Quantenprogrammiersprachen

Felix Krohn, CN 7
<felix@kro.hn>

Hochschule Furtwangen
Aktuelle Themen der Informatik

10. November 2007

Übersicht

Einleitung

- “Ein Quant ist die kleinste, unteilbare Einheit oder Menge einer physikalischen Größe“
- Beispiel: Licht $\Rightarrow$ Photonen

Parallelismus, Superposition

- wesentliche Eigenschaft der Quantenmechanik
- Grund der höheren Rechenleistung eines Quanten-Computers
- Qubit muss keinen festen Zustand haben, sondern kann zwei beliebig komplexe Zustände auf ein Mal haben
- Zustand wird durch Messung beeinflusst und steht erst danach fest
- Beispiele: Schrödinger's Katze, Doppelspaltexperiment

No-Cloning-Theorem

- Qubits können nicht perfekt kopiert werden
- Kopieren heißt lesen; in diesem Fall: Messen
- Messen heißt aber verändern des Ursprung-Bits!
- Kopieren würde überlichtschnelle Informationsübertragung bedeuten $\Rightarrow$ widerspricht Relativitätstheorie und gefährdet Kausalitätsprinzip
- Auswirkungen:
  - Herkömmliche Fehlerkorrekturcodes funktionieren nicht mehr
  - Abhören einer Quantenkommunikation nicht ohne Veränderung der übertragenen Information möglich
  - $\Rightarrow$ Quantenkryptographie

No-Cloning-Theorem

- Qubits können nicht perfekt kopiert werden
- Kopieren heißt lesen; in diesem Fall: Messen
- Messen heißt aber verändern des Ursprung-Bits!
- Kopieren würde überlichtschnelle Informationsübertragung bedeuten $\Rightarrow$ widerspricht Relativitätstheorie und gefährdet Kausalitätsprinzip
- Auswirkungen:
  - Herkömmliche Fehlerkorrekturcodes funktionieren nicht mehr
  - Abhören einer Quantenkommunikation nicht ohne Veränderung der übertragenen Information möglich
  - $\Rightarrow$ Quantenkryptographie

No-Cloning-Theorem

- Qubits können nicht perfekt kopiert werden
- Kopieren heißt lesen; in diesem Fall: Messen
- Messen heißt aber verändern des Ursprung-Bits!
- Kopieren würde überlichtschnelle Informationsübertragung bedeuten $\Rightarrow$ widerspricht Relativitätstheorie und gefährdet Kausalitätsprinzip
- Auswirkungen:
  - Herkömmliche Fehlerkorrekturcodes funktionieren nicht mehr
  - Abhören einer Quantenkommunikation nicht ohne Veränderung der übertragenen Information möglich
  - $\Rightarrow$ Quantenkryptographie

No-Cloning-Theorem

- Qubits können nicht perfekt kopiert werden
- Kopieren heißt lesen; in diesem Fall: Messen
- Messen heißt aber verändern des Ursprung-Bits!
- Kopieren würde überlichtschnelle Informationsübertragung bedeuten $\Rightarrow$ widerspricht Relativitätstheorie und gefährdet Kausalitätsprinzip
- Auswirkungen:
  - Herkömmliche Fehlerkorrekturcodes funktionieren nicht mehr
  - Abhören einer Quantenkommunikation nicht ohne Veränderung der übertragenen Information möglich
  - $\Rightarrow$ Quantenkryptographie

No-Cloning-Theorem

- Qubits können nicht perfekt kopiert werden
- Kopieren heißt lesen; in diesem Fall: Messen
- Messen heißt aber verändern des Ursprung-Bits!
- Kopieren würde überlichtschnelle Informationsübertragung bedeuten $\Rightarrow$ widerspricht Relativitätstheorie und gefährdet Kausalitätsprinzip
- Auswirkungen:
  - Herkömmliche Fehlerkorrekturcodes funktionieren nicht mehr
  - Abhören einer Quantenkommunikation nicht ohne Veränderung der übertragenen Information möglich
  - $\Rightarrow$ Quantenkryptographie

