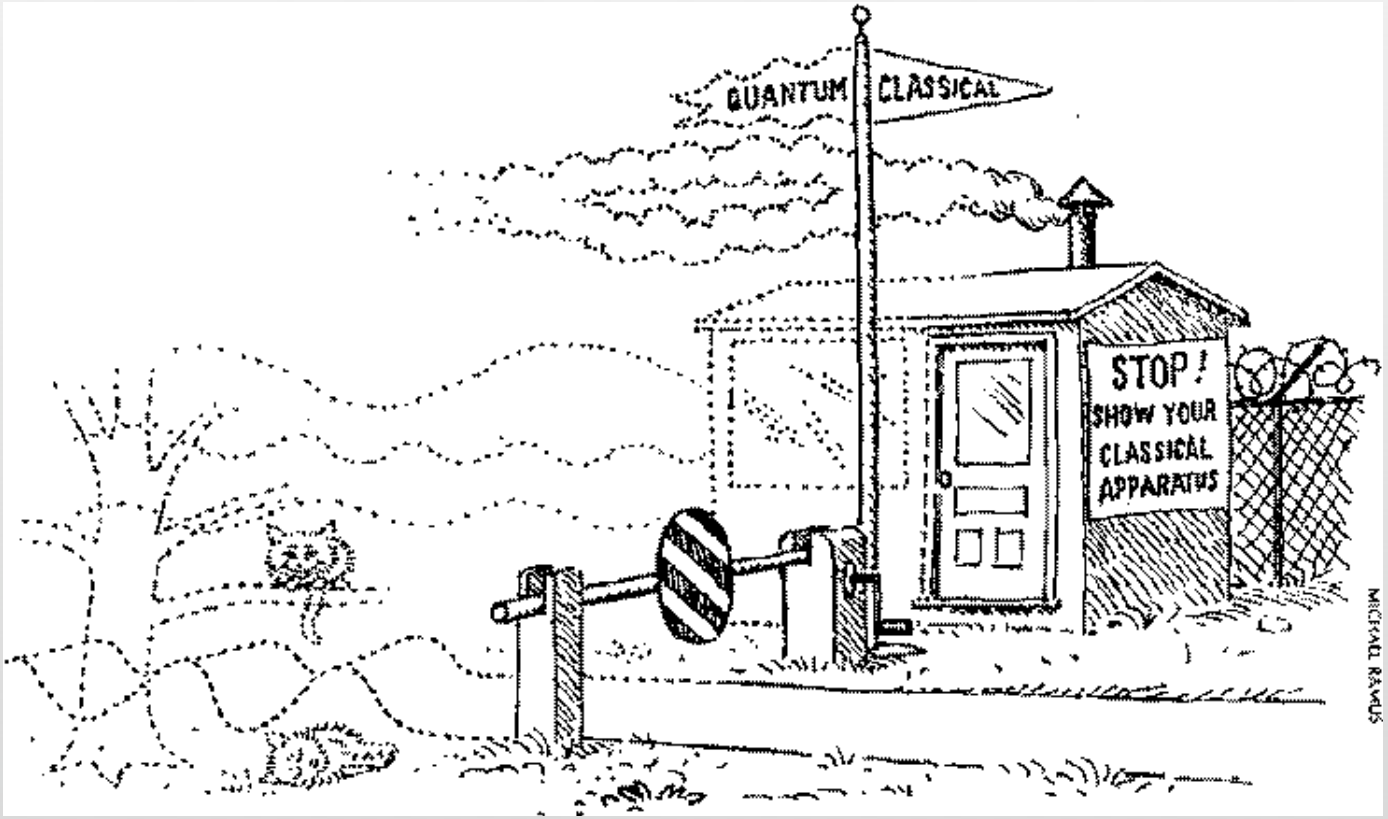
Quanten-Computing

Prof. H. Müller-Krumbhaar, Dr. E. Koch
Institut für Festkörperforschung, FZ Jülich



Information is Physical

R. Landauer

Information hängt von physikalischer Realisierung ab:

Relativität: Übertragungsgeschwindigkeit < c
Statistische Mechanik: Löschen eines Bits kostet Energie > kT ln2

DRAM: Bit durch Ladung eines Kondensators dargestellt:

b = 1 – Kondensator aufgeladen

b = 0 – Kondensator entladen

Alternative: Darstellung durch Spin-½:

$$|b\rangle = \alpha|0\rangle + \beta|1\rangle$$

Superposition klassischer(!) Basiszustände

Quanten Information

Qbits können nicht kopiert werden
(No-Cloning Theorem)

Nachteil:
Information eines Qbit nur teilweise zugänglich
(Unschärfe-Relation)

