quantencomputer.de

Eine Einführung zum Thema Quantencomputer

Matthias Bezold. 6. Februar 2007

1.Vorwort

Diese Seite basiert im Großen und Ganzen auf meiner Facharbeit, die über das Thema "Quantencomputer" ging. Diese Einführung soll allerdings nicht wissenschaftlich sein, sondern so, daß sie jeder verstehen kann. Deshalb verwende ich auch keine Formeln. Teilweise ist der Stoff aber natürlich schon etwas theoretisch.

Wenn du einen Fehler findest - entweder inhaltlich oder einen Rechtschreibfehler -, oder wenn du etwas nicht verstehst, oder sonstige Kritik hast oder mir einfach so eine Mail schreiben willst: Meine Adresse ist **quanten@mbezold.de**.

2.Einführung in die Quantenphysik

Verschränkung

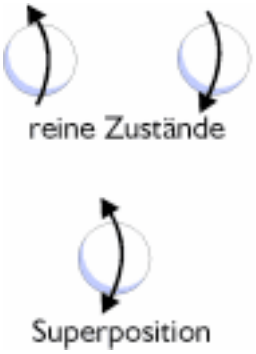
Verschränkung bedeutet, daß zwei Partikel, z.B. Photonen, miteinander verbunden sind. Wenn eines verändert wird, betrifft diese Änderung auch das andere.

Schickt man z.B. ein Photon durch einen Kristall, so können zwei Photonen von jeweils halber Energie entstehen. Diese bewegen sich nun in entgegengesetzte Richtungen, und die Polarisation von beiden ist unbekannt. Wenn aber nun eines der beiden gemessen wird, wird dadurch die Polarisation des anderen festgelegt: es erhält nämlich genau die entgegengesetzte zu der, die das erste hat.

Diese Erscheinung wurde von den Physikern Einstein, Podolsky und Rosen entdeckt und nach ihnen "EPR-Paradoxon" genannt.

Die Entfernung der Teilchen spielt dabei keine Rolle, und die Veränderung geschieht "instantan", also ohne zeitlichen Unterschied. Die Zustandänderung kann also nicht durch z.B. Photonen übermittelt werden.

Superposition und Dekohärenz



Ein klassisches Teilchen kann sich nur in einem bestimmten Zustand befinden. Ein Photon kann z.B. verschiedene Polarisationen haben, aber immer nur eine in einem bestimmten Augenblick. In der Quantenphysik kann aber ein Teilchen in einem Zwischenzustand zwischen mehreren Zuständen sein, der sog. Superposition.

Der berühmte Physiker Schrödinger hat sich dazu ein hervorragendes und gleichzeitig makaberes Gedankenexperiment ausgedacht: "Schrödingers Katze". Ein Atom, ein Detektor, ein Hammer, ein Gefäß mit einer giftigen Substanz und eine Katze befinden sich in einer Kiste. Sobald das Atom zerfällt, bemerkt der Detektor dies und bewegt den Hammer. Dieser zerstört das Gefäß, wodurch das Gift freigesetzt wird, welches die Katze tötet. Solange die Kiste aber geschlossen ist und der Betrachter daher nicht sehen kann, ob die Katze noch lebt, befindet sie sich also in einem "Zwischenzustand" zwischen lebendig und tot, also in einer Superposition der beiden Zustände.

Wenn die Kiste aber geöffnet wird, sieht man, ob die Katze noch lebt. Es wird also aus der Superposition ein "reiner Zustand", also ein klassischer. Dies nennt man "Dekohärenz".

Jede "Messung" an einer Superposition führt dazu, daß das Teilchen wieder einen eindeutigen Zustand annimmt, und zwar zufällig einen der Zustände, die in der Superposition enthalten sind. Eine Messung ist jede Interaktion mit der Umwelt, z.B. bereits das Auftreffen von Photonen.

