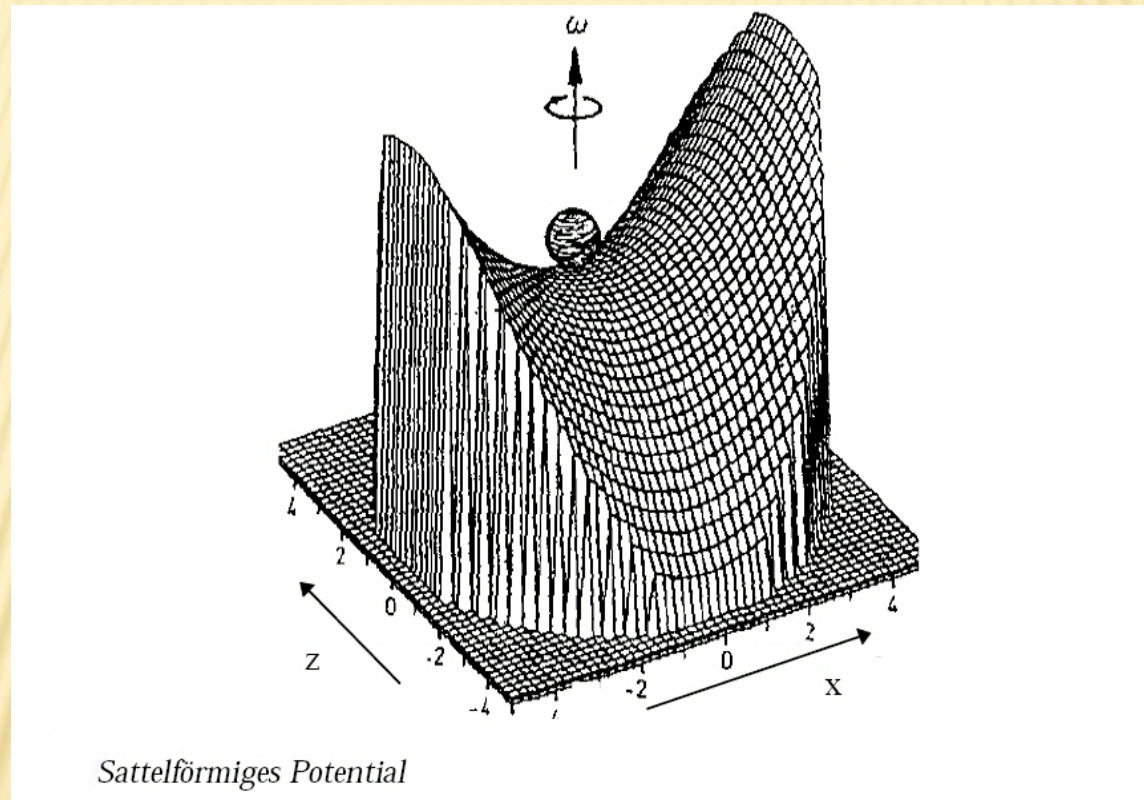


Quantencomputer



Tobias Tyborski HU Berlin

Quantencomputer

Vortragsübersicht

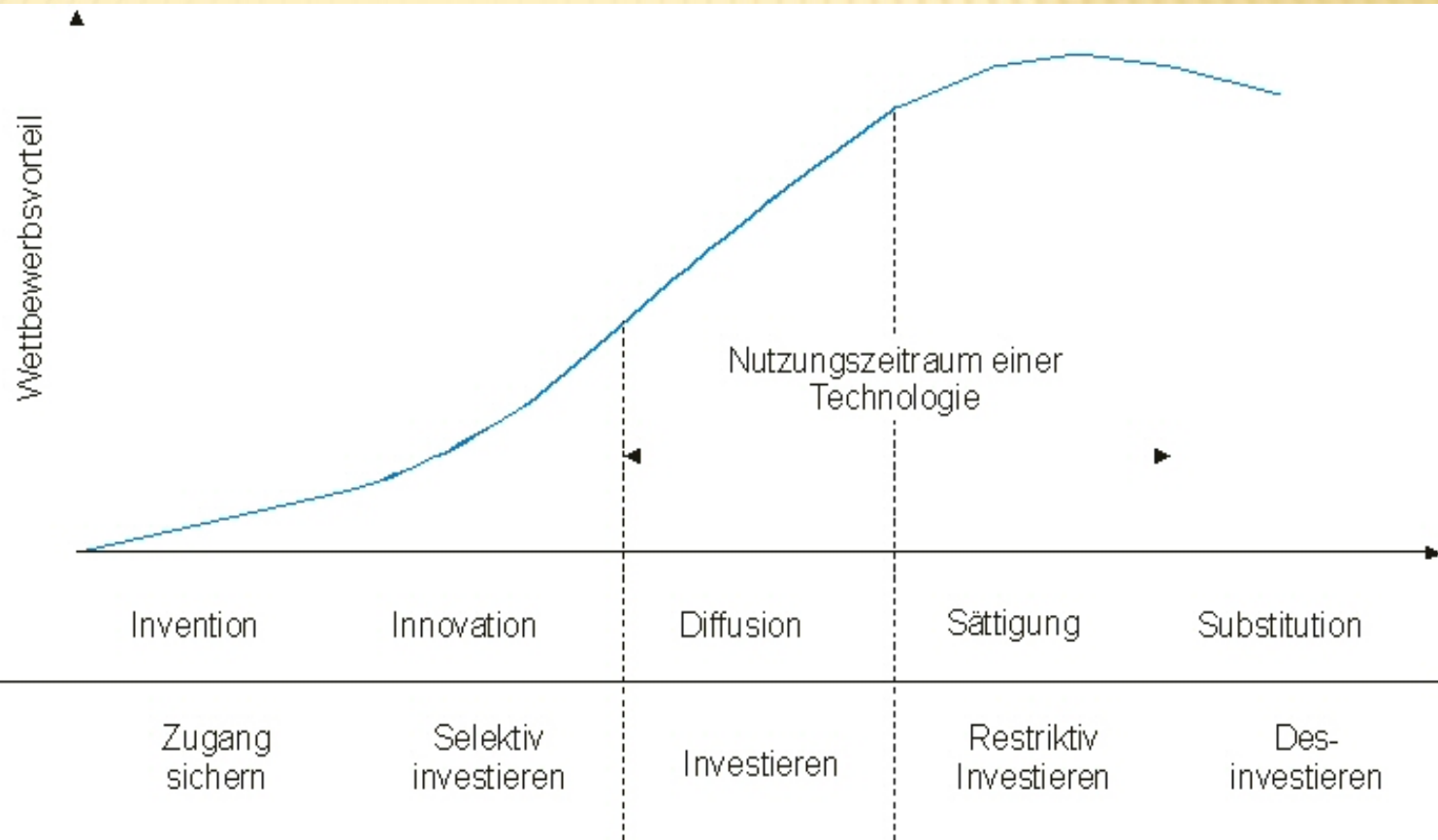
1. allgemeine Informationen
 - Stand der Technik, Definitionen
2. Wie rechnet der QC?
 - single-qubit-gate, two-qubit-gate
3. physikalische Realisierungen
4. Ionenfalle
5. Abschließendes
 - Probleme, DiVincenzo Commandments

1. allgemeine Informationen

- ✘ Darstellung und Verarbeitung von Informationen nach Gesetzen der QM
- ✘ erste Überlegungen/theoretische Ansätze in den 80er Jahren, 1982 Veröffentlichung Feynman über Modelle von QC
- ✘ QC interdisziplinär: Physik, Mathematik, Informatik

1. allgemeine Informationen

✘ Technologielebenszyklus



Lebenszyklus einer Technologie (Daimler-Benz AG, 1996 In: Weule, H. (2002), S. 32)

1. allgemeine Informationen

✗ Motivation:

- Darstellung und Simulation von QS
- in 20 Jahren Strukturen auf Halbleitern zu klein
- Synergieeffekt anwenden/lernen QM

1. allgemeine Informationen

✘ Vorteile:

