TECHNISCHE UNIVERSITÄT DRESDEN

Fakultät Informatik Institut für Technische Informatik, Professur für VLSI-Entwurfssysteme, Diagnostik und Architketur

Der Quantencomputer

Unterschiede zum Digitalrechner und Nutzungsmöglichkeiten

Simon Willeke

Dresden, 17.05.2011

„The most beautiful thing
we can experience is the mysterious.
It is the source of all true art and all science.“

Albert Einstein

Gliederung

1 Funktionsweise

1.1 Informationsdarstellung

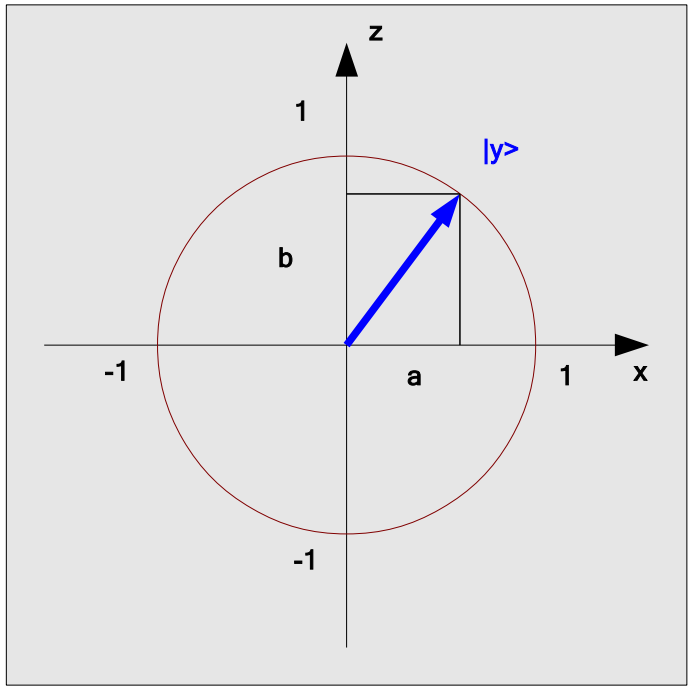
- Einheit der Information ist ein „Qubit“ (Quantum Bit)
- Basiszustände eines Qubit in Bra-Ket-Notation:
  - |0>
  - |1>

- Qubit sind Elemente eines 2-dimensionalen Hilbertraumes und lassen sich als Vektoren darstellen
  - $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$
  - $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$

1 Funktionsweise

1.1 Informationsdarstellung

- Qubit können sich in Superposition befinden
  - $|y\rangle = a|0\rangle + b|1\rangle =$
  - $|a|^2 + |b|^2 = 1$
- prinzipiell unendlich viele Zustände möglich (a und b sind komplexwertig)
- es kann nur $|0\rangle$ oder $|1\rangle$ gemessen werden, mit Wahrscheinlichkeit $|a|^2$ bzw. $|b|^2$



1 Funktionsweise

1.1 Informationsdarstellung

- Messung zerstört die Superposition
- Qubit befindet sich danach im gemessenen Basiszustand (Projektion)
- Interaktionen mit der Umwelt bewirken auch Wechsel zu Basiszustand
  - perfekte Isolierung notwendig
  - besonders kritisch bei hoher Qubit-Anzahl
  - Bezeichnung: Dekohärenz

1 Funktionsweise

1.2 Speicher

- N Qubit werden zu Register zusammengefasst
- jedes Qubit muss einzeln gemessen werden können
- Zustände der Qubit ebenfalls zusammengefasst, z.B. |000> (N=3)
- Hilbertraum der Dimension 2^N wird aufgespannt
- Basiszustände für N=3: |000>, |001>, |010>, |011>, … , |111>

- Komplettes Register kann sich in Superposition befinden
  - Beispiel

- Quantenverschränkung: Einzelzustände nichtmehr unabhängig

1 Funktionsweise
1.3 Datenverarbeitung

- beruht auf Multiplikation von Zustandsvektor und Matrix
- alle Matrizen müssen unitär sein, d.h. $M^* \bullet M = E$
  - Beispiel: NOT-Matrix

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

- Hadamard Transformation:
  - dient zum Erzeugen einer gleichmäßigen Superposition

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

1 Funktionsweise

1.3 Datenverarbeitung

- alle Funktionen $f(x_1...x_n)$ sind reversibel
- als Konsequenz muss Eingangs- und Ausgangsanzahl übereinstimmen
- Funktionsaufrufe haben die Form:

$$U_f |m\rangle |n\rangle = |m\rangle |n+f(m)\rangle$$

- n ist Ergebnis-Qubit und wird mit $|0\rangle$ initialisiert
- Ausgangszustände sind Permutationen der Eingangszustände
- gilt auch für Superposition: Linearkombination der Funktionswerte

