Basler Zeitung online

Erschienen am: 29.03.2001

Universität Basel versucht einen Quantensprung im Rechnen

Gelingt es, die Phänomene der Quantenwelt zum Rechnen zu benutzen, werden herkömmliche Computer wie Zählrahmen erscheinen. Ein Ziel des Forschungsschwerpunktes «Nanowissenschaften» ist es, den Grundbaustein für einen Quantencomputer zu bauen. Der theoretische Physiker Daniel Loss glaubt zu wissen, wie man das macht.

Der Grundbaustein eines Quantencomputers. Je ein Elektron wird in einem künstlichen Atom (Pfeile) eingefangen. Foto B. Westervelt, Harvard

Basel. «Selbst wir kommen manchmal durcheinander. Zwar kennen wir die Regeln der Quantenwelt, ertappen uns aber immer wieder dabei, dass wir klassisch denken.» Der dies sagt, ist Daniel Loss, seit 1996 Ordinarius für theoretische Physik an der Universität Basel. Mit «klassisch denken» meint er das, was Menschen tun, wenn sie denken. Mit «wir» sind Physiker und Physikerinnen gemeint, die im Geiste täglich in die Welt einzelner Atome und Elementarteilchen eintauchen, in die Quantenwelt eben. Und dort herrschen Regeln, die jedem gesunden Menschenverstand spotten, die aber dennoch gültig sind. Denn die Quantenmechanik zählt zu den best überprüften wissenschaftlichen Theorien überhaupt.
Das Spezialgebiet von Daniel Loss und seiner Gruppe ist der Quantencomputer. Kurz nachdem der gebürtige Winterthurer aus den USA nach Basel kam, veröffentlichte er zusammen mit David P. DiVincenzo vom IBM-Forschungszentrum T. J. Watson in Yorktown Heights im US-Staat New York eine Aufsehen erregende Arbeit über das Quantenrechnen mit Elektronen. Nun sind Elektronen jene negativ geladenen Elementarteilchen, die jeden Atomkern umschwirren und gemeinhin nicht fürs Rechnen, sondern für die Chemie eines Elements oder eines Moleküls zuständig sind. Loss und DiVincenzo zeigten, dass Elektronen im Prinzip auch rechnen können, wenn man einzelne von ihnen richtig miteinander kommunizieren lässt. Und weil das Verhalten einzelner Elektronen nur mit den Regeln der Quantenwelt beschrieben werden können, wäre das dann ein Quantencomputer.
Weiter zeigten die beiden, dass sich beliebig viele «Elektronenrechner» auf einem Chip anordnen lassen. Ein auf Elektronen basierender Quantencomputer wäre somit beliebig erweiterbar, und er liesse sich mit dem gängigen Halbleitermaterial Gallium-Arsenid bauen; ein Aspekt, der für die praktische Umsetzung sehr wichtig ist. Und um die geht es beim Nanoschwerpunkt an der Universität Basel. Loss betont, dass sein Ansatz nicht der einzige Weg zu einem Quantencomputer sei. Andere versuchen das selbe mit «rechnenden» Atomkernen oder Ionen zu erreichen, wobei erste einfache Quantencomputer im Labor auch schon funktionierten, doch seien sie die einzigen, die ein Konzept für einen echten, erweiterbaren Quantencomputer hätten.
Verglichen mit einem Quantencomputer sähen die schnellsten heute verfügbaren Rechner in jeder Beziehung alt aus. Sie basieren auf einem Konzept für Rechenmaschinen, die der Urgrossvater der Computer, der britische Mathematiker Charles Babbage (1792-1871), bereits im 19. Jahrhundert entworfen hatte, aufgrund von technischen Unzulänglichkeiten aber nicht verwirklichen konnte. Daniel Loss und andere Theoretiker stehen mit dem Quantencomputer jetzt an einem ähnlichen Punkt, nur basieren diese nicht auf der klassischen, auf Aristoteles

zurückgehenden uns vertrauten Rechenlogik, sondern fussen auf den Prinzipien der Quantenmechanik, deren scheinbar verquere Logik während den zwanziger Jahren des vergangenen Jahrhunderts von Wissenschaftlern wie Niels Bohr, Werner Heisenberg und Erwin Schrödinger entwickelt wurde.