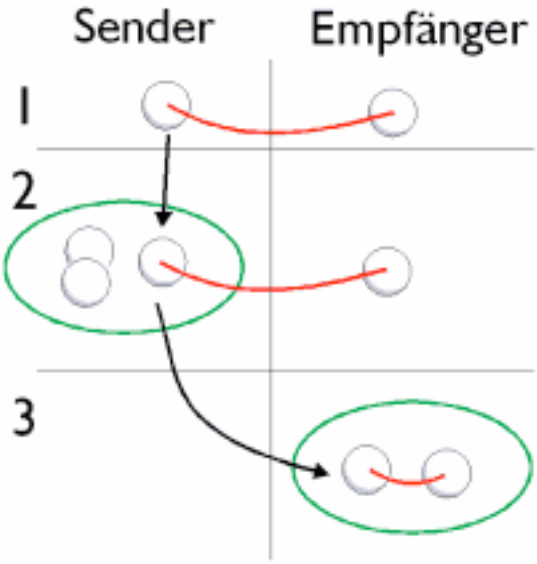
Die Dekohärenz macht auch ein "Klonen", also die Verdoppelung eines beliebigen Quantenzustandes unmöglich, da eine Messung eine Superposition zerstören würde.

3.Anwendungen der Quantenmechanik

Diese Besonderheiten der Quantenphysik können für einige interessante Anwendungen genutzt werden, z.B. die Übertragung von zwei Bits in einem, die Teleportation oder die Quantenkryptographie. Diese drei sollen hier kurz "umrissen" werden.

Übertragung von zwei Bits in einem

Klassisch kann man mit 1 Bit (z.B. 1 Photon) nur zwei Nachrichten übermitteln, nämlich 0 und 1. Mit der Quantenphysik lassen sich aber zwei Bits Information mit nur einem physikalischen Bit übertragen



1. Sender und Empfänger verfügen jeweils über ein Teilchen eines verschränkten Paares.

2. Der Sender führt eine Messung zwischen den zwei zu übertragenden Bits und seinem verschränkten Teilchen durch und übermittelt sein Teilchen an den Empfänger.

3. Durch eine Messung der beiden verschränkten Teilchen kann der Empfänger die zwei Bits auslesen, durch die vier mögliche Nachrichten übermittelt werden können. Dies ist möglich, da die Verschränkung als Informationsquelle genutzt werden kann.

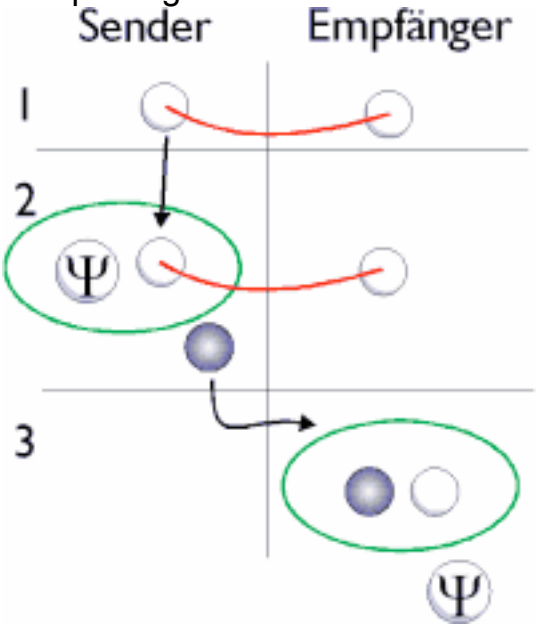
Teleportation

Klassisch ist es nicht möglich, einen unbekannten Quantenzustand komplett zu übertragen. Bei der Messung würde z.B. eine Superposition zerstört. Die Quantenphysik bietet aber auch hierfür eine Lösung. Die Übertragung eines Quantenzustandes nennt man "Teleportation".

1. Sender und Empfänger besitzen wieder ein verschränktes Teilchenpaar.

2. Der Sender führt eine Messung zwischen seinem verschränkten Teilchen und dem unbekannten Quantenzustand Psi durch. Die Information, also das Ergebnis der Messung (blaue Kugel), übermittelt er an den Empfänger.

3. Aus der übertragenen Information kann der Empfänger nun den Anfangszustand Psi wiederherstellen. Wieder ist dies möglich, da die Verschränkung als Informationsquelle genutzt wird.