1 Funktionsweise

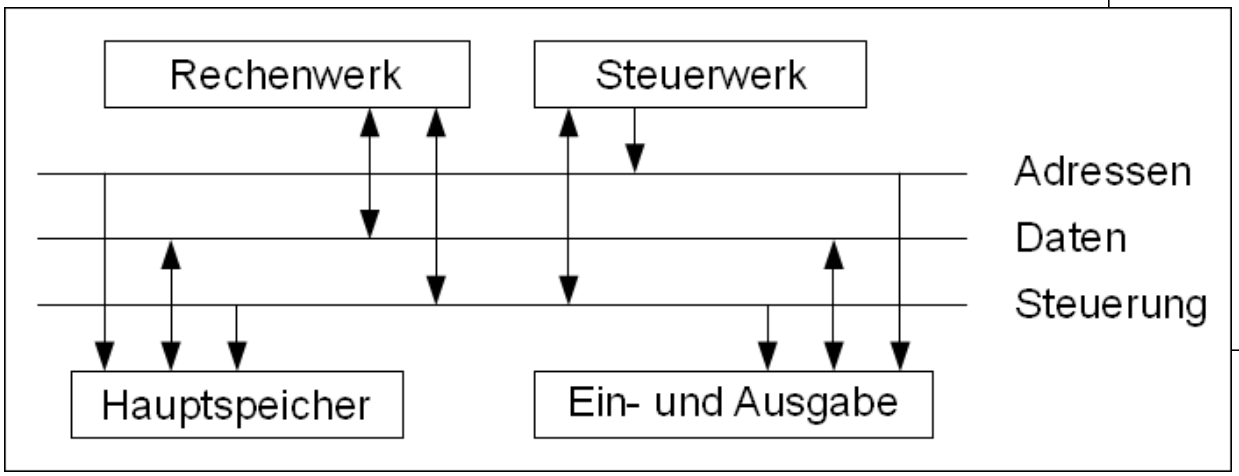
1.3 Datenverarbeitung

- Beispiel: AND mit Superposition
- Permutationen werden durch Standardgatter realisiert
  - NOT
  - C-NOT
  - Toffoli Gate
  - Fredkin Gate

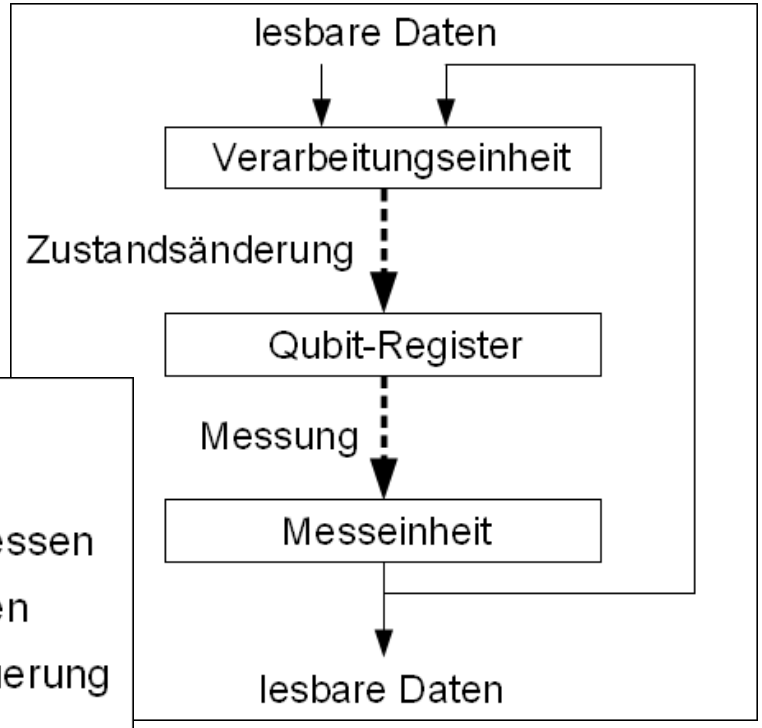
1 Funktionsweise

1.3 Datenverarbeitung

- Informationsfluss vs. Operationsfluss
- general Purpose vs. hohe Spezialisierung



