

Quantencomputer

Aleksandar Razpopov

Gliederung

- Motivation
- Qubits
- Glovers Algorithmus
- Realisierung
- Probleme und Erfolge für Quantencomputer

Kleiner Vergleich

- ENIAC(Electronic Numerical Integrator and Computer): erster Universalrechner zur Berechnung von ballistischen Bahnen
 - Er kann: Addition, Subtraktion, multiplizieren und Quadratwurzel ziehen.
 - Addition: 0,2 ms
 - Multiplikation: 2,8ms
 - Division: 24ms
 - Radizieren: 300ms
- i7 Prozessor: Radizieren : 10^{-7} s

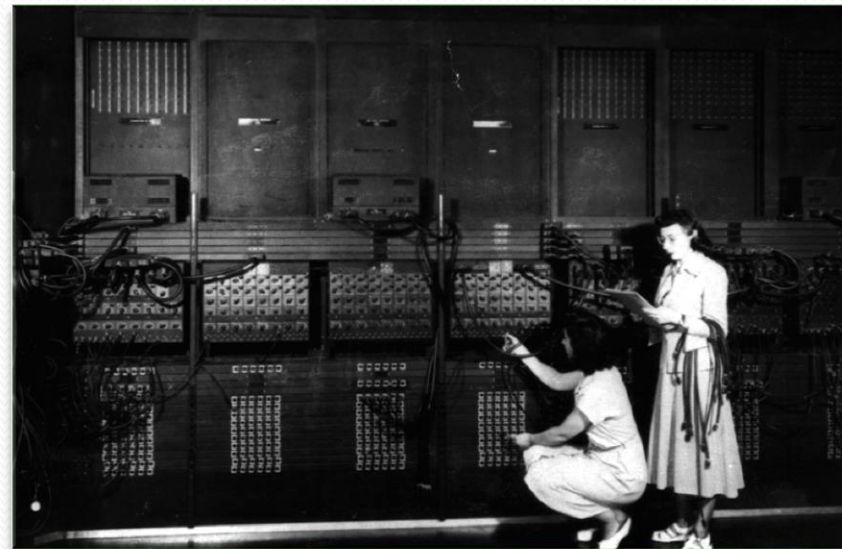


Bild: ENIAC [1]

Probleme für Computer

- Faktorisieren von Zahlen, Aufwand wächst exponentiell
- Suchprobleme: z.B. gegeben ist eine Liste, man sucht einen Eintrag mit bestimmte Eigenschaften, Aufwand in der Ordnung $O(N)$
- numerisches Problem der Form:

$$\hat{A} \times \vec{x} = \vec{b}$$

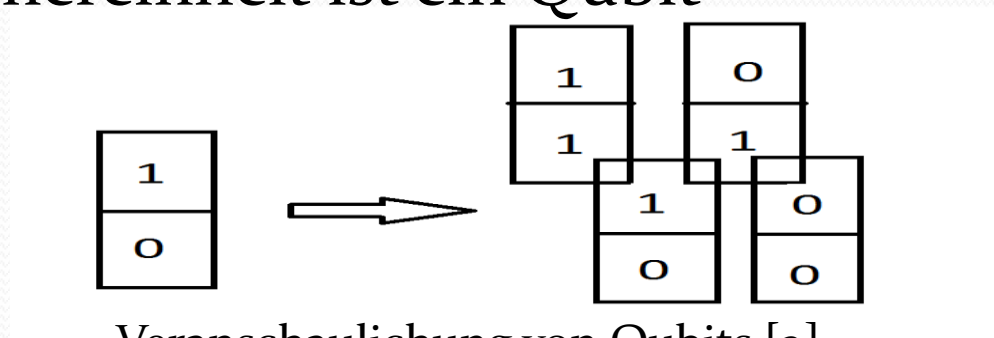
Aufwand in Ordnung $O(N^3)$

Idee:Qubits

- Klassische Computer arbeiten mit „0“ und „1“.
- Werden in Bits gespeichert
- Quantencomputer müssen auch mit „0“ und „1“
- Unterschied zur klassischen Mechanik:
Superpositionsprinzip:

$$|\psi\rangle = a|1\rangle + b|0\rangle$$

- Die Speichereinheit ist ein Qubit



Kriterien für Qubits: (DiVincenzo)

- System muss bestimmbar und skalierbar sein
- In reinen Zustand präparieren
- Das Qubitsystem muss lange Dekohärenzzeit besitzen
- System muss die Implementierung von universalen Quantengattern erlauben
- Wichtige Gatter: NOT, CNOT und Hadamard
- Möglichkeit alle Qubits zu messen

Grovers Algorithmus

- Suchalgorithmus: gegeben ist $F(x)$, suche t mit folgender Eigenschaft $F(t) = -1$
- Benötigt 3 Subroutines (Operatoren), um den Algorithmus durchzuführen
- Aufwand geht mit $O(\sqrt{N})$ (klassisch $O(N)$)
- Datenbanken lassen sich damit viel schneller durchsuchen

