



Quantencomputer

- Die Zukunft der Computer im Zeichen der Physik...

Auf der Jagd nach dem Quantencomputer

Atomkerne statt Siliziumchips – Der Quantencomputer stellt die Verbindung der Mikrophysik und der Computerwissenschaft dar. Durch diese direkte Verknüpfung versprechen sich die Wissenschaftler eine um ein vielfaches erhöhte Rechenleistung, eine Minimalisierung des Energieverbrauches und die Möglichkeit Kryptographie in Echtzeit laufen lassen zu können.

Bei einem herkömmlichen Computer sind die Informationsträger so genannte Bits, die entweder den Wert 0 oder 1 annehmen können. Die Weiterentwicklung zum Quantencomputer eröffnet nun die Möglichkeit, jeden Wert zwischen 0 und 1 darzustellen, desweiteren könnten diese Qbits auch mehrer Zustände parallel annehmen.

Der Arbeitsgruppe am Würzburger Lehrstuhl für Technische Physik unter der Leitung von Prof. Dr. Alfred Forchel gelang es zusammen mit der Forschungsgruppe von Prof. Dr. Pawel Hawrylak vom National Research Council in Ottawa, durch die Kopplung so genannter Quantenpunkte künstliche Moleküle herzustellen. Quantenpunkte können als im Labor synthetisierte Atome betrachtet werden, deren Eigenschaften der Experimentator genau einstellen kann.

Wird nun ein Elektron in ein solches Molekül injiziert, so kann es als "quantum bit" benutzt werden: Es kann sich entweder in dem einen (logische 0) oder in dem anderen Quantenpunkt (logische 1) befinden. Mehr noch, es kann sich sogar in beiden Punkten aufhalten. Werden in das künstliche Molekül zwei Elektronen injiziert, so werden die Zustände dieser beiden Teilchen gekoppelt. Somit ist ein so genanntes "quantum gate" und damit ein Bauelement realisiert, das zur Verschränkung zweier Bits dient.

Von Heißenberg, Schrödinger und Bell

Vier Formulierungen der Quantenmechanik sind für Quantencomputer von besonderem Interesse: 1. Die Schrödingergleichung, 2. Heisenbergs Unschärferelation, 3. Bells Nichtlokalität sowie 4. Everetts Viele Welten. Während die Schrödingergleichungen und Heisenbergs Unschärferelation von einer reversiblen Zeit ausgehen, berücksichtigt die Nichtlokalität und Everetts Ansatz auch die Irreversibilität der Zeit, da für das jeweilige Jetzt ständig neue Welten entstehen und vergehen. Everetts Ansatz ist insbesondere für die Erzeugung von Informationen und neuen Bedeutungen am wichtigsten.

Bohrs Prinzip der Komplementarität und Heisenbergs Unschärferelation wurden als die Kopenhagener Interpretation der Quantenmechanik bekannt. Die Quantenmechanik beschreibt, wie sich statistische Gesamtheiten von Teilchen (keine Einzelereignisse) verhalten, aber warum es Teilchen gibt, sagt sie nicht. Im Rahmen der Quantenmechanik sind die Position q und das Momentum p von Teilchen nicht länger einfache Zahlen, sondern Matrizen. Diese Matrizen gehorchen nicht immer dem kommutativen Gesetz $p \times q = q \times p$. Es gibt deshalb zwei Erklärungen für atomare Phänomene, nämlich Schrödingers Wellen- und Heisenbergs Matrizenvorstellung.

Die Schrödinger-Gleichung ist zeitlich reversibel und wird im sogenannten Hilbertraum abgebildet, der eine rekursive Struktur von Unterräumen darstellt. Gemäß der Quantentheorie kann eine Katze, die sich in einem abgeschlossenen System befindet, gleichzeitig sowohl tot als lebendig sein. Da wir nicht wissen, in welchem Zustand sich die Katze befindet, kann man gemäß der Quantentheorie aussagen, daß sich diese in einem Überlagerungszustand befindet, bei dem sie beides ist: tot und lebendig. Diese Aussage gilt solange, bis man das System öffnet und einen der beiden Zustände antrifft. Das Beispiel von Schrödingers Katze ist auch elementar für das Verständnis von Quantencomputern. Betrachtet man das Quantenbit (Qubit) in Analogie zur Katze, so gibt es bei Berechnungen nicht nur die Zustände 0 und 1, sondern Überlagerungen dieser Zustände.