Von-Neumann-Architketur

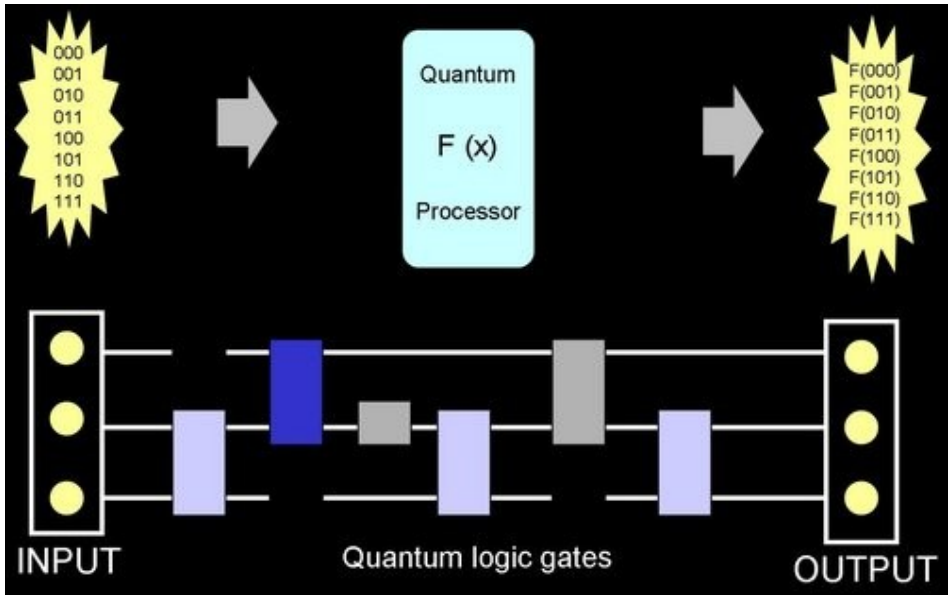


Quantencomputer - physische Struktur

1 Funktionsweise

1.3 Datenverarbeitung

- logische Struktur des Quantencomputers

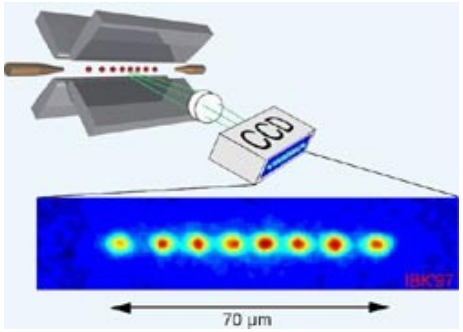


Quelle: http://www.quantiki.org/

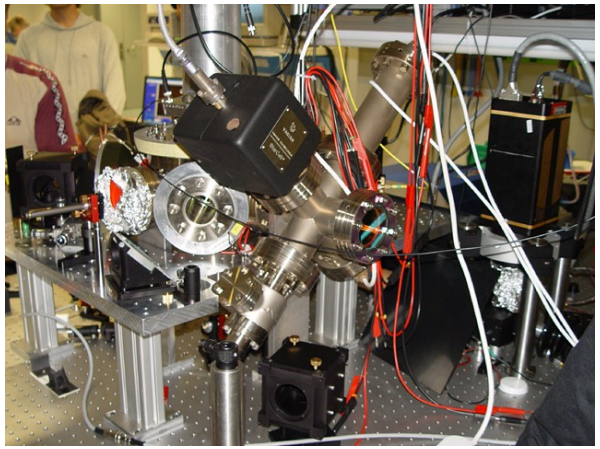
2 Vergleich mit Digitalrechner

2.2 Technologie

- Halbleitertechnologie und integrierte Schaltungen für Digitalrechner
- verschiedene Möglichkeiten für Quantencomputer
  - Ionen in Potentialfallen, Laserpulse zur Zustandsänderung