Verschränkung

- 2 oder mehr Quanten können miteinander *verschränkt* werden
- können danach nicht mehr als einzelne Teilchen mit definierten Zuständen angesehen werden, sondern nur als Gesamtsystem
- entspricht Funktion mit mehreren Eingabewerten: bilden alle Lösungen einer Funktion $f(n1, n2, \ldots)$ *gleichzeitig*
- Messung des einen Teilchens legt auch den Zustand des anderen Teilchens fest
- Beispiel: Aufspaltung eines Photons
- Anwendung: sichere Übertragung von Schlüsseln in der Quantenkryptographie

Übersicht

Quanteninformatik

- Berechnung von Interaktion von n Partikeln mit Quantenmechanik braucht n^2 Operationen auf *normalem* Computer
- Jedoch findet die „Berechnung“ in der Natur nur mit n Partikeln statt!

⇒Idee

Entwurf eines Computers, der selber mit Quanten rechnet

Quanteninformatik

- Berechnung von Interaktion von n Partikeln mit Quantenmechanik braucht n^2 Operationen auf *normalem* Computer
- Jedoch findet die „Berechnung“ in der Natur nur mit n Partikeln statt!

⇒Idee

Entwurf eines Computers, der selber mit Quanten rechnet

Quantencomputer

- Keine eigenständigen Rechner
- durch herkömmliche Computer gesteuerte Einheiten
- Bisher nur unter Laborbedingungen und von kurzer Dauer

Qubits

- entsprechen der kleinsten Informationseinheit bei Quantencomputern
- kann prinzipiell unendlich viele verschiedene Zustände annehmen
- Durch Messung wird zufällig einer der möglichen Messwerte ausgewählt
- Wahrscheinlichkeit jedes Messwertes wird bestimmt durch den vor der Messung vorliegenden Zustand
- Beispiel: Polarisierung von Photonen (Doppelspaltexperiment)

Erzeugung von echten Zufallszahlen

- Zustandsmessung eines Qubits hebt dessen Superposition auf
- Qubit nimmt daher bei Messung einen zufälligen Zustand an
- Wert lässt sich nicht vorher von aussen ohne Messung bestimmen
- Daraus resultieren *echte* Zufallszahlen; im Gegensatz zu *Pseudo*zufallszahlen

Quanten-Suchalgorithmus

- Lov Grover, 1996: Suchen in unsortiertem Feld mit n Einträgen
- Laufzeit: $O(\sqrt{n})$
- Speicherbedarf: $O(\log n)$
- Ermöglicht folgende Operationen
  - Umkehrung einer endlichen Funktion $y = f(x)$
  - Berechnung von Mittelwerten und Medianen
  - Lösung NP-vollständiger Probleme durch schnelles Durchlaufen aller Möglichkeiten

Erzeugung von echten Zufallszahlen

- Zustandsmessung eines Qubits hebt dessen Superposition auf
- Qubit nimmt daher bei Messung einen zufälligen Zustand an
- Wert lässt sich nicht vorher von aussen ohne Messung bestimmen
- Daraus resultieren *echte* Zufallszahlen; im Gegensatz zu *Pseudo*zufallszahlen

Deutsch-Jozsa-Algorithmus

- einfachster Algorithmus
- Prüfung ob eine Funktion $f(x)$ konstant ($f(0) = f(1)$)oder gleichgewichtig ($f(0) \neq f(1)$) ist
- Wurde 2002 mit nur 2 Qubits in einer Ionenfalle implementiert

Shor-Algorithmus

- Faktorisierungsverfahren: zerlegt eine Zahl in dessen Teiler
- benötigt mindestens $\log(n)$ Qubits
- polynomielle Laufzeit: $O((\log n)^3)$
- beste Verfahren bisher: exponentielle Laufzeit
- Viele moderne Verschlüsselungsverfahren basieren auf der Annahme, daß Primfaktorzerlegung nicht effizient möglich ist!