Quantencomputer sagen Jein

Ein herkömmlicher Computer, wie er auf Schreibtischen oder in Supercomputer-Zentren zu finden ist, rechnet nach dem Prinzip des «entweder/oder». Jegliche Information, zum Beispiel eine Zahl, wird in Bits zerlegt. Ein Bit ist die kleinste Informationseinheit und wurde übrigens vom kürzlich verstorbenen Kommunikationstheoretiker Claude Shannon erfunden. Er ist gewissermassen der Grossvater der Computer. Ein Bit ist entweder 0 oder 1, kann entweder für wahr oder falsch stehen, entweder Ja oder Nein lauten. Dazwischen gibt es nichts.
Ein Quantencomputer hingegen kann sowohl Ja als auch Nein sagen, und auch Jein. Denn er funktioniert nach dem in der Politik weit verbreiteten Prinzip des kräftigen «sowohl als auch». Technisch ausgedrückt: Das Quantenbit, abgekürzt qubit, kann gleichzeitig den Wert 0 und 1 annehmen und alles dazwischen. Wobei - und hier steigt der gesunde Menschenverstand aus - diese Überlagerung zweier Werte nur solange «existiert», wie sie nicht aus unserer Alltagswelt «beobachtet» werden. Richtig eingesetzt, lässt sich diese Eigenart der Quantenphysik für bestimmte Rechenprozesse nutzen.
Aber wie? Daniel Loss ist überzeugt, dass das Elektron der ideale Träger für die Quantenbits ist. Genauer gesagt: der Eigendrehimpuls der Elektronen, genannt Spin, der sich, wenn Elektronen in grosser Zahl auftreten, als Magnetismus manifestiert. Jedes Elektron rotiert, wobei sein Spin bei Beobachtung aus der klassischen (also Alltags-) Welt nur entweder nach oben oder nach unten zeigen kann. In der Quantenwelt jedoch kann der Spin eines Elektrons gleichzeitig sowohl ein bisschen nach unten als auch ein bisschen nach oben zeigen. Der Elektronenspin taugt also als Quantenbit und ist so Daniel Loss' fundamentale Recheneinheit für den Quantencomputer.

Schrödingers Katze

Diese für den Quantencomputer ausschlaggebende Überlagerung verschiedener Elektronenspins lässt anhand eines Gedankenexperiments beschreiben, das der österreichische Quantenmechaniker Erwin Schrödinger erfunden hat. Nehmen wir an, das Leben einer Katze hinge vom Spin eines bestimmten Elektrons ab. Sobald der Spin von oben nach unten wechselt, öffnet sich eine Patrone mit Giftgas, das die Katze sofort tötet. Jedes Mal, wenn ein klassischer Beobachter einen Blick auf die Katze wirft, ist diese logischerweise entweder tot oder lebendig. Solange er dies nicht tut, also nicht beobachtet, ist die Katze von der Quantenwelt abhängig, und da kann sie gleichzeitig sowohl ein bisschen tot als auch ziemlich lebendig sein. Das erscheint zwar mehr als nur ein bisschen seltsam, aber ein Pfeiler der Quantenmechanik.
Angewandt in einem Quantencomputer ergibt dieser Überlagerungseffekt eine verblüffende Parallelität im Rechnen. Während ein klassischer Computer nur eine Zahl auf einmal darstellen und verarbeiten kann, sind es beim Quantencomputer im Prinzip beliebig viele, je nach Anzahl der Bits, die es für ihre Darstellung braucht. Ein Quantencomputer lässt sich deshalb als Computer verstehen, bei dem viele Rechenprozessoren, von denen in einem normalen Computer nur einer sitzt, parallel geschaltet werden. Ein Quantencomputer wäre demnach am ehesten mit einem massiv parallel geschalteten, herkömmlichen Computer zu vergleichen.
Dazu ein Beispiel: Ein herkömmlicher Computer kann in einem Schritt jeweils nur eine von vier zweistelligen Qubit-Zahlen (Kombinationen von 0 und 1) 0, 1, 2 oder 3 verarbeiten, ein