Quantenkryptographie

Ziel der Kryptographie ist es, daß zwei Personen eine geheime Nachricht austauschen können. Dazu verwenden sie eine Zeichenkette, den sog. "Schlüssel", um die Nachricht zu ver- bzw. entschlüsseln. Ein Dritter darf nicht in Besitz dieses Schlüssels gelangen, da er sonst auch die geheime Nachricht lesen könnte. Das Problem ist, daß auch dieser Schlüssel geheim ausgetauscht werden muß, ohne daß ein Lauscher diesen herausbekommen kann.

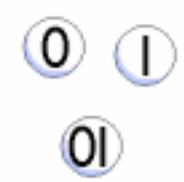
Die Quantenphysik bietet hierfür eine elegante Lösung: die "Quantenschlüsseldistribution" (-verteilung). Dabei werden Photonen als Kommunikationsmedium verwendet. Wenn ein Lauscher die Photonen mißt und wieder aussendet, verändert er sie dabei. Diese Veränderung können der Sender und der Empfänger der Nachricht bemerken, indem sie öffentlich einen Teil des Schlüssels vergleichen. Wenn dieser Teil abweicht, erzeugen sie einen neuen Schlüssel.

Die Quantenschlüsseldistribution wurde schon praktisch realisiert. Über 23 km Glasfaserkabel unter dem Genfer See wurde ein Schlüssel ausgetauscht.

4.Ein Computer

Und daraus soll jetzt ein Computer entstehen? Ja! Die "Grundbausteine" werden in diesem Kapitel erklärt.

Qubits



Jeder Computer muß seine Daten in einer kleinsten Einheit speichern können, dem sog. Bit. Dieses kann entweder den Zustand 0 oder 1 annehmen. Ein Quantenbit ("Qubit") kann sich aber, wenn es sich in einer Superposition befindet, in den beiden Zuständen *gleichzeitig* befinden.

Man könnte sich z.B. als Qubit einen Atomkern vorstellen, dessen Spins +1/2 und -1/2 die Zustände 1 und 0 darstellen. Eine Superposition wäre dann quasi +-1/2. Durch eine Messung nimmt das Qubit dann einen klassischen Wert an, also +1/2 oder -1/2.
Die Wahrscheinlichkeit, mit der eine Superposition durch eine Messung zu einem bestimmten Zustand wird, läßt sich beeinflussen. In der Regel wählt man 50% für jeden Zustand.

Register

Mit einem Bit kann man maximal zwei Zahlen darstellen, z.B. 0 und 1. In der Praxis reicht dies natürlich nicht aus, sondern man will mit größeren Zahlen rechnen können. Dazu reiht man einfach n Bits aneinander. So können maximal 2^n Zahlen dargestellt werden, mit 50 Bits also ungefähr 2^50 = 10^15 Zahlen.

Ein Register, das aus Qubits besteht ("Quantenregister") kann sich dabei nicht nur, wie ein klassisches, in einem Zustand, sondern in allen möglichen Zuständen gleichzeitig befinden, nämlich wenn sich alle Qubits in einer Superposition befinden. Wie beim Qubit zerfällt eine Superposition eines Registers durch eine Messung, wobei die Wahrscheinlichkeit für jeden Zustand gleich ist, wenn die Wahrscheinlich für jeden Zustand eines Qubits 50% beträgt.

Ein Quantenregister, das aus zwei Qubits besteht, kann z.B. folgende Zustände haben:

binär: |0>|0>, |0>|1>, |1>|0>, |1>|1> bzw. dezimal: |0>, |1>, |2>, |3>

Wenn sich das Quantenregister nun in einer Superposition dieser Zustände befindet, enthält es diese vier Zustände gleichzeitig, wobei eine Messung einen klassischen Zustand zurückliefert (0, 1, 2 oder 3). Die Wahrscheinlichkeit für jeden Zustand beträgt dabei 1/4.

Gatter

Ein Gatter ist eine Elementaroperation. Wenn eine solche Operation auf ein Qubit oder ein Register angewendet wird, das sich in einer Superposition befindet, so betrifft die Änderung alle in ihr enthaltenen Zustände.

Es gibt 1-Bit-Gatter sowie 2-Bit-Gatter. Das einfachste 1-Bit-Gatter ist das NICHT-Gatter, bei dem einfach der Inhalt eines Bits invertiert wird: 0 wird zu 1, 1 wird zu 0.