Vorteil:
Abhören von Quanteninformation ist nachweisbar
⇒ Quanten Kryptographie

No-Cloning Theorem

Wooters&Zurek *Nature 299*, 802 (1982)

Ein *unbekannter* Quantenzustand kann nicht kopiert werden

Beweis durch Widerspruch

sei U ein unitärer Cloning Operator: $U|\Psi\rangle|s\rangle = |\Psi\rangle|\Psi\rangle \quad \forall\,|\Psi\rangle$

$$\text{dann} \quad \langle s|\langle\Psi|U^\dagger \cdot U|\Phi\rangle|s\rangle \overset{\text{unitär}}{=} \underbrace{\langle s|s\rangle}_{=1}\langle\Psi|\Phi\rangle$$

$$\overset{\text{def}}{=} \langle\Psi|\langle\Psi| \cdot |\Phi\rangle|\Phi\rangle = \langle\Psi|\Phi\rangle^2$$

also $\langle\Psi|\Phi\rangle^2 \overset{!}{=} \langle\Psi|\Phi\rangle$; nur möglich, wenn $\langle\Psi|\Phi\rangle = 0$ oder 1

$\Rightarrow$ nur bekannte, orthogonale Basiszustände kopierbar

(reversibles kopieren klassischer Bits)

Klassische (Boolesche) Logik

AND Gatter

a	b	a b
0	0	0
0	1	0
1	0	0
1	1	1

XOR Gatter

a	b	a ⊕ b
0	0	0
0	1	1
1	0	1
1	1	0

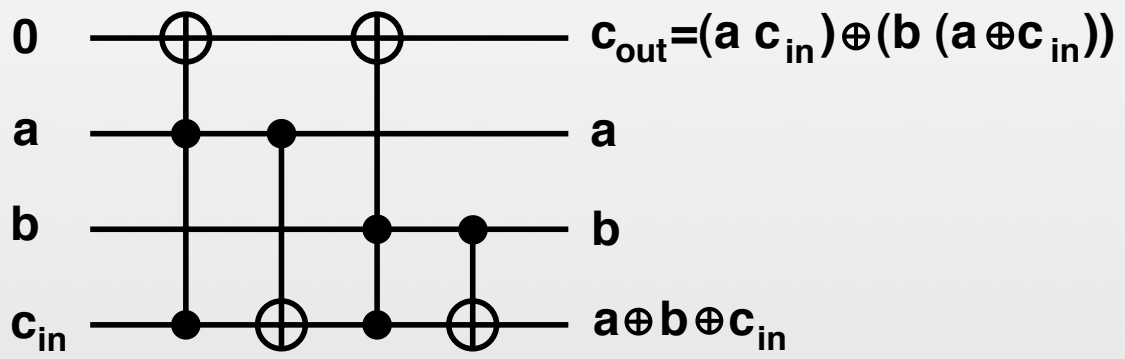
nicht reversibel!
QM: unitäre Operationen...

Reversible Logik

Ch. Bennett

z.B. controlled NOT und Toffoli Gatter

Beispiel:
Voll-Addierer



reversible Gatter definieren Operationen auf Basiszust.
natürliche Erweiterung auf unitäre Operationen

Quanten-Gatter ohne klassisches Analogon:
z.B. Hadamard Gatter (erzeugt Superpositionen)

$$U_H|0\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right)$$
$$U_H|1\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right)$$

Quanten Parallelität

$$U_h|0\rangle\, U_H|0\rangle\, \ldots\, U_H|0\rangle = U_H^{\otimes n}\,|00\ldots0\rangle = \sum_x |\mathbf{x}\rangle$$

Superposition aller 2^n Basiszustände

klassische Funktion *f(x)* durch unitären Operator realisiert:

$$U_f|\mathbf{x}\rangle|\mathbf{y}\rangle := |\mathbf{x}\rangle|f(\mathbf{x}) \oplus \mathbf{y}\rangle$$

also $U_f\, U_H^{\otimes n}|\mathbf{0}\rangle|\mathbf{0}\rangle = U_f \sum_x |\mathbf{x}\rangle|\mathbf{0}\rangle = \sum_x \underbrace{|\mathbf{x}\rangle|f(\mathbf{x})\rangle}$

x und $f(x)$ verschränkt!

gleichzeitige Berechnung von 2^n Funktionswerten!