- QC kann alles rechnen wie herkömmlicher Computer und mehr
 - abhörsichere Nachrichtenübertragung
 - Teleportation von Information
 - Erzeugung echter Zufallszahlen
 - Knacken von heutigen Verschlüsselungen

1. allgemeine Informationen

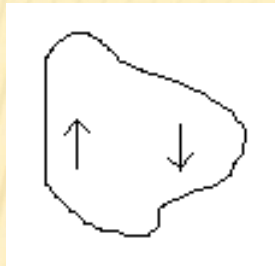
✘ spezielle Anwendungen:

- Shor's Algorithmus (Primfaktorzerlegung)
- Grover's Algorithmus (schnellere Datenbankdurchsuchung)
- schnellere Berechnung von Jones Polynomen (Knotentheorie)
 - Polymerphysik, Biochemie (Proteinvergleich), Feynmanpfade

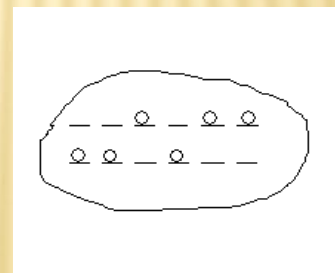
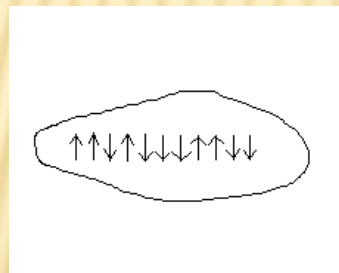
1. allgemeine Informationen

× Definitionen:

- Qubit: beliebig manipulierbares Zweizustands-Quantensystem



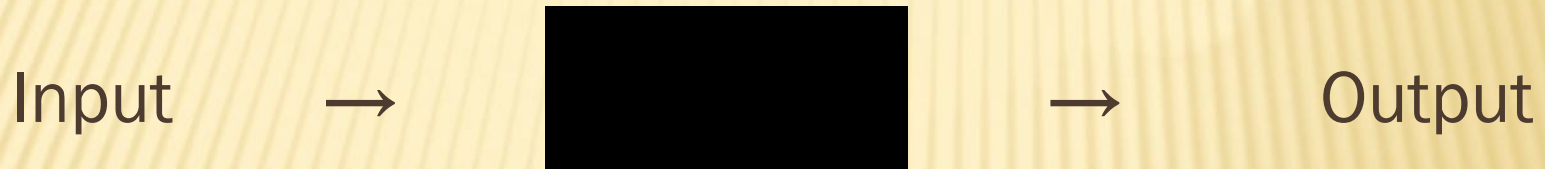
- Quantenregister: Zusammenfassung mehrerer Qubits



- gate(Gatter): Elementaroperation, die auf Qubit oder Register wirkt

2. Wie rechnet der QC?

- ✘ zunächst: QC ist Black Box



- ✘ genauer: geeignetes QS wird nach Bedarf manipuliert (Input) und ausgelesen (Output)

2. Wie rechnet der QC?

- ✗ einfachster Fall, QS ist 1-Qubit-System:
 - Qubit als ZZS Element des zweidimensionalen Hilbertraums

$$|\Psi\rangle = \alpha |0\rangle + \beta |1\rangle \quad \alpha, \beta \in \mathbb{C}, |\alpha|^2 + |\beta|^2 = 1$$

- Qubit kann sich in Superposition befinden!

2. Wie rechnet der QC?

- Manipulation am Qubit dargestellt durch unitäre Matrizen (gates)

$$|\Psi\rangle \rightarrow U|\Psi\rangle$$

- wirkt U auf ein Qubit, wird U auch single qubit gate genannt

2. Wie rechnet der QC?

- Beispiele für single qubit gates:

→ Kippen des Zustands

$$U|\Psi\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} |\Psi\rangle$$

→ phase shift gate (Änderung der Phase)

$$\Phi|\Psi\rangle = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\varphi} \end{pmatrix} |\Psi\rangle$$

(wird verwendet um Interferenz zu erreichen)