Quantencomputer jedoch alle vier auf einmal. Er braucht also für eine bestimmte Operation nur einen Viertel der Zeit. Die dreistelligen Qubit-Zahlen (0 bis 7) vermag er alle acht auf einmal zu schlucken, bei 4-Qubit-Zahlen sind es 16 und so fort. Für das Rechnen mit 128-stelligen Zahlen, wie sie für die sichere Übermittlung im Internet verwendet werden, schliesslich erreicht die theoretische Beschleunigung schon 2 hoch 128, das ist eine 1 mit 38 Nullen. Die Software, also die Befehle, welche einem Quantencomputer erteilt werden müssten, ist seit einigen Jahren bekannt. Die Theoriegruppe um Daniel Loss und ihre experimentell orientierten Mitstreiter im Rahmen des Forschungsschwerpunkts «Nanowissenschaften wollen nun die entsprechende Hardware dafür schmieden. «Dabei geht es gewissermassen um den grundlegenden Lego-Baustein, mit dem dann ein richtiger Quantencomputer gebaut werden kann», sagt Loss. Das sei viel mehr als ein Ingenieurproblem. Vielmehr stelle sich die fundamentale Frage, ob «die Hardware des Quantencomputers in der physikalischen Realität überhaupt machbar ist». Der experimentelle Beweis dafür fehlt noch, doch gebe es kein physikalisches Gesetz, das gegen eine Verwirklichung spreche.
Die Lösung des Problems liegt in der Antwort auf die folgende Frage: Wie bringe ich einen Quantencomputer dazu, sich mit klassischen Daten füttern zu lassen und die quantenmechanisch errechneten Ergebnisse wiederum klassisch auszuspucken? Ein Rechenergebnis, das unerfahrbar bleibt, nützt schliesslich niemandem etwas. Oder anders und technischer formuliert: Gibt es eine Maschine, welche die Information, die in den Qubits der Elektronenspins steckt, lange genug aufrecht erhält, damit sie in die reale Alltagswelt gerettet und damit auch verwendet werden kann? Und damit ist ein weiteres grundsätzliches Problem der Quantenphysik angesprochen: die Quantenwelt der Elektronen ist eine sehr labile. Stört nur das geringste ihre Kreise, ist alles hin und die errechnete Information unwiederbringlich zerstört. Physiker nennen das Dekohärenz. Auf eine technische Frage reduziert, lautet die Aufgabe, den Zustand eines einzigen, unvorstellbar schwachen Elektronenspins zu messen, der zudem von Milliarden von störenden Atomen umgeben ist.

Wasserstoff-Molekül ohne Kern

Die Lösung, die Loss vorgeschlagen hat und die jetzt im Schwerpunkt Nanowissenschaften angestrebt wird, steckt in künstlichen Atomen, auf englisch auch Quantum Dots (Quantenpunkte) genannt. Zwei einzelne Elektronen werden in je einem künstlichen Atom eingefangen und nebeneinander platziert. Das Ganze entspricht damit einem 2-Qubit-System, das den Grundbaustein für einen Quantencomputer bilden könnte. Als Ganzes entsprechen die beiden künstlichen Atome einem Wasserstoff-Molekül (H_2) ohne Atomkerne (siehe Bild Seite 3). Die beiden Elektronen sind zwar räumlich getrennt, können aber über quantenphysikalische (Tunnel-)Effekte miteinander kommunizieren.
Die Kommunikation zwischen den beiden Elektronen spielt für die Rechenfähigkeit des Quantencomputers eine zentrale Rolle. Im Fachjargon wird sie Verschränkung genannt und stellt die verblüffendste Eigenschaft der Quantenmechanik dar: Die beiden Elektronen wissen voneinander, in welchem Zustand sie sich befinden, und verhalten sich so, als ob sie ein einziges System wären. Im Prinzip können sie räumlich beliebig weit voneinander entfernt werden. Allerdings ist die Verschränkung unablässig von der allgegenwärtigen Dekohärenz bedroht und ist deshalb sehr schwer zu beobachten.
Künstliche Atome zu bauen, mit denen das dennoch gelingt, wird die Aufgabe von Klaus Ensslin von der ETH Zürich sein. Der Spezialist auf Halbleiterstrukturen wird in Zusammenarbeit mit Christian Schönenberger von der Uni Basel versuchen, den Grundbaustein für einen Quantencomputer zu bauen. Als Grundmaterial kommt zum Beispiel Gallium-Arsenid in Frage, das heutzutage in Mobiltelefonen eingesetzt wird. Es wird jedoch