Problem: nur ein (zufälliges!) *f(x)* kann gemessen werden

Die Kunst des Quanten Computing:

relevante Information mittels Interferenz extrahieren

Dimension des Hilbert Raums

n Qbit – Hilbert-Raum: C^{2^n}

n	2^n	
10	1 024	1 kb (kilo)
20	1 048 576	1 Mb (Mega)
30	1073 741 824	1 Gb (Giga)
40	1 099 511 627 776	1 Tb (Tera)
50	1 125 899 906 842 624	1 Pb (Peta)
60	1 152 921 504 606 846 976	1 Eb (Exa)
70	1 180 591 620 717 411 303 424	1 Zb (Zetta)
80	1 208 925 819 614 629 174 706 176	1 Yb (Yotta)

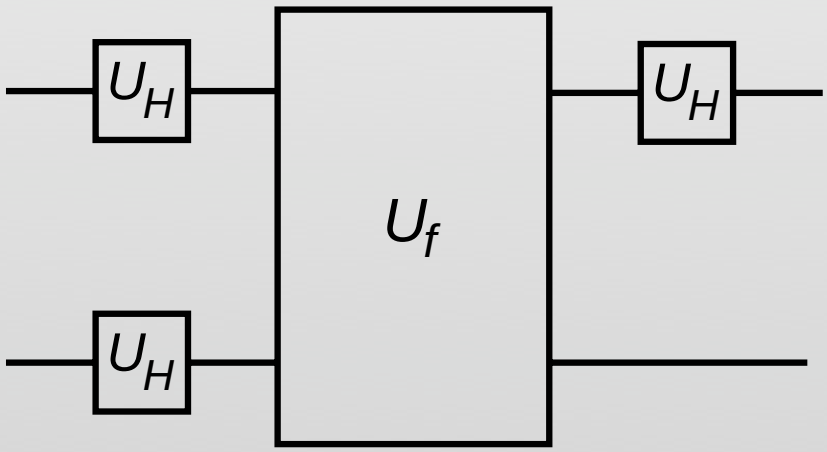
Deutsch Algorithmus

Proc. Roy. Soc. London, Ser. A *400*, 97 (1985)

gegeben $f : \{0,1\} \rightarrow \{0,1\}$ $f(0)=f(1)$ oder nicht?

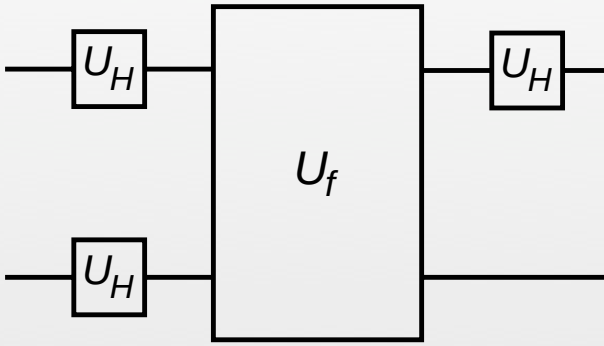
klassischer Computer: zweimal f aufrufen

Quanten Computer: ein Aufruf von f reicht!



Deutsch Algorithmus

Proc. Roy. Soc. London, Ser. A *400*, 97 (1985)



Superposition herstellen

$$U_H|0\rangle\, U_H|1\rangle = \tfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\ \tfrac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

$$= \tfrac{1}{2}\Big(|0\rangle|0\rangle \quad -|0\rangle|1\rangle \quad +|1\rangle|0\rangle \quad -|1\rangle|1\rangle \Big)$$

f aufrufen (beachte: $0 \oplus a = a$ und $1 \oplus a = \overline{a}$)

$$\xrightarrow{U_f} \tfrac{1}{2}\Big(|0\rangle|0\oplus f(0)\rangle - |0\rangle|1\oplus f(0)\rangle + |1\rangle|0\oplus f(1)\rangle - |1\rangle|1\oplus f(1)\rangle\Big)$$

$$= \tfrac{1}{2}\Big(|0\rangle|f(0)\rangle \quad -|0\rangle|\overline{f(0)}\rangle \quad +|1\rangle|f(1)\rangle \quad -|1\rangle|\overline{f(1)}\rangle \Big)$$

$$= \tfrac{1}{2}\Big(\ |0\rangle\ [|f(0)\rangle - |\overline{f(0)}\rangle] \quad +\ |1\rangle\ [|f(1)\rangle - |\overline{f(1)}\rangle] \Big)$$

Interferenz

$$= \begin{cases} \tfrac{1}{2}(|0\rangle + |1\rangle)\ [|f(0)\rangle - |\overline{f(0)}\rangle] \xrightarrow{U_H} \tfrac{1}{\sqrt{2}}|0\rangle\ [|f(0)\rangle - |\overline{f(0)}\rangle] & \text{falls } = \\ \tfrac{1}{2}(|0\rangle - |1\rangle)\ [|f(0)\rangle - |\overline{f(0)}\rangle] \xrightarrow{U_H} \tfrac{1}{\sqrt{2}}|1\rangle\ [|f(0)\rangle - |\overline{f(0)}\rangle] & \text{falls } \neq \end{cases}$$