2. Wie rechnet der QC?

→ Hadamard gate

$$H|\Psi\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} |\Psi\rangle \quad (\text{Matrixschreibweise})$$

$$H = \frac{|0\rangle_+ |1\rangle}{\sqrt{2}} \langle 0|_+ + \frac{|0\rangle_- |1\rangle}{\sqrt{2}} \langle 1| \quad (\text{Dirac - Schreibweise})$$

2. Wie rechnet der QC?

→ Hadamard gate (Beispielrechnung)

$$H|0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \langle 0|0\rangle + \frac{|0\rangle - |1\rangle}{\sqrt{2}} \langle 1|0\rangle = \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle)$$

=> überführt einen Basiszustand in Superposition der Basiszustände mit gleicher Wichtung

=> dies kann ein herkömmlicher Computer nicht!

=> Hadamard gate und phase shift gate bilden universelles gate

2. Wie rechnet der QC?

✗ 2 – Qubit – System :

- 2 – Qubit – System wird als „Produkt“ der einzelnen Qubits dargestellt z.B.:

$$|\Psi \rangle = |1\rangle|0\rangle$$

- allgemeiner: Qubit 1 und Qubit 2 überlagern in Superposition \rightarrow Tensorprodukt

$$|\Psi \rangle = \lambda (|0\rangle + |1\rangle) \otimes \kappa (|0\rangle + |1\rangle) = \alpha |0\rangle|0\rangle + \beta |0\rangle|1\rangle + \gamma |1\rangle|0\rangle + \delta |1\rangle|1\rangle$$

($\alpha, \beta, \gamma, \delta, \lambda, \kappa$ Normierungskonstanten)

2. Wie rechnet der QC?

- Beispiel für einen Zustand:

$$|\Psi\rangle = |0\rangle|1\rangle + |1\rangle|1\rangle = (|0\rangle + |1\rangle)|1\rangle$$

- verschränkter Zustand:

$$|\Psi\rangle = |0\rangle|0\rangle + |1\rangle|1\rangle$$

→ Zustand lässt sich nicht als Produkt zweier Zustände schreiben

→ Zustände nicht unabhängig voneinander

2. Wie rechnet der QC?

- ✗ Manipulationen am 2 - Qubit - System :
→ controlled-not gate (c-not gate)

$$cn|m\rangle|n\rangle = |m\rangle|n+m\rangle \quad (\text{schematisch})$$

($m, n \in 0, 1$ und "+" addition modula 2)

$$cn = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \quad (\text{Matrixdarstellung})$$

2. Wie rechnet der QC?

- Beispiele:

$$cn|0\rangle|1\rangle = |0\rangle|1\rangle$$

$$cn|1\rangle|1\rangle = |1\rangle|0\rangle$$

$$cn(|0\rangle|1\rangle + |1\rangle|1\rangle) = |0\rangle|1\rangle + |1\rangle|0\rangle$$

- Änderung am 2. Qubit abhängig vom Zustand des ersten
- aus dem Zustand des ersten Quantenbits kann auf das zweite geschlossen werden, ohne es direkt messen zu müssen und damit seinen Quantenzustand zu stören
- jede Rechenoperation durchführbar als Folge von single qubit gates und c-not gates

2. Wie rechnet der QC?

✗ paralleles Rechnen :

→ herkömmliche Darstellung von Informationen mit Bits

- Bit im Zustand 0 oder 1
- n Bits können 2^n verschiedene, klar definierte Zustände annehmen

→ Beispiel: 3 – Bit – System

- 8 verschiedene Zustände
- 011 = 3, 111 = 7

2. Wie rechnet der QC?

- quantenmechanische Darstellung von Informationen mit Qubits:
 - Qubit im Superpositionszustand von 0 und 1
 - n Qubits im Superpositionszustand der 2^n Möglichkeiten
- Beispiel: 3 – Qubit – System
 - 8 Zustände gleichzeitig
 - immernoch: 011 = 3 , 111 = 7

