abstrakten mathematischen Sprache. Dennoch hat ihre Anwendung bereits zu technischen Errungenschaften wie Transistor, Laser u.a. geführt, die in Geräten wie PC, CD, DVD und Mobiltelefon alltagstauglich geworden sind.

Auch in der Rechentechnik und Informatik gibt es seit den Achtzigerjahren Bemühungen, die eigenartigen Gesetzmäßigkeiten des Quantenverhaltens für den Rechenprozess selbst zu nutzen – beginnend mit einem Vortrag des amerikanischen Physikers Richard Feynman (1918–1988) unter dem Titel *There's Plenty of Room at the Bottom* (1959), wo er die Frage stellte, warum wir nicht alle 24 Bände der *Encyclopædia Britannica* auf eine Nadelspitze schreiben können, wo doch übergenug Platz vorhanden sei (Bild 1). In seinem Artikel *Simulating Physics with Computers* (1982), der häufig als Geburtsstunde des Quantencomputers angesehen wird, stellte Feynman fest, dass es extrem schwierig ist, quantenmechanische Systeme auf klassischen Computern zu berechnen. Als Ausweg überlegte er, ob nicht eventuell jedes beliebige quantenmechanische System von einer Maschine simuliert werden könne, die selbst auf quantenmechanischen Prinzipien beruht.

Seither wird auf den Gebieten des Quantenrechnens und der Quanteninformatik eine intensive Forschung betrieben, die bereits zu ersten Implementationen kleiner Prototypen von Quantenrechnern geführt hat. Die klassischen Bits mit den logischen Werten 0 und 1 werden durch *Quantenbits* (Qubits) ersetzt, die einen Überlagerungszustand der klassischen Bits darstellen und ein prinzipiell paralleles Rechnen (*Quantenparallelismus*) ermöglichen. Zum Verständnis der Besonderheiten des Quantenverhaltens wird (im vorliegenden ersten Teil dieser Beitragsserie) ein Graphenmodell mittels Adjazenzmatrizen analysiert, wobei der Übergang vom klassisch-deterministischen zum quantentheoretisch-proba-

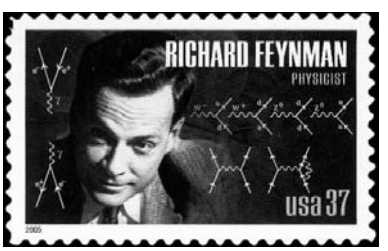

Bild 1: Richard P. Feynman: „Es ist noch viel Platz da unten" (1959).
Physics-Related Stamps

bilistischen Verhalten mit der Möglichkeit von Interferenzeffekten erfolgt. Diese *Überlagerungen* (Superpositionen) verknüpfen die Qubits miteinander. Die zur Ausführung von Algorithmen notwendigen Rechenschritte werden durch unitäre (reversible) Operatoren (sogenannte Quantengatter) ausgeführt, die im Wesentlichen mit Ein- und Zwei-Bit-Operationen auskommen. Eine wichtige Rolle spielen die *verschränkten Zustände*, die die beiden Bits korrelieren lassen und in der klassischen Physik kein Analogon besitzen.

Die Analyse eines einfachen Quantenalgorithmus zum Auffinden einer Boole'schen Funktion zeigt den Vorteil solcher Superpositionen gegenüber klassischen Algorithmen, der bei komplizierteren Problemen so beträchtlich werden kann, dass beispielsweise bisher als sicher betrachtete Chiffriermethoden sich künftig als unsicher erweisen könnten, worüber im dritten Teil dieses Collegs berichtet werden soll.

Systeme der klassischen Physik

Um die Besonderheiten quantenmechanischer Systeme zu verstehen, gehen wir zunächst von einem klassischen System aus, das durch ein deterministisches Verhalten charakterisiert ist. Im nächsten Schritt modifizieren wir das System durch den Übergang zu einem nicht-deterministischen Verhalten, indem wir den Zustandsübergängen reelle Zahlen als Wahrscheinlichkeiten zuordnen. Erst die Zulassung komplexer Zahlen führt zur Beschreibung echten Quantenverhaltens, mit den Effekten von Überlagerung und Interferenz – entsprechend dem Wellencharakter der Quantenteilchen.

Klassische deterministische Systeme

Wir gehen von einem Graphen aus, einer in der Informatik häufig vorkommenden mathematischen Struktur, bestehend aus einer Menge von Punkten („Knoten") und einer Menge von Verbindungslinien („Kanten"). Auf die Kanten setzen wir Spielsteine, die schrittweise („Klick") verschoben werden können, und definieren damit die Dynamik des Systems. Der Anfangszustand wird durch einen Spaltenvektor **x** festgelegt, der angibt, wie viele Steine sich auf welchem Knoten befinden.

