Quantum Computing

Seminar: Informatikanwendungen in Nanotechnologien

Wladislaw Debus

20.06.2006

Inhalt

Einführung

Was ist Quantum Computing

Ein Quantencomputer ist ein Computer, der die Gesetze der Quantenmechanik ausnutzt, um gewisse Rechungen effizienter durchzuführen, als konventionelle Computer.

- eine neue art des Rechnens
- hohe Parallelität
- hohe technische Voraussetzungen

1 Einführung

2 Aufbau eines Quantencomputers
- Qubits
- Quantenregister
- Schaltkreise

3 Komplexitätsklassen

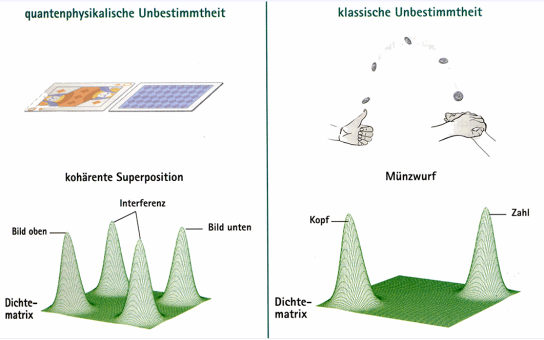
4 Quantenalgorithmen
- Faktorisierung nach Shor
- Suchalgorithmus von Grover

5 Realisierung von Quantencomputern
- Ionenfallen
- Kernspinresonanz

Superposition

Definition

Superposition bedeutet die Überlagerung von zwei oder mehreren Zuständen eines Objektes. Die Zustände einer Superposition können nicht gleichzeitig beobachtet werden.

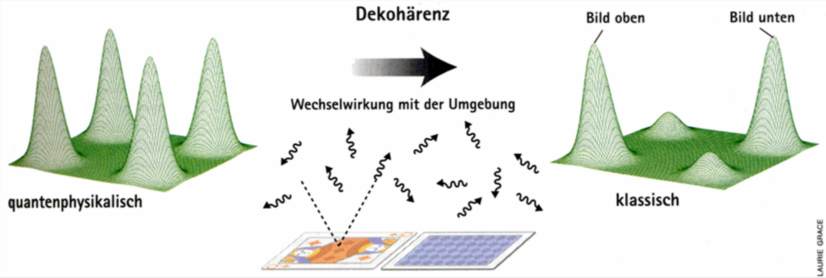


Vom Quant zum Kosmos, Spektrum Dossier

Dekohärenz

Definition

Eine Superposition mehrerer Zustände wird durch Wechselwirkung mit der Umgebung zerstört. Diesen Effekt nennt man Dekohärenz.



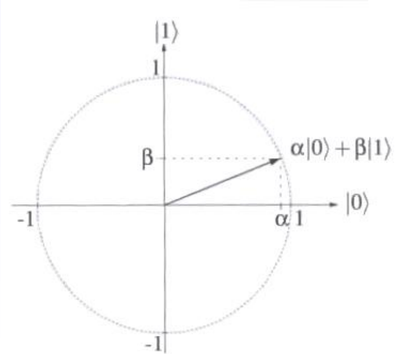
Vom Quant zum Kosmos, Spektrum Dossier

Qubits

Zustand eines Qubits:

$|\phi>= \alpha|0> +\beta|1>$ $\qquad \alpha, \beta \in \mathbb{C}$

mit $|\alpha|^2 + |\beta|^2 = 1$



Qubits

Mathematische Darstellung

Ersetze:

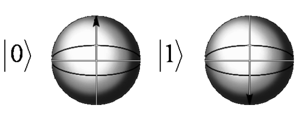
$$|0> \quad := \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

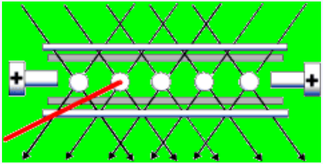
$$|1> \quad := \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

Dann gilt:

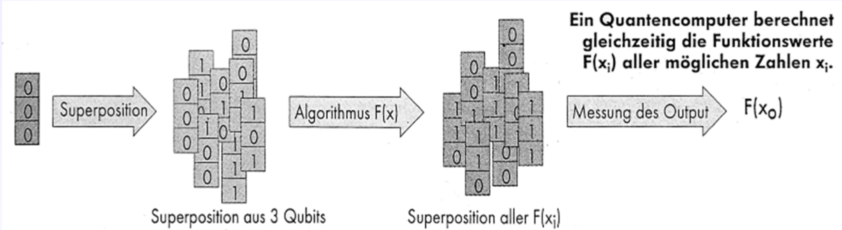
$$\alpha\ |0> + \beta\ |1> = \alpha \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \beta \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

Qubits - Realisierung





Operationen auf Qubits



Alice im Wunderland, c't 3/1997

Operationen auf Qubits

Operationen

dargestellt durch unitäre Matrizen $\quad \mathrm{A}^{-1} = (A^*)^T$

Beispiele

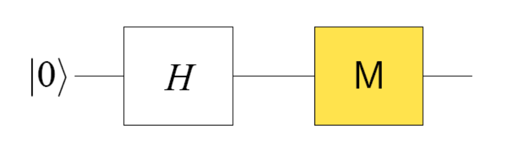
NOT $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$
$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

H $\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

$$\begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix}$$
$$\begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{pmatrix}$$

Ein Zufallsgenerator



Algorithmus

1. $|x\rangle \leftarrow |0>$
2. $|x\rangle \leftarrow H|x>$
3. Messe $|x\rangle$