2. Wie rechnet der QC?

→ Beispiel: 3 – Qubit – System

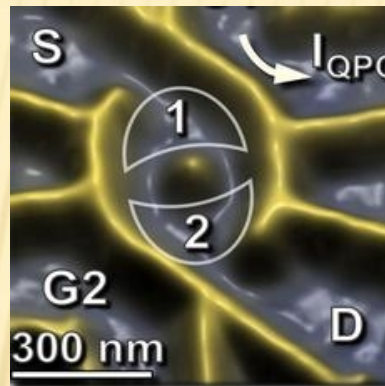
$$\begin{aligned} |\Psi\rangle &= |000\rangle + |001\rangle + |010\rangle + |100\rangle + |011\rangle + |101\rangle + |110\rangle + |111\rangle \\ &= |0\rangle + |1\rangle + |2\rangle + |3\rangle + |4\rangle + |5\rangle + |6\rangle + |7\rangle = \sum_{x=0}^7 |x\rangle \end{aligned}$$

=> jeder Zustand ist in $|\Psi\rangle$ enthalten

=> alle Informationen gleichzeitig
gespeichert

3. Physikalische Realisierungen

- ✗ Ionen in Ionenfallen
- ✗ Elektronen in Quantenpunkten



(Quelle: Gustavsson S et al. (2008), Nano Letters Quantenpunkte)

- ✗ Kernspinresonanz
- ✗ Photonenzustände
- ✗ Cooper Paar auf supraleitender Insel

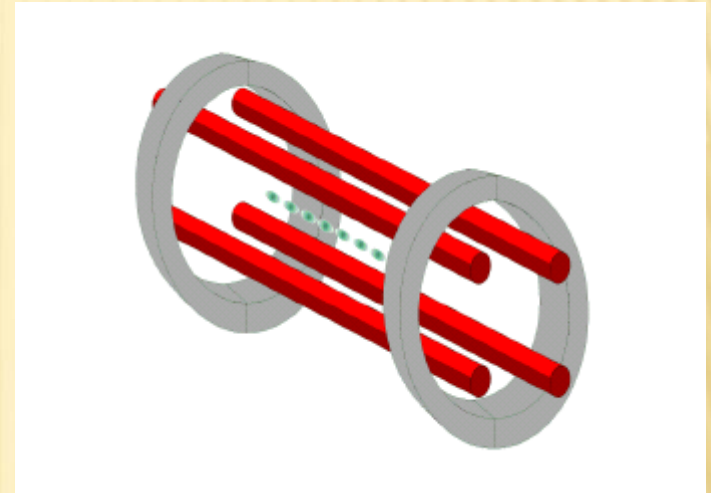
4. Ionenfalle

→ Paul-Falle

- an gegenüberliegenden Metallstäben liegt zeitabhängiges

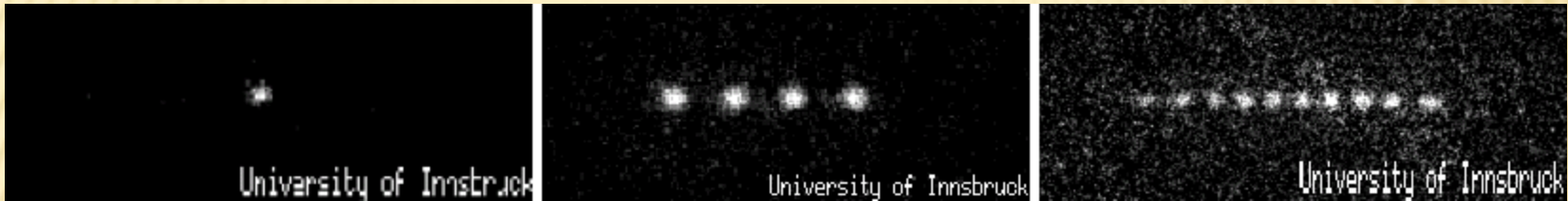
Radiofrequenzpotential => Ionen auf Kette