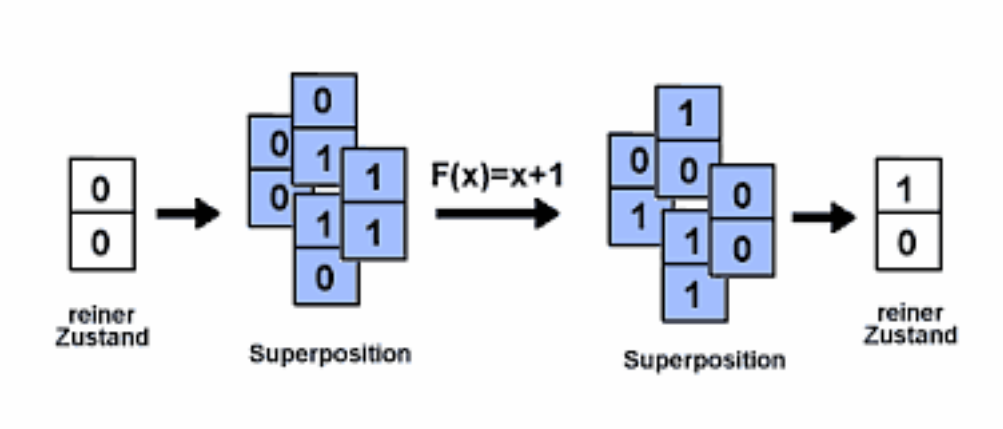
Das wichtigste 2-Bit-Gatter ist das sog. "kontrollierte NICHT", bei dem ein Bit in Abhängigkeit davon, ob ein zweites Bit gesetzt, also gleich 1, ist, negiert wird. Dieses zweite Bit heißt "Kontrollbit". Die zweite Zahl stellt jeweils das Kontrollbit dar, die erste das Bit, auf das die Operation angewendet wird:

0 / 0 -> 0 / 0
1 / 0 -> 1 / 0
0 / 1 -> 1 / 1
1 / 1 -> 0 / 1

Erstaunlicherweise benötigt man für einen kompletten Quantencomputer nur 1-Bit-Gatter sowie das "kontrollierte NICHT"-2-Bit-Gatter. Alle anderen Operationen lassen sich durch eine Aneinanderreihung dieser Gatter realisieren.

Funktionen

Auch mathematische Funktionen lassen sich realisieren, indem man die Elementargatter mehrmals hintereinander in einer bestimmten Reihenfolge auf das Register anwendet. Eine Superposition bleibt dabei erhalten, und das Register enthält nach der Anwendung der Funktion nicht mehr die ursprünglichen Werte, sondern die dazugehörigen Ergebnisse:



1. Das Register befindet sich im klassischen Grundzustand 00.

2. Es wird in eine Superposition aller möglichen Zustände versetzt, wobei jeder Zustand gleich wahrscheinlich ist.

3. Die Funktion F(X)=x+1 wurde auf das Register angewendet. Es enthält jetzt nicht mehr die ursprünglichen Werte, sondern die dazugehörigen Ergebnisse.

4. Durch eine Messung nimmt das Register wieder einen klassischen Zustand an. Man verwendet aber nicht nur ein einziges Register, sondern eines für die zu berechnenden Werte und eines für die Ergebnisse. |x> ist das Register mit den Werten, |y> das mit den Ergebnissen. Durch die Berechnung wurden die beiden Register aber verschränkt: wenn man eines der beiden Register nun mißt, verändert sich auch das zweite. Nach der Messung enthält das zweite Register nur noch die Werte, die dem Ergebnis der Messung des anderen entsprechen:

|x>|0> **=>** |x>|y=f(x)>
das erste Register enthält die zu berechnenden Werte, in das zweite werden die Ergebnisse geschrieben
|x>|y> **=>** |j>|f(j)>
das erste Register wird gemessen; dadurch befinden sich im zweiten Register nur noch die Werte, die von f(x) für j zurückgeliefert werden

5.Quantenalgorithmen

Man könnte mit einem Quantencomputer normale, klassische Algorithmen verwenden. Allerdings würde dies gegenüber einem normalen Computer keinen Vorteil bringen, da die besonderen Eigenschaften des Quantencomputers, v.a. Superposition und Verschränkung, nicht genutzt werden.