Beispiel: $\mathbf{x} = (6, 2, 1)^T$ bedeutet, dass sich 6 Steine auf dem ersten Knoten befinden, 2 auf dem zweiten usw. Die Topologie des Graphen wird durch eine *Adjazenzmatrix* M erfasst (auch *Nachbarschaftsmatrix* genannt), deren Elemente $M_{ij} = 1$ sind, falls eine gerichtete Kante (Pfeil) von Knoten j nach Knoten i zeigt, andernfalls ist $M_{ij} = 0$. Wendet man M auf den Anfangszustand **x** an, so ergibt sich ein neuer Zustand $\mathbf{y} = M\mathbf{x}$, entsprechend einer Verschiebung der Spielsteine mit einem Klick. Das System geht vom Zustand **x** zur Zeit t in den Folgezustand **y** zum Zeitpunkt t + 1 über. Anwendung von M auf **y** liefert den zweiten Folgezustand zu **x**, nämlich $\mathbf{z} = M\mathbf{y} = (M \cdot M)\mathbf{x} = M^2\mathbf{x}$. Das heißt: Das Quadrat der Matrix M gibt den Systemzustand nach zwei Zeitschritten (bei t + 2) an. Die Matrixelemente von M^2 sind nur dann $\neq 0$, wenn ein durchgehender Weg („Pfad") der Länge 2 von j nach i existiert. Entsprechend muss es für k Schritte einen Pfad der Länge k geben.

Klassische stochastische Systeme

Um die Besonderheiten des quantentheoretischen Verhaltens zu verstehen, verlassen wir zunächst unsere klassische Systembeschreibung noch nicht, berücksichtigen jedoch die Möglichkeit zufälligen Verhaltens. Während bei einem deterministischen System von einem bestimmten Knoten stets nur ein Pfeil ausgeht, der eindeutig den Nachfolgerknoten festlegt, verwenden wir jetzt gewichtete Graphen, bei denen die Pfeile mit reellen Zahlen zwischen 0 und 1 bewertet werden. Diese Zahlen geben die Übergangswahrscheinlichkeiten dafür an, dass ein Spielstein vom Knoten j zum Knoten i verschoben wird.

Beispiel: Graph mit drei Knoten i = 0, 1, 2. Die Adjazenzmatrix lautet:

$$M = \begin{pmatrix} 0 & 1/6 & 5/6 \\ 1/3 & 1/2 & 1/6 \\ 2/3 & 1/3 & 0 \end{pmatrix},$$

wobei etwa $M_{01} = 1/6$ bedeutet, dass der Übergang vom Knoten 1 zum Knoten 0 mit der Wahrscheinlichkeit 1/6 erfolgt. Wegen der Normierung der Wahrscheinlichkeiten müssen in M sowohl die Spalten- als auch die Zeilensummen = 1 sein (doppelt-stochastische Matrix).

Der Anfangszustand **x** wird jetzt durch die Angabe der Wahrscheinlichkeit p beschrieben, mit der sich ein Spielstein an einem bestimmten Knoten befindet (Aufenthaltswahrscheinlichkeit). Ist beispielsweise $\mathbf{x} = (1/6, 1/6, 2/3)^T$, so befindet sich der Stein mit p = 1/6 am Knoten Nr. 0 usw. Für beliebige Zustandsvektoren muss die Summe der Komponenten = 1 sein, da sich der Stein auf irgendeinem der Knoten befindet (sicheres Ereignis). Nach Anwendung von M ergibt sich der neue Zustand **y** (zum Zeitpunkt t + 1):

$\mathbf{y} = M\mathbf{x} = (21/36, 9/36, 6/36)^T$.

Kehrt man die Pfeilrichtungen im Graphen um, so wird der Rückwärtsprozess von t nach t – 1 beschrieben. Hierzu sind in der Adjazenzmatrix M die Zeilen und Spalten zu vertauschen, d.h. man bildet die transponierte Matrix M^T. Bei zeitinvarianten Systemen sind die Prozesse reversibel, weshalb die Kombination von M und M^T zum Ausgangszustand zurückführt:

$M \cdot M^T = M^T \cdot M = E$

mit E als Einheitsmatrix. Die transponierte Matrix M^T ist somit hier gleich der inversen Matrix M^{-1}. Analog zu vorher bedeutet das Quadrat $M \cdot M = M^2$ die Ausführung von zwei Zeitschritten. Das Matrixelement M^2_{ij} gibt die Wahrscheinlichkeit dafür an, in 2 Schritten vom Knoten j zum Knoten i zu gelangen.

Beispiel (klassisches stochastisches Billardspiel): Eine Kugel kann sich auf 4 Knoten bewegen, wobei die mög-

Fortsetzung übernächste Seite

Von der klassischen Physik zur Quantenphysik

Einstein: „Gott würfelt nicht."
Bohr: „Sie behaupten also, Gottes Handeln zu kennen?"