- zirkulare Elektroden an den Enden
- Coulomb-Abstoßung hält Ionen auf Abstand



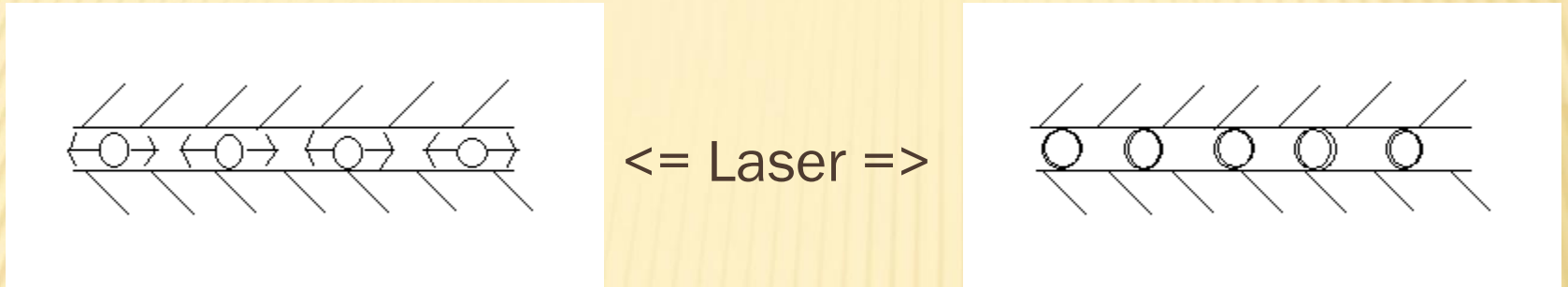
(Ionenfallen als Quantencomputer, Vortrag Markus Fleger)

4. Ionenfalle



- Gleichgewichtslage der Ionen aus Fallenpotential (Einführungsbild)
- Energieniveaus sind metastabile Ionenzustände mit Lebensdauer etwa 1s
- Schwingungen der Ionenkette entsprechen kleinen Auslenkungen entlang der Potentialachse, phononische WW dienen als Datenbus für Verschränkung der Ionenzustände

4. Ionenfalle



-zu Beginn einer Rechnung werden Ionen auf
gewünschten Anfangswert gebracht

z.B.: $|0\rangle|0\rangle\dots|0\rangle$

-Beenden der Rechnung erfordert auslesen =>

Methode der Quantensprünge

→ Bestrahlung der Ionen mit bestimmten Laserlicht =>
Fluoreszenz der Ionen im Zustand $|1\rangle$

keine Fluoreszenz der Ionen im Zustand $|0\rangle$

4. Ionenfalle

- Manipulation am Qubit durch rotverschmierten Laserpuls => Qubitzustand wechselt: $|1\rangle \Rightarrow |0\rangle$
 - Ionenkette wird durch Phononenabgabe in Schwingung versetzt
 - ein zweites Qubit kann so den Zustand ändern $|0\rangle \Rightarrow |1\rangle$
 - wird abschließend der Anfangszustand vom ersten Qubit wieder hergestellt, ist dies eine Realisierung vom c-not gate