Quantenregister

Quantenregister

$R = |x_1> |x_0>$

mit $|x_1>= \gamma_0 \ |0> + \gamma_1 \ |1>$

$|x_0>= \beta_0 \ |0> + \beta_1 \ |1>$

Einsetzen:

$|x_1> |x_0>= (\gamma_0 \ |0> + \gamma_1 \ |1>)(\beta_0 \ |0> + \beta_1 \ |1>)$

$= \alpha_{00} \ |00> + \alpha_{01} \ |01> + \alpha_{10} \ |10> + \alpha_{11} \ |11>$

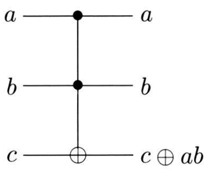
$$R = \begin{pmatrix} \alpha_{00} \\ \alpha_{01} \\ \alpha_{10} \\ \alpha_{11} \end{pmatrix}$$

Schaltkreise

Hadamard	$-\boxed{H}-$	$\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$
Pauli-X	$-\boxed{X}-$	$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$
Pauli-Y	$-\boxed{Y}-$	$\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$
Pauli-Z	$-\boxed{Z}-$	$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$
Phase	$-\boxed{S}-$	$\begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$
$\pi/8$	$-\boxed{T}-$	$\begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$

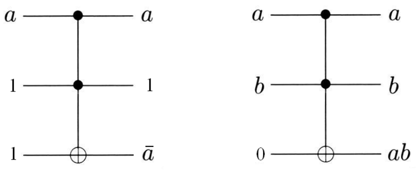
Simulation klassischer Schaltkreise

Toffoli-Gatter:



$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

Negation und Konjunktion mit einem Toffoli-Gatter:



Probleme bei der Realisierung

Reversibilität

Jede Rechnung muss reversibel sein.

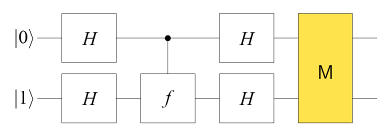
No-Cloning-Theorem

Es gibt keine unitäre Transformation, die einen Quantenzustand kopieren kann.

Unentscheidbarkeit von Zuständen

Zwei Zustände lassen sich nur dann zweifelsfrei unterscheiden, wenn sie zueinander orthogonal sind.

Das Problem von Deutsch



Ablauf

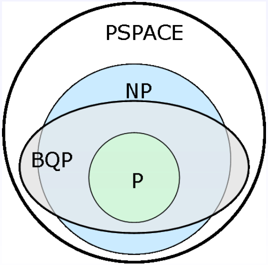
1. $|x>|y> \leftarrow |0>|1>$
2. Wende die Hadamard-Transformation H auf beide Bits an:
   $|x>|y> \leftarrow H|x> H|y>$
3. Werte f aus:
   $|x>|y> \leftarrow U_f|x> |y>$
4. Wende die Hadamard Transformation H auf beide Bits an:
   $|x>|y> \leftarrow H|x> H|y>$
5. Messe das Register:
   Hat $|x>$ den Wert $|0>$: Ausgabe konstant, sonst balanciert.

Quanten-Komplexitätsklassen

Klasse BQP

Durch Quantenschaltkreise polynomieller Grösse berechenbare Funktionen, bei einer Fehlerwahrscheinlichkeit $< \frac{1}{3}$

$$\mathcal{P} \subseteq \mathcal{BQP} \subseteq \mathcal{PSPACE}$$



Faktorisierungsalgorithmus von Shor

Ziel:

Schnelle Faktorisierung grosser Zahlen.

- Schnellster klassischer Algorithmus: $O(e^{n^{\frac{1}{3}}\ log(n^{\frac{2}{3}})})$
- Shors Algorithmus: $O(n^2)$
- benutzt Quanten-Fourier-Transformation.

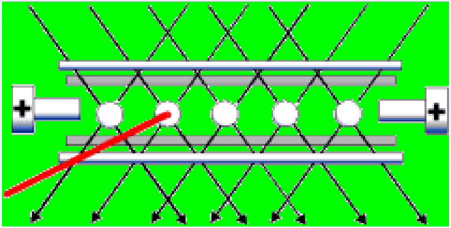
Suchalgorithmus von Grover

Ziel:

In einer Menge n unsortierter Daten muss ein ausgezeichneter Zustand x_0 gefunden werden.

- Algorithmus
  1. nimm einen n-Qubit Register
  2. erzeuge eine Superposition aller 2^n Zustände
  3. wende unitäre Transformationen auf das Register an, die die Amplitude des Ausgezeichneten Zustandes erhöht
  4. wiederhole die Transformation $O(\sqrt{n})$ mal an
  5. führe eine Messung durch - $W(x_0) = 1$
- Komplexität des Algorithmus $O(\sqrt{n}\ log(n))$

Ionenfallen



- Kette von Ionen in elektromagnetischer Falle
- Operationen werden durch Laserimpulse realisiert
- 1-Qubit Operationen umgesetzt
- Faktorisierung der Zahl 15
- nur wenige Sekunden Stabil

Kernspinresonanz

- Moleküle in flüssigem Zustand
- Operationen werden durch Radiofrequenzimpulse realisiert
- elementare Gatteroperationen umgesetzt
- Grovers Suchalgorithmus für vier Datensätze realisiert

Literatur

- Quantum Computing verstehen. Grundlagen - Anwendungen - Perspektiven von Matthias Homeister, Vieweg-Verlag
- Quantum Computing
  von Mika Hirvensalo, Springer-Verlag
- http://home.in.tum.de/ nguy-enh/files/qc/Quantencomputer.ppt
- www.wikipedia.de
- http://www.itp.uni-hannover.de/ kreutzm/data/qit1main.pdf
- http://www.thi.informatik.uni-frankfurt.de/ klauck/QC05.html