# Mit Quanten kann gerechnet werden

Christina KRAUS
Max-Planck-Institut für Quantentechnik

## 1 Einleitung

Quantenmechanik ist ein Meilenstein der modernen Physik. Die Theorie, die in den letzten hundert Jahren unter anderem von Dirac und Heisenberg entwickelt wurde, hat bereits viele technische Anwendungen z. B. in Lasern oder Halbleitertransistoren gefunden. Bereits in den sechziger Jahren gab es Vorschläge, die Gesetze der Quantenmechanik zur Informationsverarbeitung zu verwenden. Die Konstruktion eines solchen Quantencomputers ist aktueller Forschungsgegenstand der Physik, Mathematik und Informatik. Im Folgenden möchte eine Einführung in dieses Gebiet geben.

## 2 Wozu brauchen wir einen Quantencomputer?

Informationsübertragung und -Verarbeitung sind wesentliche Technologien unserer Gesellschaft. War der Gebrauch von Computern vor etwa 25 Jahren auf den wissenschaftlichen Sektor beschränkt, so ist der PC aus unserem heutigen Leben kaum mehr wegzudenken. Die Entwicklung neuer Computer findet dabei mit rasanter Geschwindigkeit statt. Bereits im Jahre 1965 legte J. Moore, einer der Gründer der Firma Intel, als Zielvorgabe fest, dass sich die Zahl der Transistoren auf einem Chip alle 18 Monate verdoppeln solle. Diese als „Mooresches Gesetz“ bekannt gewordene Vorgabe ist anstelle von 18 für 24 Monate tatsächlich Wirklichkeit geworden. Geht man davon aus, dass sich der technologische Fortschritt ungebremst fortsetzen kann, so wird die heutige Transistortechnik gegen das Jahr 2020 an ihre physikalischen Grenzen stoßen. Zur weiteren Effizienzsteigerung wird man dann so kleine Systeme verwenden müssen, dass Effekte der Quan-

tenmechanik signifikant werden. Davon abgesehen verspricht ein Quantencomputer eine minutenschnelle Lösung von Problemen, die auf einem herkömmlichen Computer Hunderte von Jahren benötigen würde. Das bekannteste dieser Probleme ist die Faktorisierung großer Zahlen. Zur Verschlüsselung bei Informationsübertragung z. B. im Internet wird das Public-Key System verwendet. Als Schlüssel dient eine sehr große Zahl N, die das Produkt zweier Primzahlen p und q ist. Da zur Entschlüsselung sowohl p als auch q bekannt sein müssen, kann der Schlüssel N öffentlich bekannt gegeben werden. Der Grund dafür ist, dass es mittels heutiger Computer Jahre dauert, um die beiden Primzahlen p und q aus N zu bestimmen. Mittels eines Quantencomputers könnten p und q aber innerhalb weniger Minuten aus N bestimmt werden.

Um die Funktionsweise eines Quantencomputers erläutern zu können, möchte ich zuerst die für das Verständnis notwenigen Grundlagen der Quantenmechanik erläutern.

## 3 Eine Einführung in die Quantenmechanik

Die Welt, die wir täglich erleben, unterliegt den Gesetzen der klassischen Physik, insbesondere ist sie deterministisch. Lassen wir einen Stein fallen, so können wir mittels der klassischen Mechanik vorhersagen, wann der Stein auf dem Boden aufschlagen wird. Die Gesetze, die unseren Alltag zeichnen verlieren jedoch ihre Gültigkeit, sobald wir uns mit Systemen von atomarer Größe beschäftigen. Auf diesen Längenskalen gelten die Gesetze der Quantenmechanik, die nur Wahrscheinlichkeitsaussagen über den Ausgang von Messungen machen. Die wichtigsten Eigenschaften quantenmechanischer Systeme sind *die Superposition von Zuständen* und *Verschränkung*. Diese Begriffe werden im Folgenden am Beispiel eines Elektron-Positron-Systems erklärt.