4. Ionenfalle

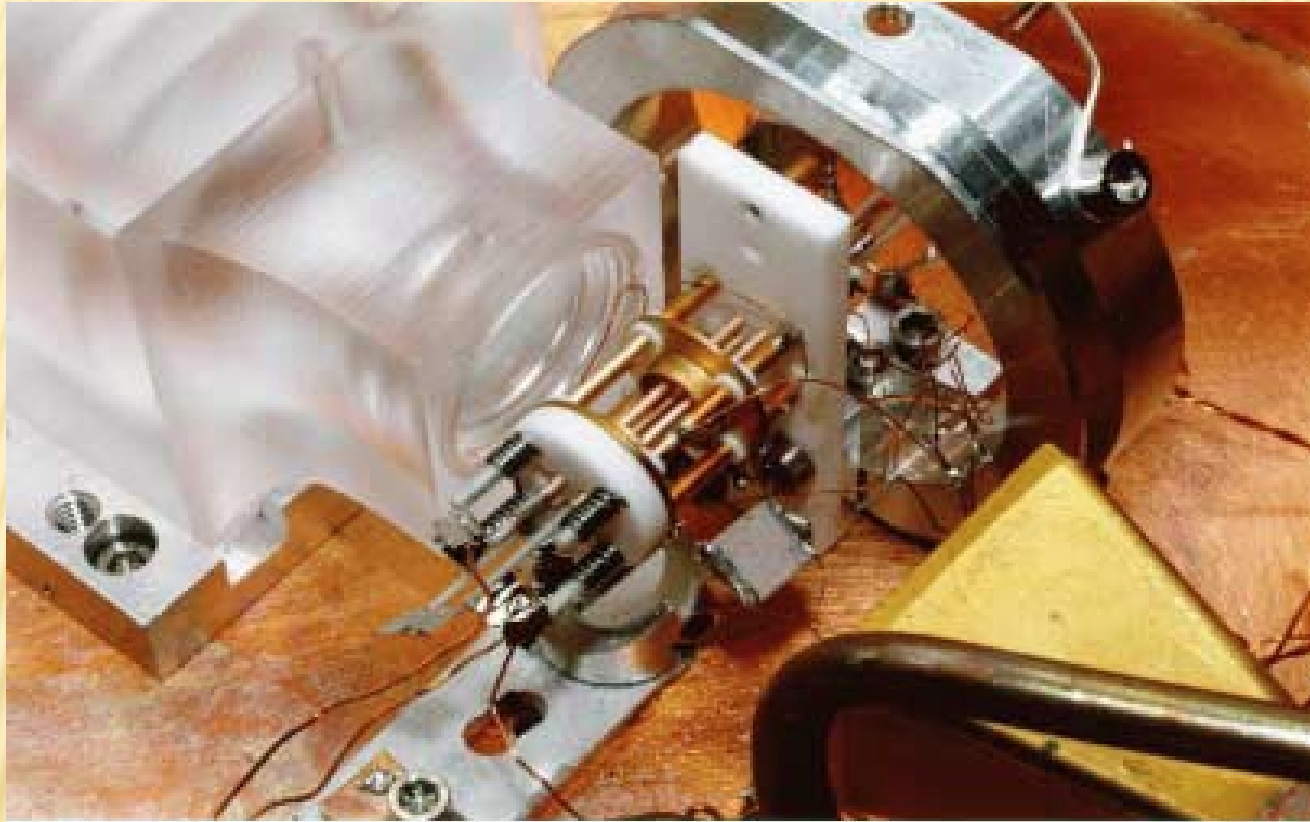
-Schwierigkeiten:

- Manipulierbarkeit von Ionenpaaren, speziell bei großen Ketten
- Laserkühlung in den Grundzustand experimentell aufwendig

-Vorteil:

- sehr gut abgestimmte Qubits

4. Ionenfalle



(Quelle unbekannt)

5. Abschließendes

DiVincenzo Commandments

- ✗ wohldefinierte, skalierbare Qubits
- ✗ Qubits müssen sich in wohldefiniertem Anfangszustand initialisieren lassen
- ✗ ein universeller Satz an Qubit-Manipulationen (gates) muss kohärent durchgeführt werden können
- ✗ Phasenkohärenzzeit groß für viele Manipulationen
- ✗ Qubits müssen verlässlich ausgelesen werden können

5. Abschließendes

✘ Probleme:

- äußere Einflüsse können QS manipulieren

 - => Fehlerkorrektur notwendig

 - (wie bei herkömmlicher

 - Computertechnik, mathematisch

 - bewiesen, dass es möglich ist)

 - => Dekohärenz (großes Problem)

5. Abschließendes

✘ Quellen

- Quantum Computing verstehen. Grundlagen - Anwendungen - Perspektiven von Matthias Homeister, Vieweg-Verlag
- file:///D:/vortragquantencomputer/Quantencomputer2.htm von Franz Embacher
- <http://www3.imperial.ac.uk/quantuminformation>
- <http://heart-c704.uibk.ac.at/>
- Quantum computations with cold trapped ions, Cirac, J.I. & Zoller, P., Phys. Rev. Lett. 74, 4091-4094 (1995)

5. Abschließendes

Danke für die Aufmerksamkeit und viel
Spaß bei der Diskussion!