auch mit exotischeren Materialien experimentiert werden. Erstes Ziel ist es, ein funktionierendes Zwei-Qubit-System zu fabrizieren.
Soweit die theoretischen Aussagen reichen, sollte das klappen: Die in einem Qubit verborgene Information kann via die negative Ladung der Elektronen in das System hinein- und wieder hinaustransportiert werden, wobei das Zeitfenster, bis die Spin-Zustände der Elektronen der allgegegenwärtigen Dekohärenz zum Opfer fallen, gross genug (einige hundert Nanosekunden) sein sollte, um sie via herkömmliche Leiterbahnen (einige hundert Mikrometer) in die Alltagswelt zu retten. Anders ausgedrückt: die in den Spinzuständen der Elektronen steckende Information überlebt lange genug, damit sie abgezapft werden kann. Gelingt dieses Unterfangen, wäre die erste und höchste Hürde auf dem Weg zu einem echten Quantencomputer genommen, sagt Loss. Dann wäre an den nächsten Schritt zu denken: den Bau eines logischen XOR-Gatters, das sich aus zwei oben beschriebenen künstlichen Atomen zusammensetzt. Damit wäre eine weitere wichtige Hürde genommen und der echte Quantencomputer wäre in Griffweite. Denn XOR-Gatter sind die logischen Arbeitspferde aller Computer, sämtliche notwendigen mathematischen Operationen lassen sich damit ausführen. Und hier käme die Erweiterbarkeit von Daniel Loss' Konzept zum Tragen. Sind die ersten beiden Hürden genommen, lassen sich die XOR-Gatter beliebig nebeneinanderreihen und ein echter Quantencomputer damit bauen.

Forschungsgelder aus den USA

Ob und wann dies gelingen wird, darüber wagt Loss keine Aussagen: «Ich bin Grundlagenforscher und freue mich schon jetzt auf die interessante Physik, die wir unabhängig vom Erreichen des Ziels Quantencomputer sehen werden.» Doch die Zeichen stehen gut. An einem Kongress in Seattle (USA) hat er soeben erfahren, dass er zusammen mit fünf anderen Top-Forschungsgruppen an den Universitäten Harvard, Princeton, Urbana (alle USA), Delft und Tokio über fünf Jahre einen amerikanischen Forschungskredit in Millionenhöhe erhalten wird. Ziel des Konsortiums: Einen Quantencomputer zu bauen, der einen Rechenvorgang mit 30 aufeinanderfolgenden Schritten ausführen kann.
Das sind gute Nachrichten nicht nur für Daniel Loss, der das Konsortium als theoretischer Kopf leiten wird, sondern auch für die beteiligten Forschungsgruppen im Schwerpunkt «Nanowissenschaften». Denn die neuen Erkenntnisse des weltweiten Konsortiums werden auch den Schweizer Effort vorantreiben, und umgekehrt. Es sieht ganz danach aus, als ob die Universität Basel definitiv zu einem globalen Schwerpunkt des Rechnens mit Quanten geworden ist. Thomas Müller

Von Thomas Müller