Quelle: http://www.innovations-report.de/

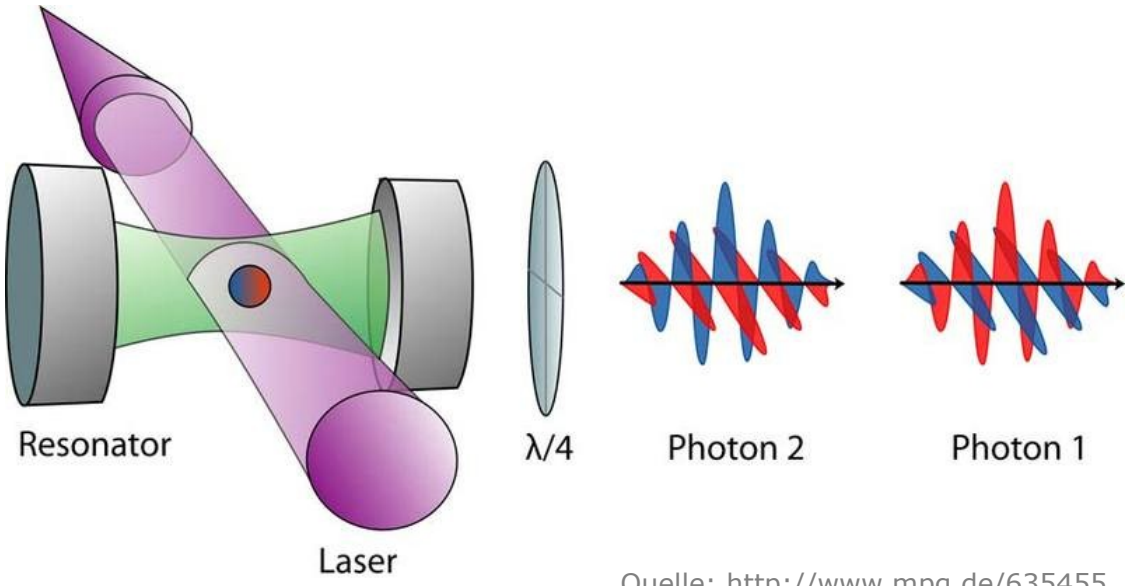


Quelle: https://wiki.ldv.ei.tum.de

2 Vergleich mit Digitalrechner

2.2 Technologie

- Photonenpolarisation, Laserpulse zur Zustandsänderung

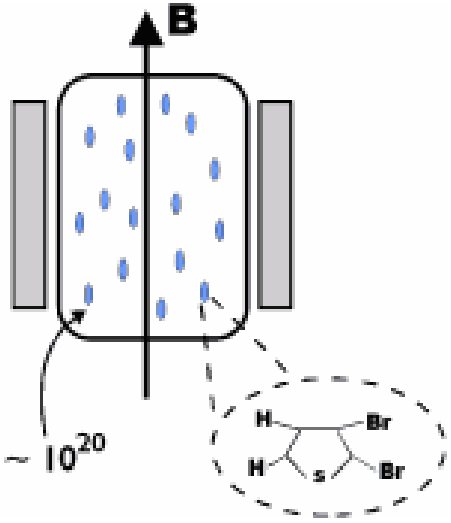


Quelle: http://www.mpg.de/635455

2 Vergleich mit Digitalrechner

2.2 Technologie

- Kernspin-Resonanz: Moleküle bei Zimmertemperatur, Magnetfelder zur Zustandsänderung
  - Probleme: alle Moleküle gleichzeitig beeinflusst, verschränkte Zustände bisher nicht erzeugbar



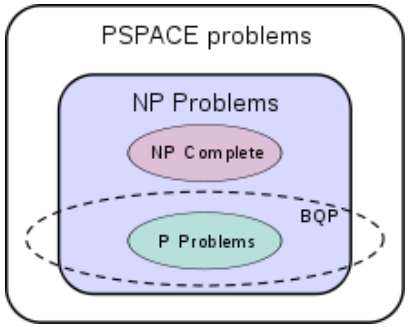
Quelle: http://www.mbezold.de

- bisherige Realisierungen mit 1-7 Qubit
- Dekohärenz problematisch, Fehlerkorrektur in Entwicklung

3 Nutzungsmöglichkeiten

3.1 Parallelisierbarkeit

- Superposition ermöglicht gleichzeitige Berechnung aller möglichen Werte in einem Rechenschritt
- „Massiver Parallelismus“
- Messung liefert immer nur einen Basiszustand
  - Nachbearbeitung notwendig
  - fehlerbehaftete Ergebnisse



- Komplexitätsklasse BQP liegt wahrscheinlich zwischen P und NP
  - BQP = bounded error, quantum, polynomial time