Spezielle Quantencomputeralgorithmen können aber wesentlich schneller sein als klassische. So lassen sich Probleme lösen, für deren Lösung die klassische Methode in der Praxis viel zu lange dauert (z.B. Dauer des Universums!). Die Berechnungszeit bei einem Quantenalgorithmus nimmt weniger zu als bei herkömmlichen Algorithmen.

Zwei Quantenalgorithmen sollen hier vorgestellt werden: ein Faktorisierungsalgorithmus und ein Suchalgorithmus.

Der Faktorisierungsalgorithmus von Shor

Den ersten praktisch verwendbaren Algorithmus entdeckte 1994 Peter Shor von den AT&T Bell Labs. Es handelt sich dabei um einen Algorithmus, mit dem man eine Zahl in ihre Primfaktoren zerlegen kann.

Im Prinzip funktioniert dieser Algorithmus so, daß zuerst alle möglichen Werte aus einem Register in einer Superposition aller möglichen Werte errechnet werden. Das richtige Ergebnis kann nun allerdings nicht durch eine Messung ermittelt werden, da diese lediglich einen zufälligen Wert zurückliefern würde. Mit der sog. "Diskreten Fourier-Transformation" ist es aber möglich, das richtige Ergebnis zu ermitteln.

Die Berechnungszeit dieses Algorithmus nimmt deutlich langsamer zu als die des besten klassischen. Die einfachste klassische Methode zur Faktorisierung ist, alle Werte von 1 bis Wurzel N auszuprobieren. Ein Computer, der pro Sekunde 10^10 Teilungen durchführen kann, bräuchte dann für eine 100-stellige Zahl länger als die geschätzte Dauer des Universums! In der Praxis wäre die Methode also nicht verwendbar. Der Quantencomputer könnte allerdings solche Zahlen in einer verhältnismäßig kurzen Zeit faktorisieren.

Eine Umsetzung dieses Algorithmus wäre eine Gefahr für die bestehende Kryptographie. Die Sicherheit des RSA-Algorithmus z.B. basiert darauf, daß es klassisch unmöglich ist, große Zahlen zu faktorisieren. Der Quantencomputer könnte dies aber.

Der Suchalgorithmus von Grover

Will man z.B. in einem Telephonbuch mit 1.000.000 Einträgen eine bestimmte Telephonnummer finden, muß man so lange einen Eintrag nach dem anderen durchsehen, bis man den richtigen findet. Allgemein braucht man, um einen bestimmten Eintrag in einer unsortierten Liste zu finden, N/2 Versuche, beim Telephonbuch z.B. 500.000.

Mit dem Quantenalgorithmus benötigt man dagegen im Schnitt nur Wurzel N Schritte. Dies ist möglich, indem durch die sog. "Grover-Iteration" im Quantenregister die Wahrscheinlichkeit für das richtige Ergebnis erhöht wird, die für die falschen aber verringert. So kann man durch einfaches Auslesen das richtige Ergebnis erhalten.

Für diesen Suchalgorithmus gibt es eine große Anzahl von Anwendungsmöglichkeiten: indem man einfach alle Ergebnisse ausprobiert, kann man auch Probleme lösen, für die es entweder überhaupt keinen Algorithmus gibt oder nur einen, dessen Berechnungszeit zu lange ist. Ein Beispiel wäre prinzipiell ein Schachcomputer.

6.Praktische Umsetzung

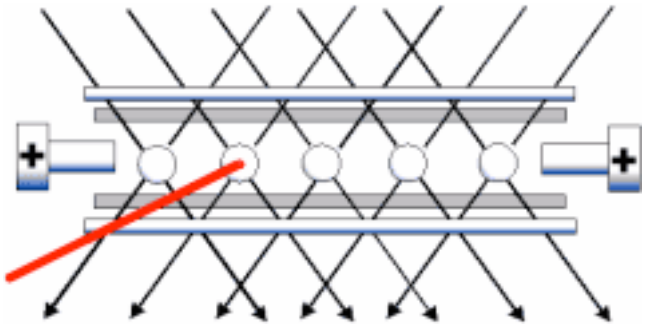
Für die Realisation eines Quantencomputers gibt es viele Ansätze. Zwei sollen hier vorgestellt werden: die Ionenfalle und die Kernspinresonanz.

