Quantenrechner

Ideen der Informatik

Kurt Mehlhorn

max planck institut
informatik

16. Januar 2016

Übersicht

- Vorteile von Quantenrechnern
- Qbits und Überlagerungen
- Quantenrechner
- Grovers Algorithmus
- Technische Realisierung
- Zusammenfassung

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
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, etwa Faktorisieren ist schwer	möglich, ohne jegl. Annahmen
Asymm. Kryptogr.	nur unter Annahmen, etwa Faktorisieren ist schwer	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 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.

Es ist in einer Überlagerung (Superposition) der N möglichen Zustände, d.h., 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 können gleichzeitig auf allen Gewichten wirken.

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 $i = \sqrt{-1}$.

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

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

$$\overline{w} = a - bi \qquad \text{Konjugation, } w = a + bi$$

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

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., $\sum_i |w_i|^2 = 1$. Die Gewichte sind also komplexe Zahlen.

Quantenphysik erlaubt jede Operation, die jeden Vektor der Norm 1 eineindeutig in einen Vektor der Norm 1 überführt. Manche solche Operationen erlauben eine effiziente Realiserung in Quantenhardware. Welche das sind, hängt von der Technologie ab.

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

Suchen (ohne weitere Information)

Eingabe: eine klassisches Schaltnetz (bestehend aus Und, Oder, Nicht) f 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.

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:

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 $O(\sqrt{N})$.

Algorithmus von Grover:

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

Wiederhole

- Phase Inversion, d.h. Vorzeichen des Gewichts von x^* wird geändert, alle anderen Gewichte bleiben gleich.

- Spiegeln am Mittelwert, d.h. für all i wird w_i ersetzt durch $2m - w_i$, wobei m der Mittelwert aller Gewichte ist.

bis das Gewicht von x^* über $1/\sqrt{2}$ liegt.

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 $1/2$ liegt.

Das Gewicht von x^* wächst (fast) um $2/\sqrt{N}$ in jeder Iteration.
Also $\leq \sqrt{N}/2$ Iterationen.

Technische Realisierung

- Quantenrechner mit wenigen Qbits wurden realisiert; höchstens fünf.
- 2012: Quantum Factorization of 143 on a Dipolar-Coupling NMR system
- Firma D-WAVE verkauft einen Quantencomputer mit angeblich 503 QBits.
- Science 2014: The D-Wave computer, marketed as a groundbreaking quantum machine, solves problems no faster than an ordinary rival, a new test shows. . . . , the time it took the D-Wave machine to solve a problem increased exponentially with the problem's size, just as with a conventional computer, report . . . . Some researchers call the test . . . the fairest comparison yet. But D-Wave argues that the computations used in the study were too easy to show what its novel chips can do.
- D-WAVE Aktien kosten unter einem Dollar; Hoch war 150$.

Quantenrechner: Zusammenfassung

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

Problem	klassisch	Quantenrechner
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, etwa Faktorisieren ist schwer	möglich, ohne jegl. Annahmen
Asymm. Kryptogr.	nur unter Annahmen, etwa Faktorisieren ist schwer	die meisten Verfahren werden unsicher
Symm. Kryptogr.	da ändert sich nichts	

Realisierung von Quantenrechnern steht noch am Anfang