3 Nutzungsmöglichkeiten

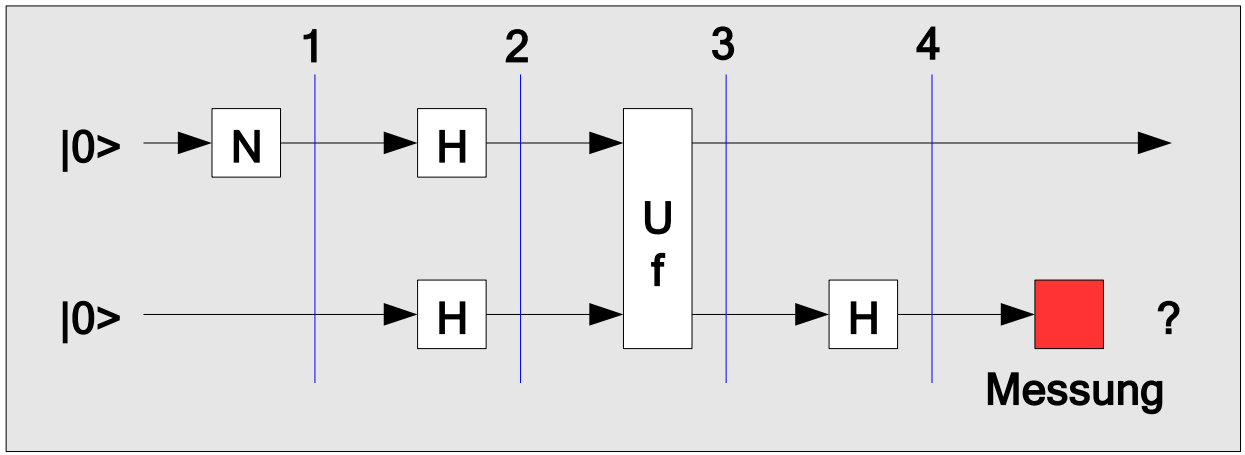
3.2 Anwendungen

- Faktorisierung
  - SHOR'scher Algorithmus
  - Zeitkomplexität $O((\log N)^3)$, besser als $O(e^{(\log N)^{1/3}} (\log \log N)^{2/3})$ klassisch
- Suche in ungeordneten Listen
  - GROVER'scher Algorithmus
  - Zeitkomplexität $O(\sqrt{N})$, besser als O(N) klassisch
- Black-Box-Algorithmen, z.B. Deutsch-Jozsa-Algorithmus
- uvm...

3 Nutzungsmöglichkeiten

3.3 Beispielalgorithmus

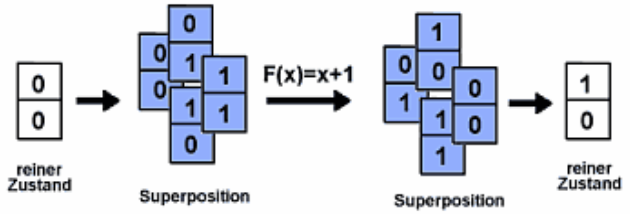
- nach „Quantencomputer 2“ von Franz Embacher (Universität Wien)
  - Deutsch-Jozsa-Algorithmus: Berechnung der Summe (mod 2) aller Funktionswerte einer (einstelligen) unbekannten Funktion U_f



4 Zusammenfassung

- Qubit ist kleinste Informationseinheit
- Qubit können überlagerte Zustände annehmen
- Operationen sind reversible Matrixmultiplikationen
- Superposition ermöglicht gleichzeitige Berechnung mehrerer Werte
- bisher nur kleine experimentelle Realisierungen
- Vorteil Digitalrechner: effizienter realisierbar, besser skalierbar
- Vorteil Quantencomputer: schnellere Algorithmen implementierbar

Quelle: http://www.qubit.org



Quelle: http://www.quantencomputer.de

5 Quellen

[1] "Algorithmen für Quantencomputer", aus: www.quantencomputer.de

[2] "Quantencomputer – Was verbirgt sich dahinter?", von Dr. Gesche Pospiech, Universität Frankfurt, http://user.uni-frankfurt.de/~pospiech/q_comp.html

[3] "Quantencomputer. Einige interaktive Modelle", von Franz Embacher, Universität Wien, http://homepage.univie.ac.at/franz.embacher/Quantencomputer/

[4] "Neue Bestleistungen bei Quantencomputern", von Günter Sturm, ScienceUp Sturm und Bomfleur GbR, http://www.quanten.de/quantencomputer.html

[5] "Quantencomputer". In: Wikipedia, Die freie Enzyklopädie. Bearbeitungsstand: 20. April 2011.
URL: http://de.wikipedia.org/w/index.php?title=Quantencomputer&oldid=87915902

[6] "Qubit". In: Wikipedia, Die freie Enzyklopädie. Bearbeitungsstand: 25. Februar 2011, 22:06 UTC. URL: http://de.wikipedia.org/w/index.php?title=Qubit&oldid=85767212

[7] "Experimente und Realisierungen". In: LVD Wiki. Bearbeitungsstand: 26. Juni 2009.
URL: https://wiki.ldv.ei.tum.de/tiki-index.php?page=Experimente+und+Realisierungen

»Wissen schafft Brücken.«