Nach der quantenmechanischen Sicht ist alles im Universum miteinander verbunden, d.h. die Wirklichkeit ist nicht kausal, sondern akausal verwoben. In seinem Buch "Speakable and Unspeakable in Quantum Mechanics" beschreibt Bell das Phänomen der Socken des Mathematikers Bertlmann, die unterschiedliche Farben (rosa und grün) haben: Wie weiß der eine Socken vom anderen, was er getan hat? Wenn man nur einen seiner Füße sieht und eine grüne Socke erblickt, weiß man sofort, daß am anderen Fuß sich eine rosa Socke befindet und dies, ohne daß eine Signalübertragung stattfinden muß.





Quantencomputer – Ein Überblick -2- von -3-

1957 schlug Hugh Everett eine völlig neue Interpretation der Quantenmechanik vor, nach der immer dann, wenn eine Vielzahl von Möglichkeiten besteht, sich die Welt in eine Vielzahl von Universen aufspaltet. Nach Everett entsteht bei jeder Interaktion eines Teilchens mit einem anderen eine neue Welt. Jedoch verschwinden in gleichem Maße Welten wie Neue entstehen. In jeder dieser Welten ist alles identisch, mit Ausnahme der getroffenen Auswahl. Danach entwickeln sich die Welten unabhängig voneinander weiter. Da jede Quantenwelt anders ist, gibt es nicht die einzige Wirklichkeit, sondern eine Vielzahl paralleler Wirklichkeiten.

Die Gödelmaschine – mehr als der Mensch ??

Das Lösen von Problemen ist immer relativ zum Problemlösungspotential des Systems zu sehen, welches das Problem bearbeitet. Es gibt unlösbare Probleme, noch nicht bewiesene unlösbare Probleme und lösbare Probleme. Die Lösbarkeit der lösbaren Problemen hängt von den Algorithmen, der Größe des involvierten Systems und der Rechenleistung der verfügbaren Rechner ab. Zukünftige Computer könnten die Lösung von Problemen gestatten, die für Menschen bisher als unlösbar galten. Derartige Maschinen nennt man Gödel-Maschinen, da sie dem Menschen erlauben könnten, hinter seine eigene Gödelgrenzlinie zu sehen. Dieser Computer kann eine unendliche Anzahl von Rechenschritten in einem unendlich kleinen Zeitintervall berechnen.

Ein derartiger Quantenrechner müßte zwangsläufig nichtlokale Eigenschaften haben, wenn Berechnungen in Echtzeit durchgeführt werden sollen. Nur ein Hyper-System im Quantenzustand kann alles potentielle Wissen umfassen, d.h. authentisch die Realität abbilden. Die Idee eines solchen Quantenrechners, der auf Nichtlokalität basiert, bleibt jedoch solange theoretischer Natur, bis es Möglichkeiten gibt, die Nichtlokalität, z.B. durch besondere Raumkrümmungen oder Überlichtgeschwindigkeiten, im Makrokosmos nachzuweisen und diese für Berechnungen zu nutzen. Das Jetzt ist für einen universellen Quantencomputer, wie Gödels Axiome verdeutlichen, ein unüberwindbare Grenze, da durch infinitesimale Differenzen, die immer weiter divergieren, ständig ein neues Jetzt, d.h. neue Universen entstehen. Während Turing-Maschinen Software programmieren, könnten Gödel-Maschinen auch Hardware neu verschalten.

Moravec hat abgeschätzt, daß die Prozesse des Gehirns durch einen Computer mit einer Rechenleistung von 10^{13} , d.h. 10 Billionen Berechnungen pro Sekunde, durchgeführt werden könnten, was nur mehr einem Faktor 1000 gegenüber heutigen Super-Computern entspricht. Unterstellt man, daß das Mooresche Gesetz gilt, wobei 10 Jahre einer Verbesserung um den Faktor 1.000 entsprechen, so könnte die Differenz zwischen Computern und dem Gehirn bezüglich der Rechenleistung in absehbarer Zeit überbrückt werden. Es ist kaum anzunehmen, daß unser Gehirn nach den Regeln eines Turing-Computers funktioniert. Vielmehr handelt es sich bei unserem Gehirn um ein hochkomplexes Interface, das uns den Weg zu einem neuartigen Rechner, der Gödel-Maschine, weisen kann, die möglicherweise ihr eigenes Bewußtsein hervorbringt.

