Quantenrechner

Ideen der Informatik

Kurt Mehlhorn

max planck institut
informatik

SIC Saarland
Informatics Campus

Übersicht

Vorteile von Quantenrechnern

Heutige Rechner beruhen auf klassischer Physik.
Quantenphysik erlaubt aber eine größere Klasse von Rechnern, die für manche Probleme potentiell schneller sind.

Problem	klassisch	Quantenrechner
Sortieren, kürzeste Wege, ...	keine Änderung	
Faktorisieren	kein polynomieller Alg. bekannt	Polynomzeitalgorithmus (Peter Schor)
Simulation von Quantenphysik	kein polynomieller Alg. bekannt	Polynomzeitalgorithmus
Suchen in ungeordneter Datenbank	kein sublinearer Alg. möglich	$\sqrt{\text{Größe}}$ möglich (Lov Grover)
Sichere Datenübertragung	nur unter Annahmen, z.B. Faktorisieren ist schwer	möglich, ohne jegl. Annahmen
Asymm. Kryptogr.	nur unter Annahmen, z.B. Faktorisieren ist ...	die meisten Verfahren werden unsicher
Symm. Kryptogr.	da ändert sich nichts	

Realisierung von Quantenrechnern steht noch am Anfang

Was macht Quantenrechner so mächtig?

Klassisch: Ein Register mit n Bits ist in genau einem von $N = 2^n$ möglichen Zuständen. Wir identifizieren die möglichen Zustände mit den Zahlen 0 bis $N - 1$.

Quantenrechner: Ein Quantenregister mit n Qbits (Quantenbits) kann gleichzeitig ein bißchen in jedem der N möglichen Zustände sein.

Das Register ist in einer Überlagerung (Superposition) der N möglichen Zustände: mit Gewicht w_0 im Zustand 0, mit Gewicht w_1 im Zustand 1, ..., mit Gewicht w_{N-1} im Zustand $N - 1$.

Rechnungen operieren auf diesen Überlagerungen und wirken parallel auf allen 2^n reinen Zuständen. Parallelität ist aber nicht beliebig.

$n = 20$, klassisch: in einem von 10^6 Zuständen;
Quanten: ein bißchen in jedem der 10^6.

Überlagerungen

Zustand eines Quantenregisters mit n Qbits ist ein Vektor ($N = 2^n$)

$$(w_0, w_1, \ldots, w_{N-1})$$

von $N - 1$ komplexen Zahlen mit Norm 1, d.h., $\sum_i |w_i|^2 = 1$. Die Gewichte sind also komplexe Zahlen.

Komplexe Zahlen sind Zahlen der Form $a + bi$, wobei $i = \sqrt{-1}$.

$$(a + bi) + (c + di) = (a + c) + (b + d)i \qquad \text{Addition}$$

$$(a + bi) \cdot (c + di) = (ac - bd) + (ad + bc)i \qquad \text{Multiplikation}$$

$$|w|^2 = a^2 + b^2 \qquad \text{Betrag, } w = a + bi$$

$n = 20$, klassisch: Zustand ist eine ganze Zahl zwischen 0 und 10^6
Quanten: Zustand ist ein Vektor von 10^6 komplexen Zahlen

Rechnen und Messen

Zustand eines Quantenregisters mit n Qbits ist ein Vektor ($N = 2^n$)

$$(w_0, w_1, \ldots, w_{N-1})$$

von $N - 1$ komplexen Zahlen mit Norm 1, d.h., $\sum_i |w_i|^2 = 1$.

Grundoperationen: Quantenphysik erlaubt jede Operation, die jeden Vektor der Norm 1 eineindeutig in einen Vektor der Norm 1 überführt (unitäre Transformationen).

$w \mapsto Uw$, wobei U eine komplexe Matrix mit Determinante ± 1.

Manche Operationen erlauben eine effiziente Realiserung in Quantenhardware. Welche das sind, hängt von der Technologie ab.

Bemerkung: Quantenrechner rechnen im Verborgenen. Wenn man ein Register inspiziert, dann sieht man einen klassischen Zustand. Man sieht den Zustand i mit Wahrscheinlichkeit $|w_i|^2$.

erfordern eine neue Denkweise, da die Grundoperationen gänzliche andere sind.

Erfahrung im klassischen Algorithmenentwurf hilft wenig.

Suchen (ohne weitere Information)

Eingabe: eine klassisches Schaltnetz f bestehend aus Und, Oder, und Nicht-Gattern mit n booleschen Eingaben mit der Eigenschaft, dass es genau eine Eingabe x^* gibt mit $f(x^*) = 1$.