Quanten Computing

Begriff der Berechenbarkeit bleibt unverändert
(Quantensysteme auf klassischen Computern simulierbar)

Komplexität von Algorithmen stark reduziert:
Quanten Computer können wesentlich schneller sein

Problem	klass. Algorithmus	Quanten-Algorithmus
faktorisiere N	number field sieve $O(e^{(\log N)^{1/3} (\log \log N)^{2/3}})$	Shor Algorithmus: $O(\log^3 N)$
Suche in ungeordeter Menge von N Einträgen	brute force: $O(N)$	Grover Algorithmus: $O(\sqrt{N})$

DiVincenzo Kriterien

Fortschr. Physik *48*, 771-783 (2000)

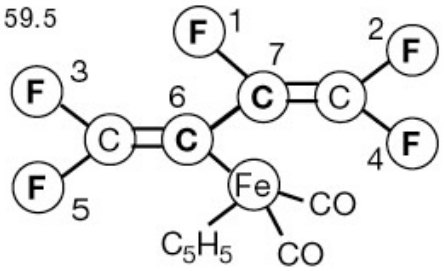
- skalierbares physikalisches System wohldefinierter Qbits
- Möglichkeit, Qbits zu initialisieren
- universeller Satz von Quanten-Gattern
- Dekohärenz-Zeit $\gg$ Gatter-Schaltzeiten
- Möglichkeit, Qbits zu messen
- Möglichkeit, Qbits zu übertragen

Quanten Hardware: NMR

NMR an Flüssigkeiten

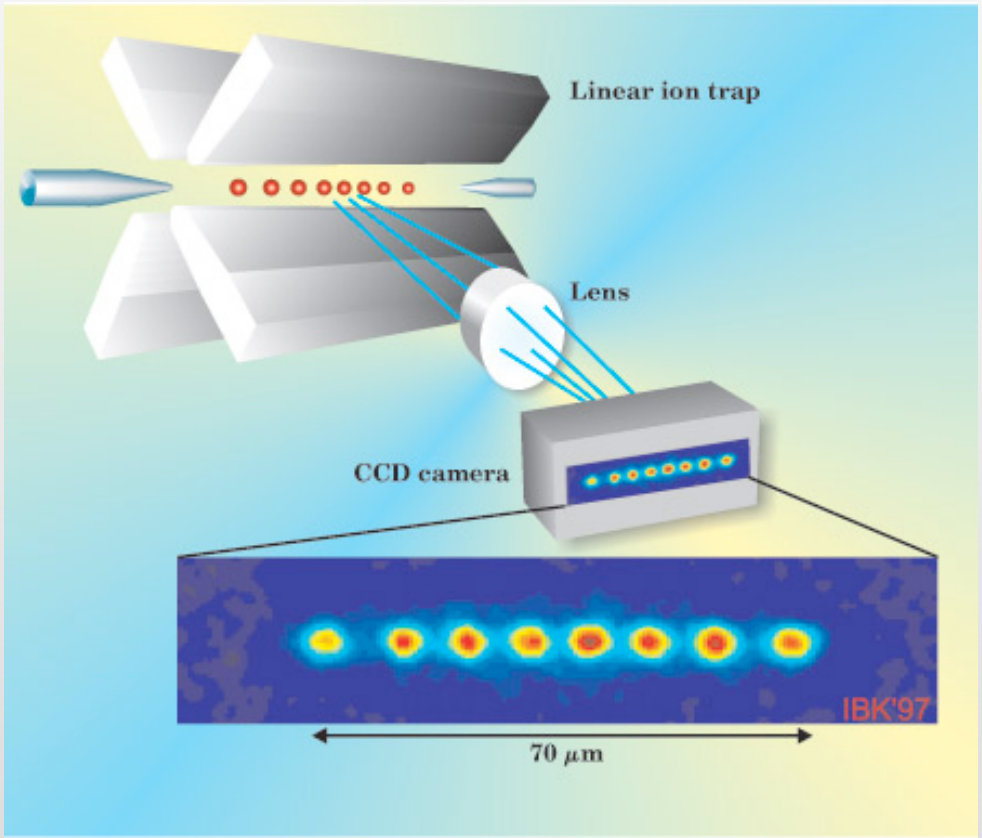
- Kernspins in Molekülen
- 7 Qbits realisiert
- Problem: Skalierung
- Nature *414*, 883 (2001): Shor-Faktorisierung 15=3x5