Anforderungen für Quantencomputer

- „Closed Box“ für die Qubits
- Qubits sollen leicht zu manipulieren sein, aber abgeschirmt von der restlichen Welt
- Quantencomputer soll skalierbar sein
- Universelle Logik
- Entropie bestimmbar



"Closed Box"

Allgemeines Prinzip [3]

Realisierung

- Anzahl von Operationen pro Kohärenzzeit

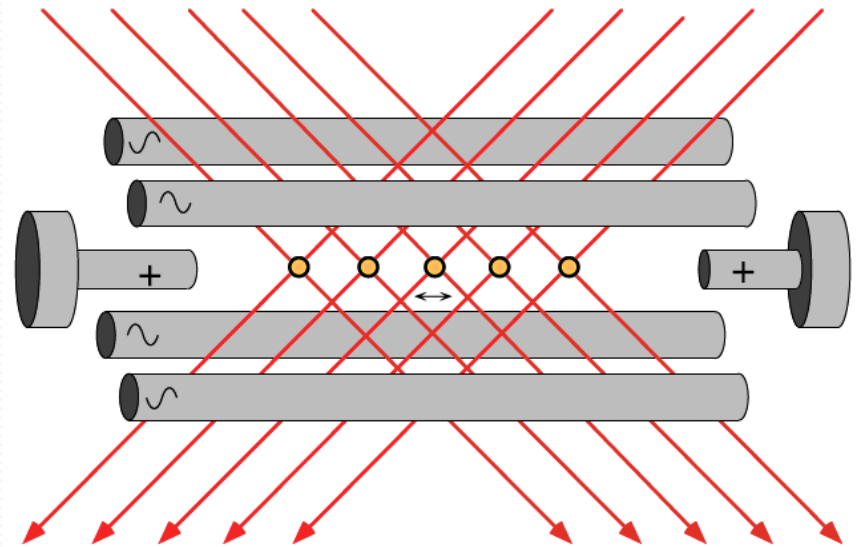
$$n_{op} = \lambda^{-1} = \frac{\tau_Q}{\tau_{op}}$$

System	τ_Q	τ_{op}	$n_{op} = \lambda^{-1}$
Nuclear spin	$10^{-2} - 10^8$	$10^{-3} - 10^{-6}$	$10^5 - 10^{14}$
Electron spin	10^{-3}	10^{-7}	10^4
Ion trap (In^+)	10^{-1}	10^{-14}	10^{13}
Electron – Au	10^{-8}	10^{-14}	10^6
Electron – GaAs	10^{-10}	10^{-13}	10^3
Quantum dot	10^{-6}	10^{-9}	10^3
Optical cavity	10^{-5}	10^{-14}	10^9
Microwave cavity	10^0	10^{-4}	10^4

Kohärenzzeiten für verschiedene Systeme [4]

Ionen Falle

- Qubits sind Ionen
- Ionen in Pauli-Falle stabilisiert
- $|0\rangle$ und $|1\rangle$ entsprechen Anregungen durch Laser
- Genauigkeit bis 80%
- Messung: Fluoreszenz
- Problem: Große Anzahl, Kühlungsprobleme



Schematische Darstellung Ionen-Falle [5]

Kernspinresonanz

- Flüssigkeit von „Designer-Moleküle“
- Zustände werden durch „spin up/down“ repräsentiert
- Quantengatter durch Magnetfeld realisierbar
- Vorteil: viele Qubits $\sim 10^{20}$
- Nachteil: Reinen Zustand, Messung von einzelnen Qubits, (Kosten)

Probleme für Quantencomputer

- Fehler steigen exponentiell
 - Messungen sind schwer
 - Keine Kopien möglich
 - Kohärenzzeit
 - Sehr empfindlich
- Im Moment ist es einfacher, einen klassischen Computer schneller zu machen

Anwendungen

- Kein Ersatz für klassische Rechner, ergänzend
- Lösen von numerischen Problemen
- Quantensimulationen: brauchen $k \cdot N$ Qubits
- Schnelles Durchsuchen von Datenbanken
- Sicherheit
- Echten Zufall generieren
- ...

Erfolge bis jetzt

- 2001 Faktorisierung von 15 von IBM durch ein System von 7 Qubits (Kernspinresonanz)
- 2003 Deutsch-Jozsa-Algorithmus realisiert
- 2005 Rainer Blatt an Innsbruck 8 Qubits Register
- 2011 Innsbruck 14 Qubits gefangen
- 2013 sollen NASA und Google Computer mit 512 Qubits gekauft haben ***
- 2015 stellen NASA und Google Quantencomputer mit 1000 Qubits vor***

Quellen

- [1] <http://www.columbia.edu/cu/computinghistory/eniac.html>
- <https://de.wikipedia.org/wiki/ENIAC>
- [2],[3] Ich
- [4] Dominik Bauernfeind, Universität Regensburg
- QUANTUM COMPUTATION von Dorit Aharonov
- [5] Quantum computing von Andrew Steane
- Quantum computers von T. D. Ladd, F. Jelezko, R. Laflamme, Y. Nakamura, C. Monroe & J. L. O'Brien¹⁰