Ausgabe: x^*.

Klassisch: man geht die $N = 2^n$ möglichen Eingaben durch, bis man x^* findet. (Vorlesung Suchen)

Laufzeit: N im schlechtesten Fall, $N/2$ im Mittel.

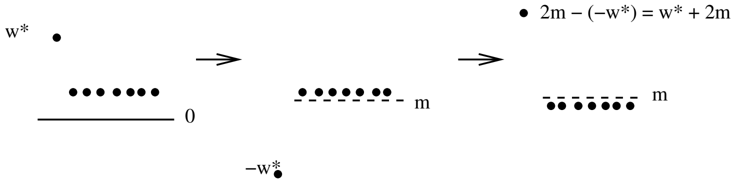
Besser geht es nicht.

Grovers Quantenalgorithmus braucht nur Zeit $O(\sqrt{N})$.

Der Algorithmus benutzt zwei Operationen; beide Operationen sind unitär und daher im Prinzip möglich:

Phase Inversion bei x^*: Vorzeichen des Gewichts von x^* wird geändert, alle anderen Gewichte bleiben gleich.

Spiegeln am Mittelwert: für all i wird w_i ersetzt durch $m + (m - w_i)$, wobei m der Mittelwert aller Gewichte ist.



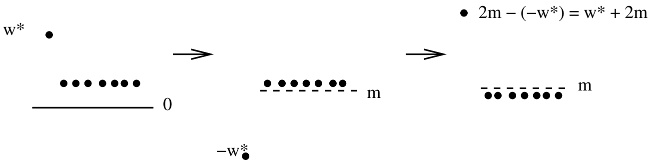
Grovers Quantenalgorithmus braucht nur Zeit $O(\sqrt{N})$.

Initialisierung: $w_i := \frac{1}{\sqrt{N}}$ für alle i.

Wiederhole

- Phase Inversion, d.h. flippe Vorzeichen des Gewichts von x^*.
- Spiegeln am Mittelwert

bis das Gewicht von x^* über $1/\sqrt{2}$ liegt. Inspektion liefert dann x^* mit Wahrscheinlichkeit $\geq 1/2$.



Das Gewicht von x^* wächst in einer Iteration um das Doppelte des aktuellen Mittelwerts. Der Mittelwert ist am Anfang $1/\sqrt{N}$ und wird im Laufe der Rechnung unwesentlich kleiner. Also wächst das Gewicht von x^* um mindestens um $1/\sqrt{N}$ in jeder Iteration. Also $\leq \sqrt{N}$ Iterationen.

Stand der Technischen Realisierung

Viele große Computerfirmen (IBM, Google, Microsoft, Intel) und einige Startups entwicklen Quantencomputer. Universitäten und Forschungsinstitute arbeiten an den Grundlagen.

Schwierigkeiten gemäß Bericht der NAS (National Academy of Science)

- Qubits Cannot Intrinsically Reject Noise
- Error-Free QC Requires Quantum Error Correction
- Large Data Inputs Cannot Be Loaded into a QC Efficiently
- Quantum Algorithm Design Is Challenging
- Quantum Computers Will Need a New Software Stack
- The Intermediate State of a Quantum Computer Cannot Be Measured Directly

To create a quantum computer that can run Shor's algorithm to find the private key in a 1024-bit RSA encrypted message requires building a machine that is more than five orders of magnitude larger and has error rates that are about two orders of magnitude better than current machines, as well as developing the software development environment to support this machine.

Quantenrechner: Zusammenfassung

Heutige Rechner beruhen auf klassischer Physik.
Quantenphysik erlaubt aber eine größere Klasse von Rechnern, die für manche Probleme potentiell schneller sind.

Problem	klassisch	Quantenrechner
Sortieren, kürzeste Wege, ...	keine Änderung	
Faktorisieren	kein polynomieller Alg. bekannt	Polynomzeitalgorithmus (Peter Schor)
Simulation von Quantenphysik	kein polynomieller Alg. bekannt	Polynomzeitalgorithmus
Suchen in ungeordneter Datenbank	kein sublinearer Alg. möglich	$\sqrt{\text{Größe}}$ möglich (Lov Grover)
Sichere Datenübertragung	nur unter Annahmen, z.B. Faktorisieren ist schwer	möglich, ohne jegl. Annahmen
Asymm. Kryptogr.	nur unter Annahmen, z.B. Faktorisieren ist ...	die meisten Verfahren werden unsicher
Symm. Kryptogr.	da ändert sich nichts	

Realisierung von Quantenrechnern steht noch am Anfang.