i	$\omega_i/2\pi$	$T_{1,i}$	$T_{2,i}$	J_{7i}	J_{6i}	J_{5i}	J_{4i}	J_{3i}	J_{2i}
1	–22052.0	5.0	1.3	–221.0	37.7	6.6	–114.3	14.5	25.16
2	489.5	13.7	1.8	18.6	–3.9	2.5	79.9	3.9	
3	25088.3	3.0	2.5	1.0	–13.5	41.6	12.9		
4	–4918.7	10.0	1.7	54.1	–5.7	2.1			
5	15186.6	2.8	1.8	19.4	59.5				
6	–4519.1	45.4	2.0	68.9					
7	4244.3	31.6	2.0						



Quantum Hardware: Ionen-Falle

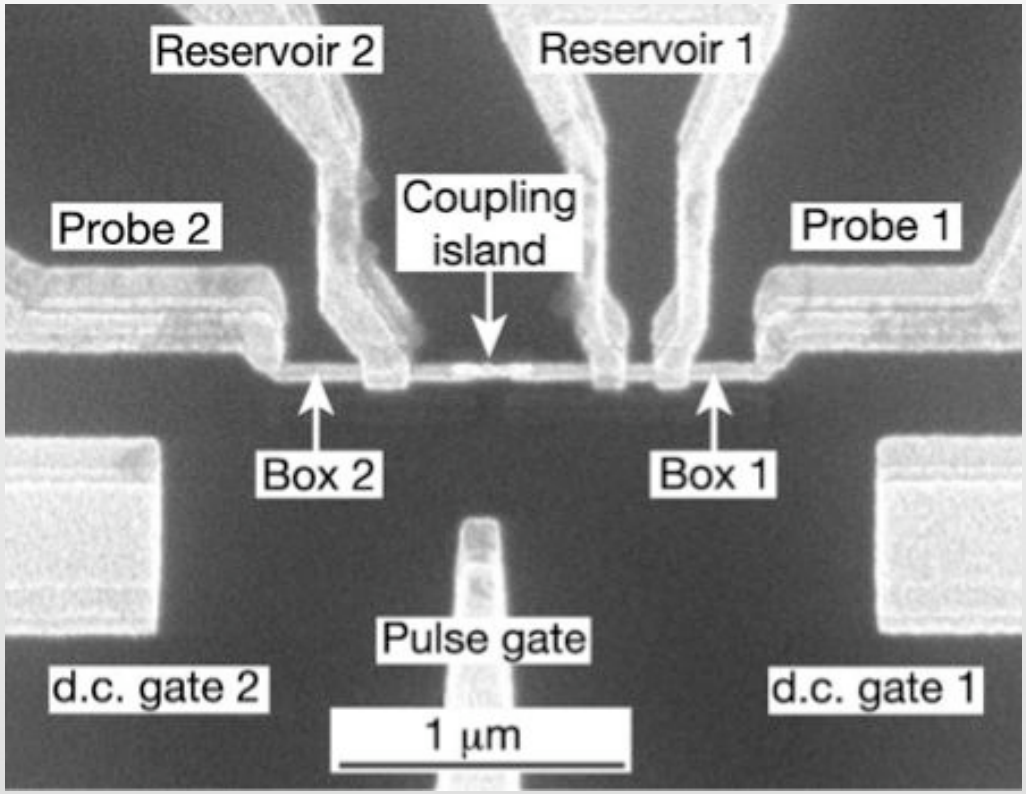
- 1 Qbit Gatter: Laser
- 2 Qbit Gatter:
  Schwingungen (Phononen)
- 2 Qbits realisiert
- Nature *422*, 408 (2003)
  Physics Today, März 2004



Quantum Hardware: Josephson

Josephson Kontakte

- Phase oder Besetzungszahl
- 2 Qbit Operations
  fast realisiert
- Nature *421*, 823 (2003)



Landauer's disclaimer

Nature 400, 720 (1999)

This proposal, like all proposals for quantum computation, relies on speculative technology, does not in its current form take into account all possible sources of noise, unreliability and manufacturing error, and probably will not work.

Siemens Prognose für 2020

http://w3.siemens.de/horizons2020/

Die Quantencomputer bieten quasi unlimitierte Rechenleistung und haben der Anwendung von Computern völlig neue Möglichkeiten erschlossen. Paralleles Rechnen wird zur Selbst-verständlichkeit.

Durch die technische Komplexität und die damit verbundenen Kosten ist der breite Einsatz von Quantencomputern noch nicht möglich.