Quanteninformation/ Quantencomputer

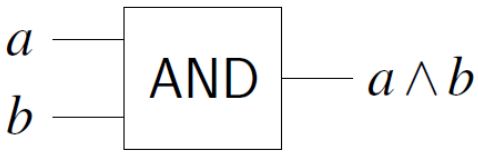
Jonas Heinze

Proseminar SS 2013

Übersicht

- Ein klassicher Computer arbeitet mit Bits {0,1}, realisiert durch *Spannung an* oder *Spannung aus*
- Register sind Kombination von Bits
- Ein Register mit n Bits kann 2^N verschiedene Zustände annehmen

- Register werden mithilfe von Logikgattern (engl. gates) verarbeitet
- Ein Logikgatter ist das AND-Gatter, welches die logische Verknüpfung $a \wedge b$ beschreibt



a	0	1	0	1
b	0	0	1	1
$a \wedge b$	0	0	0	1

- Komplexere Operationen lassen sich als Schaltkreis von Gattern darstellen

- Die Komplexitätstheorie beschreibt den Aufwand eines Problems
- Wichtige Komplexitätsklassen
  - **P**: von einer deterministischen Turingmaschine in Polynomialzeit lösbar
  - **NP**: von einer *nicht*deterministischen Turingmaschine in Polynomialzeit lösbar
  - **PSPACE**: von einer *nicht*deterministischen Turingmaschine in polynomiellen Platz lösbar
  - **EXPTIME** von einer deterministischen Turingmaschine in exponentieller Zeit lösbar
- P gilt als Grenze des Berechenbaren
- Der klassische Computer ist äquivalent zur deterministischen Turingmaschine

- Quantenbit (Qubit): Zustand eines Quantenmechanischen Zwei-Niveausystems (z.B. Spin)
- Dargestellt als Superposition der zwei Basiszustände: $|\Psi\rangle = \beta_0|0\rangle + \beta_1|1\rangle$
- Qubit kann *0* oder *1* annehmen, aber auch beliebige Überlagerungen.

Der Quantencomputer

Das Quantenregister

- Quantenregister:Zusammensetzung von Qubits
- Dargestellt als Tensorprodukt der Qubits:
  $R = |\Psi_0\rangle|\Psi_1\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$
- Quantenregister hat 2^N Basiszustände

Der Quantencomputer

Das Quantegatter

- Quantengatter: Unitäre $2^N \times 2^N$ Matrizen
- Schaltkreise durch Hintereinanderausführen bzw. Muliplizieren
- Da unitäre Matrizen invertierbar sind, ist jeder Algorithmus reversibel.

Der Quantencomputer

Vergleich mit klassischem Computer

- Der Quantencomputer kann einen klassischen Computer einfach simulieren.
- Der klassische Computer kann einen Quantencomputer ebenfalls simulieren, allerdings nur mit großem Aufwand.
  Diese Simulation liegt in PSPACE.
- Der Quantencomputer kann echte Zufallszahlen erzeugen
- Er kann deutlich besser "parallel"rechnen.

- Eine Münze sei echt, wenn eine Seite einen Adler und die andere eine Zahl zeigt. Tut sie dies nicht ist sie eine Fälschung. Wie oft muss man eine Müenze anschauen um die Echtheit festzustellen?
- Mathematisch: $f : \{0, 1\} \to \{0, 1\}$.
- Eine solche Funktion heißt konstant falls gilt $f(0) = f(1)$, sonst balanciert.
- Ist f konstant?

- Man sucht aus einer unsortierteten Menge ein bestimmtes Element.
- Mathematisch: $f : \{0, 2^N - 1\} \rightarrow \{0, 1\}$, wobei $f(i) = 1$, wenn i das gesuchte Element ist.
- Klassisch braucht eine solche Suche $O(n)$, Grovers Algorithmus hingegen nur $O(\sqrt{2})$
- Lässt sich auch auf die Suche nach beliebig vielen oder sogar unbekannt vielen Elementen erweiternt
- Ein sehr ähnlicher Algorithmus findet sogar das Minimum einer Menge.