Die Ionenfalle

Bei dieser Methode werden Ionen in einer sog. Paulfalle eingefangen. Die "Falle" befindet sich im Hochvakuum, und die Ionen müssen auf beinahe 0 Kelvin abgekühlt werden. Diese Abkühlung ist z.B. mit einem Laser möglich.

Jedes Ion in der Falle entspricht einem Qubit. Befinden sich in der Falle z.B. 7 Ionen, verfügt der Quantencomputer über 7 Qubits. Die Elementaroperationen können mit einem Laser implementiert werden.

Das Hauptproblem bei der Ionenfalle stellt das Herabkühlen auf die Anfangstemperatur von fast 0 Kelvin dar. Mit dieser Methode kann kein Quantencomputer mit einer großen Anzahl von Qubits gebaut werden, sondern wahrscheinlich mit höchstens 10-20. Man kann aber schon daran sehen, ob der Quantencomputer im Prinzip funktioniert.



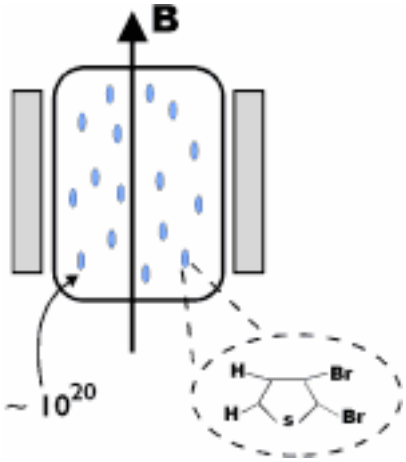
Kernspinresonanz

Diese Methode beruht auf der Kernspinresonanz (engl. nuclear magnetic resonance = NMR), die in der Chemie schon lange bekannt ist und in der Medizin z.B. für die Tomographie verwendet wird.

Einen "Quantencomputer" bildet ein einzelnes Molekül, wobei jedes Atom ein Qubit darstellt. Ein Molekül mit 10 Atomen verfügt also über 10 Qubits. Die Zustände 0 und 1 eines Qubits bilden jeweils die Spin-Zustände -1/2 und +1/2 der Kerne.

Eine Messung bzw. Änderung eines einzelnen Moleküls ist allerdings nicht möglich. Deshalb verwendet man statt einem ca. 10^20 Moleküle! Es ergibt sich nun allerdings das Problem, daß sich alle gleich entwickeln müssen und den gleichen Anfangszustand haben müssen. Aber auch dieses Problem ist durch verschiedene Methoden in den Griff zu bekommen.

Im Moment ist die Kernspinresonanz die führende Technik für einen Quantencomputer: es gelang, den Suchalgorithmus von Grover mit zwei Qubits zu implementieren, also aus vier Zuständen den richtigen zu finden.



Und sonst?

Es gibt noch viele weitere Ansätze, z.B. die "High-Q-optical-cavity", aber bis jetzt taugen alle nicht für einen Quantencomputer mit einer großen Anzahl von Qubits. Aber erst mit ein paar hundert Qubits kann einen Quantenrechner merklich schneller sein als ein klassischer.

Es hat sich aber gezeigt, daß ein Quantencomputer zumindest im Prinzip realisierbar ist.

Das Hauptproblem bei der Realisation ist die spontane, ungewollte Dekohärenz. Man hofft, diese durch verschiedene Fehlerkorrekturmethoden eindämmen zu können.

7.Ausblick

Wohin die Reise geht, kann niemand sagen - die Meinungen sind geteilt. Es ist nicht klar, ob es jemals einen Quantencomputer mit einer großen Anzahl von Qubits geben wird.

Durch die praktische Auseinandersetzung mit der Welt der Quanten erhält man aber tiefe Einblicke in die Natur, so daß die Forschung auf diesem Gebiet auf keinen Fall sinnlos ist.

Klar ist aber, daß die ersten Quantencomputer natürlich nicht den PC ersetzen werden, sondern für spezielle Anwendungen in der Wissenschaft und Forschung eingesetzt werden. Die Zukunft ist aber schwer vorherzusagen: Wer hätte schon vor 50 Jahren an die Omnipräsenz des Computers gedacht, wie wir sie heute kennen?