Elektronen und Positronen sind neben ihrer Masse und ihrer Ladung noch durch ihren Spin charakterisiert. Der Spin ist eine Eigenschaft, den quantenmechanische Systeme haben können, und die Tatsache, dass so etwas wie ein Spin existiert, findet z. B. in der Kernspintomographie eine Anwendung. Wie die Geschwindigkeit ist der Spin eine vektorielle Größe, d. h. er hat einen Betrag und eine

Richtung. Wichtig ist nun, dass der Spin eine so genannte quantisierte Größe ist. Möchte man in einem Experiment messen, wie groß die Komponente des Spins in eine Richtung, z. B. die z-Richtung ist, so stellt man fest, dass man nur zwei mögliche Messergebnisse erhalten kann, und zwar $\eta / 2$, wobei $\eta$ (Plancksches Wirkungsquantum) eine Naturkonstante ist. In der Quantenmechanik beschreibt man dieses Phänomen, indem man ein Teilchen, dessen Messung der z-Komponente des Spins $+ \eta / 2$ ergibt, durch $|\uparrow\rangle$ beschreibt, und im Falle von $- \eta / 2$ durch $|\downarrow\rangle$. Betrachten wir nun ein Elektron $e^-$ und ein Positron $e^+$, die beim Zerfall eines Pions $\pi^0$, einem Elementarteilchen mit Spin Null, entstehen (siehe Abb. 1). Die Gesetze der Physik sagen uns, dass von den beiden entstehenden Teilchen eines im Zustand $|\uparrow\rangle$ und das andere im Zustand $|\downarrow\rangle$ sein muss. Jedoch macht die Quantenmechanik keine Aussage, welches der beiden Elektronen in welchem Zustand ist. Das liegt nicht daran, dass die Quantenmechanik eine unvollständige Theorie ist, sondern dass quantenmechanische Systeme intrinsisch, nicht deterministisch sind, d. h. es sind nur Wahrscheinlichkeitsaussagen möglich. Jedes der beiden Teilchen für sich genommen wird nun folgendermaßen beschrieben:

$$\left|\Psi\right\rangle = \frac{1}{\sqrt{2}}\left(\left|\uparrow\right\rangle + \left|\downarrow\right\rangle\right) \tag{1}$$

$\left|\Psi\right\rangle$, die so genannte Wellenfunktion, beschreibt den Zustand quantenmechanischer Systeme. Ganz allgemein kann ein Elektron oder Positron im Zustand

$$\left|\Psi\right\rangle_{e^\pm} = a\left|\uparrow\right\rangle + b\left|\downarrow\right\rangle \tag{2}$$

sein, wobei a und b komplexe Zahlen sind, und $|a|^2$ bzw. $|b|^2$ die Wahrscheinlichkeit angeben, mit der man bei einer Messung die Ergebnisse $+ \eta / 2$ bzw. $- \eta / 2$ erhält. Die Wellenfunktion aus Gleichung (1) besagt also, dass wir bei der Spinmessung an einem der beiden Teilchen mit 50 % Wahrscheinlichkeit den Messwert $+ \eta / 2$ erhalten und mit 50 % Wahrscheinlichkeit den Messwert $- \eta / 2$. Der Zustand des Teilchens ist also eine Superposition der Zustände $|\uparrow\rangle$ und $|\downarrow\rangle$.

Wie bereits erwähnt können wir zwar keine Aussage machen, welchen Spin wir an dem linken oder rechten Teilchen messen werden,

doch wissen wir etwas über den Gesamtzustand der beiden Teilchen. Angenommen, wir haben den Spin des rechten Teilchens gemessen, und erhalten als Messergebnis z. B. $+\eta/2$. Dann sagen uns die Gesetze der Physik, dass wir bei der Messung des linken Teilchens den Messwert $-\eta/2$ erhalten müssen.

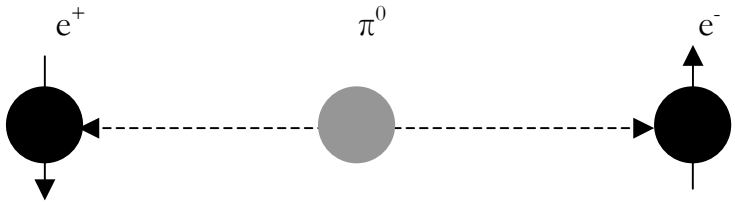


*Abbildung 1* Zerfall eines Pions mit Spin Null in ein Elektron-Positron-Paar

Im Formalismus der Wellenfunktion beschreibt man das nun durch eine Gesamtwellenfunktion für das Elektron-Positron-Paar

$$\left|\Psi\right\rangle_{gesamt} = \frac{1}{\sqrt{2}}\left(\left|\uparrow\right\rangle_L\left|\downarrow\right\rangle_R + \left|\downarrow\right\rangle_L\left|\uparrow\right\rangle_R\right) \qquad (3)$$