Übersicht

Warum Quantenprogrammiersprachen?

- Bisher: QC als Feld der theoretischen Physik
- Daher Notationen, Matrizen, Operatoren etc. aus der Physik
- führt zu Desinteresse seitens der Informatiker
- Quantenprogrammiersprachen sollen Brücke zur Informatik schlagen
- Vereinheitlichung auch innerhalb der Physik benötigt

QCL - Quantum Computation Language

- Prozedurale Hochsprache, angelehnt an Sprachen wie C und Pascal
- Vereinigt herkömmliche Programmierung mit Quantenalgorithmen
- Quelloffen (GPL), Linux 2.6, glibc2.4, gcc 4.1
- Bernhard Oemer, TU Wien

Beispielcode: diskrete Fourier-Transformation (Coppersmith)

```
operator dft(qureg q) { // main operator
  const n=#q;           // set n to length of input
  int i; int j;         // declare loop counters
  for i=1 to n {
    for j=1 to i-1 {    // apply conditional phase gates
      V(pi/2^(i-j),q[n-i] & q[n-j]);
    }
    H(q[n-i]);          // qubit rotation
  }
  flip(q);              // swap bit order of the output
}
```

Beispielcode: 5QB-Rechner im Interpreter simulieren

```
$ qcl --bits=5 // Interpreter/Simulator mit 5 QB starten
[0/8] 1 |00000>// Status der 5 QB
qcl> qureg a[1];
qcl> dump a
: SPECTRUM a: |....0>
1 |0>// Status von a[1] ist 0 mit Wahrscheinlichkeit von 1
// Nur im Simulator möglich!
```

Qlang

- Erweiterung zu $C++$
- Klassen für grundlegende Quantenoperationen: QHadamard, QFourier, QNot, QSwap, QSwap, QReg (Speicherverwaltung)
- Erweiterung cQPL generiert C++-Code zur Ausführung im libqc-Simulator
- GPL-lizenziert, Linux 2.4 aufwärts, von Stefano Bettelli

Qlang Beispielcode

- Beispielcode:

```
qureg x1[2]; // 2-qubit quantum register x1
qureg x2[2]; // 2-qubit quantum register x2
H(x1); // Hadamard operation on x1
H(x2[1]); // Hadamard op on 1st QB qubit of register x1
```

Qlang

- mehr Beispielcode:

```
operator diffuse(qureg q) {
     H(q);                    // Hadamard Transform
     Not(q);                  // Invert q
     CPhase(pi,q);            // Rotate if q=1111..
     !Not(q);                 // undo inversion
     !H(q);                   // undo Hadamard Transform
}
```

Übersicht

Stand der Technik heute

- 1998: 2 QB-Rechner; Uni Berkeley
- 1999: 3 QB-Rechner; IBM
- 2000: 5 QB-Rechner; IBM
- 2001: 7 QB-Rechner; IBM. Faktorisiert die Zahl 15 in die Primzahlen 3 und 5
- Nicht in absehbarer Zeit marktreif
- Hoffnung auf Quantencomputer in 2020, wenn Moore's Law zu einem Ende kommen muss
- Angestrebtes Design: Quantenrechner als Ko-Prozessor für bestimmte Aufgabenstellungen

Fragen?

„I think I can safely say that nobody understands Quantum Mechanics.“

Richard P. Feynman

Quellen

- Artikel bei der GI
- Video zum Doppelspaltexperiment
- Grovers Suchalgorithmus
- IBM: Introduction to Quantum Computing
- QCL - A Programming Language for Quantum Computers
- Quantum Programming Language: qlang
- Quantencomputing für Normalsterbliche: Wikipedia
- „Quantum Computing verstehen“ von *Matthias Homeister*, Vieweg Verlag 2005 (Hochschulbibliothek)