- Man sucht die Primfaktorzerlegung einer Zahl N.
- Erste Vereinfachung: Es genügt, die Zahl N in zwei Teiler zu zerlegen.
- Restklassenrechnung: Gibt es ein nichttriviales r, sodass:

$$r^2 = 1 \mod N \Rightarrow r^2 - 1 = nN \Rightarrow (r+1)(r-1) = nN$$

  und $r \pm 1$ kein Vielfaches von N ist, so haben beide Teiler mit N gemeinsam.
- Suche ggT. Dieses Problem besitzt einen effizienten Algorithmus (euklidischer Algorithmus)

- Neues Problem: Finde ein r mit den obigen Eigenschaften.
- Suche die Ordnung der Zahl q Modulo N, also die ganze Zahl k:

$$q^k \mod N = 1$$

- Ist k gerade, so wähle $r = q^{k/2}$, wenn nicht versuche mit neuem q.
- Klassisch lässt sich die Ordnung nicht effizient berechnen.

- Quantenmechanisch: Operator U

$$U|x\rangle = |xq \mod N\rangle$$

- Suche die Ordnung der Zahl q Modulo N, also die ganze Zahl k:

$$q^k \mod N = 1$$

- Die Eigenwerte dieses Operators sind:

$$U|u_s\rangle = \lambda_s|u_s\rangle \Rightarrow \lambda_s^k = 1 \Rightarrow \lambda_s = e^{i\frac{2\pi s}{k}}$$

- Aus den Eigenwerten lässt sich die Ordnung bestimmen.

- Die Eigenwerte lassen sich durch die *diskrete Fouriertransformation* bestimmen.
- Quantenalgorithmus: Quantenfouriertransformation. Liefert Lösung mit hoher Wahrscheinlichkeit
- Liefert Lösung mit hoher Wahrscheinlichkeit nach $O(\log \log r)$ Wiederholungen
- Laufzeit insgesamt: $((\log n)^3)$

Algorithmen

Shor-Algorithmus

- ein Algorithmus zur Zerlegung in Primfaktoren in Polynialzeit.
- klassisch: exponentielle Zeit.
- Viele aktuelle Verschlüsselungen (z.B. RSA) basieren auf Nichtzerlegbarkeit von großen Zahlen.

Physikalische Umsetzung

Allgemeine Probleme

- *Relaxation*: Ein quantenmechanisches System neigt dazu, in seinen Grundzustand zurück zu fallen.
  Die Relaxationszeit ist dabei exponentialverteilt
- *Dekohärenz*: Durch äußere Einflüsse kann ein System in den Zustand $|0\rangle$ oder $|1\rangle$ gebracht werden.
  Die Superposition geht verloren.
- Daraus ergibt sich eine hohe Fehlerwahrscheinlichkeit bei aktuellen Systemen.

Physikalische Umsetzung

Architektur

- Ionen werden Ionenfallen kontrolliert.
- Ringströme in supraleitenden Materialien werden untersucht.
- An Stickstoff-FehlstellenZentren (NV-Zentren) werden Kernspins untersucht.

Physikalische Umsetzung

Architektur

- In Innsbruck konnte man den Shor-Algorithmus an einem 7 Qubit-Register zur Zerlegung von 15 in seine Primfaktoren nutzen.
- Es gelang, ein 14 Qubit-Register herzustellen
- "Die Chancen stehen bei 50%, dass sowas in 50 Jahren möglich ist "*Theodor Hänsch*

Quellen

- Michael A. Nielsen, Isaac L. Chuang: *Quantum Computation and Quantum Information.* Cambridge University Press, Cambridge 2000, ISBN 0-521-63503-90
- Matthias Homeister: *Quantum Computing verstehen.* Vieweg, Wiesbaden 2005, ISBN 3-528-05921-4
- http://iffwww.iff.kfa-juelich.de/ ekoch/QC05/truhnpaper.pdf (Stand 11.6.2013)
- http://www.drillingsraum.de/theodor_haensch/theodor_haensch_3.html (Stand 11.6.2013)