Dies ist ein so genannter verschränkter Zustand. So paradox es auch klingen mag: Obwohl wir nur eine Wahrscheinlichkeitsaussage über den Zustand von Elektron und Positron machen können, wissen wir bei Messung eines der beiden Teilchen sofort, in welchem Zustand sich das andere Teilchen befindet. Die Verschränkung von Quantensystemen wurde in vielen Experimenten überprüft und ist neben der Superposition von Zuständen eine wichtige Eigenschaft zum Bau eines Quantencomputers.

## 4 Der Quantencomputer

Wie kann man nun die Gesetze der Quantenmechanik benutzen, um einen Quantencomputer zu bauen? Betrachten wir dazu erst einmal einen „herkömmlichen" Computer. Die zu verarbeitende Information wird in Bits umgewandelt, d. h. in Folgen von Nullen und Einsen. Eine Null wird durch „kein Stromsignal am Transistor" und eine Eins durch „Stromsignal am Transistor" implementiert. Mittels Transisto-

ren werden logische Gatter erzeigt, mit denen sämtliche mathematische Operationen durchgeführt werden können.

Das Analogon zum Bit für einen Quantencomputer ist das *Qubit*. Dazu benötigt man ein quantenmechanisches System, das nur zwei mögliche Zustände einnehmen kann, wie z. B. der Spin des Elektrons oder Positrons. Die beiden Zustände werden nun mit $|0\rangle$ und $|1\rangle$ bezeichnet, um die Analogie zum klassischen Computer herzustellen. Ein System aus N Zwei-Niveausystemen stellt nun ein System aus N Qubits dar, die sich alle in einem Überlagerungszustand $a|0\rangle+b|1\rangle$ befinden, wobei $|a|^2$ und $|b|^2$ die Wahrscheinlichkeiten sind, dass man bei einer Messung des Systems die Zustände $|0\rangle$ bzw. $|1\rangle$ erhält. Neben der Superposition ist das System auch noch verschränkt. Diese beiden Eigenschaften ermöglichen nun den so genannten Quantenparallelismus, d. h. durch Verwendung quantenmechanischer Systeme können Prozesse nebeneinander ablaufen, die auf einem gewöhnlichen Computer nacheinander durchgeführt werden müssen, was bei komplexen Problemen einen enormen Zeitgewinn bedeutet.

## 5 Experimentelle Realisierung

Auch wenn bereits eine Zahl von Algorithmen für einen Quantencomputer entwickelt wurden, so ist es bisher noch nicht möglich, einen solchen Rechner zu bauen. In derzeitigen Experimenten versucht man z. B. Atome oder Ionen mittels elektromagnetischer Felder einzufangen und als Qubits zu verwenden. Dazu benutzt man ganz bestimmte Energieniveaus der Elektronen in den Atomen oder Ionen und erzeugt logische Operationen durch das Einstrahlen von Laserlicht. In diesen Experimenten hat man aber mit vielen Schwierigkeiten zu kämpfen. Zum einen ist es nicht einfach, eine genügend große Anzahl von Teilchen einzufangen und mit dem Laser anzusteuern. Zum anderen bestehen Probleme bei der Initialisierung der Qubits in einem gewünschten Eingangszustand und beim Auslesen des Rechenergebnisses.

# 6 Zusammenfassung

Die Gesetze der Quantenmechanik ermöglichen eine neue Generation von Computern, die die besten erdenklichen klassischen Computer um ein Vielfaches an Leistungsfähigkeit übertreffen. Wann und ob es möglich sein wird einen Quantencomputer im Experiment zu realisieren ist jedoch derzeit nicht absehbar. Trotz aller Schwierigkeiten sind durch die heutigen Experimente wunderbare Möglichkeiten zur Untersuchung quantenmechanischer Systeme Wirklichkeit geworden, die neue Einsichten in die Welt auf kleinsten Längenskalen geben.