Man stelle sich ein Gedankenexperiment vor, bei dem das menschliche Gehirn parallel und gleichzeitig in mehrere Quantencomputer transferiert wird. Für eine kurze Korrelationszeit könnte dann derselbe Geist in mehreren Universen gleichzeitig existieren. Interessant an dieser Vorstellung ist, was passiert, wenn die Quantencomputer dann miteinander gekoppelt würden und wenn unterschiedliche Welten mit denselben Zuständen aufeinandertreffen. Wenn man unterschiedliche Menschen auf einer Party trifft, entstehen neue Kontakte. Eine gewisse Anzahl davon sind fruchtbar, während andere nach dem Ende der Party wieder aufgehoben sind. Nichts anderes geschieht auch mit Quantenpartikeln, die aufeinandertreffen. Befremdlich wären jedoch auch hier Kontakte, bei der wir auf eine identische Kopie von uns treffen würden, vor allem wenn diese Kopie dieselben Zustände im Gehirn hätte.





Hindernisse

Während ein klassisches Bit den Zustand 0 oder 1 repräsentieren kann, kann ein Quantenbit eine Überlagerung zweier Zustände sein. Gelingt es gezielt, solche Interferenzen zu konstruieren, so lassen sich die in Quantensystemen auftretenden Fehler vermindern. Dies ist deshalb die Grundvoraussetzung, um Quantencomputer überhaupt bauen zu können. Mittlerweile wurden Codes für Quantensysteme entwickelt, die einen Schutz gegenüber Fehlern erlauben.

Für die Realisierung von Quantencomputern muß ein Modell entwickelt werden, das dem Modell der universellen Turing-Maschine bei klassischen Berechnungen entspricht. Es wird deshalb vorgeschlagen, dieses Modell die universelle Gödel-Maschine zu nennen. Ob Quantencomputer die Church-Turing-These erfüllen, bleibt ebenso zu klären wie die Frage des Halte-Problems. Da bei überlagerten Zuständen die einzige Möglichkeit, das Programm zu stoppen, darin besteht eine Messung vorzunehmen, muß es gelingen, die Kohärenz der Berechnung aufrechtzuerhalten. Darüberhinaus muß geklärt werden, für welche Problemklassen sich besonders der Einsatz von Quantencomputer eignet und welche Problemstellungen womöglich nur mit klassischen Computern zu lösen sind. Dies hätte jedoch zur Folge, daß es keinen universellen Quantencomputer geben kann und somit die Anwendung des Church-Turing-Prinzips auf physikalische Systeme keinen Sinn machen würde. Eine physikalische Interpretation der Church-Turing-These würde bedeuten, daß sich jedes physikalische System durch eine universelle Maschine in endlichen Schritten simulieren ließe. Sollte es jedoch möglich sein, daß ein Quantencomputer jede Art von Problem lösen kann, stehen wir vor einem völlig neuartigen Universum von Möglichkeiten, sowohl für das Leben im Jetzt, als auch für die Evolution von Mensch-Maschine-Systemen.

IBM erreicht Durchbruch bei Quantencomputer – das 1.Kapitel

Armonk/London, 21.12.2001 (dpa) – Der US-Computerkonzern IBM hat in der Grundlagenforschung mit Computern aus einzelnen Atomen einen Durchbruch erreicht. Zum ersten Mal konnten Wissenschaftler am IBM-Forschungszentrum in Almaden eine einfache Entschlüsselungsaufgabe mit Hilfe eines so genannten Quantencomputers berechnen, berichtete am Freitag das britische Wissenschaftsjournal "Nature".

Dabei ging es um die Frage, welche Zahlen multipliziert 15 ergeben (3 und 5). Das wichtige Forschungsergebnis bedeute aber noch keinen Durchbruch für die kommerzielle Nutzung von Quantencomputern. Für das aktuelle Experiment hat der Konzern einen Quantencomputer aus sieben einzelnen Atomen zusammengestellt. In anderen Versuchen konnten die IBM-Forscher bereits 1.000 Atome kontrollieren.

Computer arbeiten heute mit Mikroprozessoren auf der Basis von Silizium-Halbleitern. Für die Entschlüsselung großer Zahlen müssen heutige Supercomputer Jahre lang rechnen. 1994 hatte der Wissenschaftler Peter Shor von AT&T die These aufgestellt, dass Quantencomputer diese Aufgaben viel schneller lösen könnten. Mit dem aktuellen Experiment in den IBM-Labors wurde der Shor-Algorithmus für die kleine Zahl 15 gelöst.

IBM hat im vergangenen Jahr 5,2 Milliarden Dollar (5,8 Milliarden Euro) für Entwicklung und Forschung ausgegeben.