Vor mehr als dreihundert Jahren schuf Isaac Newton (1643–1727) mit der Aufstellung seiner Bewegungsgesetze für feste Körper und mit seiner Gravitationstheorie die Grundlagen dessen, was wir heute als *klassische Physik* bezeichnen. Mehr als zweihundert Jahre hat das von ihm geprägte naturwissenschaftliche Weltbild unangefochten Gültigkeit besessen. Der Erfolg dieser Theorie für die Beschreibung von Bewegungen, insbesondere der von Himmelskörpern, führte Newton wohl dazu, auch das Verhalten des Lichts im Sinne von Teilchen, also festen (kleinen) Gegenständen, zu verstehen. Man sieht ja, dass Lichtstrahlen sich geradlinig fortpflanzen und dass Licht von einem Spiegel in ganz ähnlicher Weise abprallt wie ein Ball von einer harten Wand. Mit seiner *Korpuskulartheorie des Lichts* konnte Newton eine Reihe optischer Phänomene bis hin zur Brechung von Lichtstrahlen widerspruchsfrei erklären.

LOG-IN-Archiv

Newton:
Licht als Teilchenstrom.

Physics-Related Stamps

Huyghens:
Licht als Wellenfront.

Und doch gab es bereits zu Newtons Zeiten eine andere Erklärung. Der niederländische Physiker und Mathematiker Christiaan Huyghens (1629–1695) entwickelte die Vorstellung, dass Licht aus Stoßwellen besteht, die mit endlicher Geschwindigkeit durch den Äther laufen. Den Äther dachte er sich homogen und aus winzigen elastischen Partikeln bestehend. Jedes angeregte Ätherpartikel ist Ausgangspunkt einer schwachen Elementarwelle; diese zusammen ergeben durch Überlagerung die tatsächliche Lichtwellenfront (*Huyghens'sches Prinzip*). Die Wellentheorie erklärte Beugung und Brechung ebenso gut wie die Korpuskulartheorie, doch nahm sie im achtzehnten Jahrhundert (außer Leonhard Euler) kaum jemand ernst. Erst zu Beginn des neunzehnten Jahrhunderts stellten der Engländer Thomas Young (1733–1829) und der Franzose Augustin Fresnel (1788–1827) neue Experimente an, die zur *Wellentheorie des Lichts* führten, wobei als Trägermedium (nach wie vor) ein hypothetischer Äther diente. Als es dem schottischen Physiker James Clerk Maxwell (1831–1879) gelang, die Natur des Lichts auf die wellenförmig sich ausbreitenden Änderungen elektrischer und magnetischer Felder zurückzuführen und damit die Synthese von Optik und Elektrizitätslehre herzustellen, war der Triumph der Wellentheorie des Lichts vollendet. Die Entdeckung von Radiowellen durch Heinrich Hertz (1857–1894) um 1887 führte dann zu dem uns vertrauten theoretischen System der Elektrodynamik und der elektromagnetischen Wellen.

LOG-IN-Archiv

Ludwig Boltzmann.

Gleichzeitig formte sich im neunzehnten Jahrhundert – gegen vielfältige philosophische Einwände – der Begriff des Atoms und Moleküls heraus. Die kinetische Gastheorie Ludwig Boltzmanns (1844–1906) und die Erklärung der Brown'schen Molekularbewegung durch atomare Stöße mit Pollenkörnern durch Albert Einstein (1879–1955) im Jahr 1905 erhärteten das Bild vom atomaren Aufbau der Materie.

Als man nun zu Beginn des zwanzigsten Jahrhunderts versuchte, die Gesetze der klassischen Physik auf den atomaren Bereich zu übertragen, gelangte man zu Ergebnissen, die im Widerspruch zur Erfahrung standen. Dies erkannte man beispielsweise bei der Anwendung der Elektrodynamik auf das experimentell gut bestätigte *Rutherford'sche Atommodell*, wonach das Atom nach Art eines Planetensystems aus einem Kern und einer Anzahl von diesen umkreisenden Elektronen besteht. Letztere müssten bei dieser Bewegung kontinuierlich elektromagnetische Wellen aussenden und dadurch Energie verlieren, sodass sie schließlich in den Kern stürzen würden; danach gäbe es also keine stabilen Atome. Ebenso hatte es sich als unmöglich erwiesen, die Absorption und Emission von Strahlung durch die Atome nach der klassischen Physik in Übereinstimmung mit der Erfahrung zu erklären. Max Planck (1858–1947), ein im tiefsten Innern konservativer Physiker, machte anlässlich des Rätsels der Hohlraumstrahlung die revolutionäre Annahme, dass Energie „gequantelt", d.h. nur bestimmter diskreter Werte fähig sei. „In einer Art von Verzweiflung muss er wohl diesen Schluss der Quantelung des Lichtfeldes gezogen haben, der in krassem Widerspruch zur elektromagnetischen Feldtheorie von kontinuierlichen und magnetischen Feldern stand. Die Annahme führte in der Tat auf die verworfene Korpuskulartheorie des Lichtes von Newton zurück" (Lüth, 2009, S.2).

Physics-Related Stamps

Heinrich Hertz und
James Clerk Maxwell.

Max Planck schuf die Bezeichnung *Quanten*, die dem ganzen späteren Gebiet der Quantenphysik den Namen gab. Aus dem vergeblichen Bemühen, die Rutherford'sche Atomtheorie einerseits und die