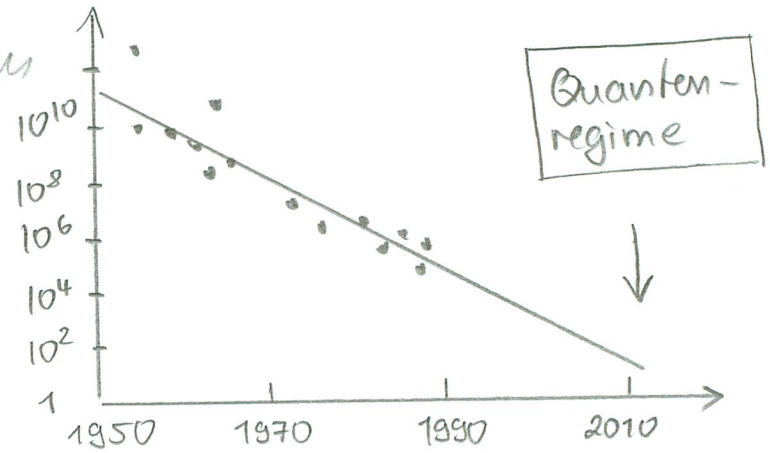
0. Einleitung

0.1. Warum "Quanteninformationsverarbeitung"?

- Moor'sches Gesetz: (Gerald Moore, Mitbegründer von Intel)
  Zahl der Transistoren auf einem Computerchip verdoppelt sich alle 18–24 Monate

Anzahl der Dotierungen (Störstellenatome) pro Bipolartransistor
R.W. Keyes
IBM Research Develop.
32 (1988)



⇒ etwa im Jahre 2015–2020 hat ein Transistor nur noch 1 Dotierungsatom → Quanteneffekte!

logische Operationen wie "und" oder "oder" irreversibel
⇒ Wärmeproduktion ↔ Elementaroperationen möglichst reversibel

> zukünftige Computertechnologie erfordert reversible Elementarprozesse die den Gesetzen der Quantenmechanik genügen

sind Quanteneffekte nur eine technologische Schranke für

zukünftige Informationstechnologie?

- Richard Feynman: 1st conference on the physics of computation (1981)

die Simulation der Dynamik eines allg. Quantensystems auf klassischen Rechnern ist i.A. exponentiell langsamer als die tatsächliche Quantendynamik, d.h. der Zeitaufwand wächst exponentiell mit der "Größe" des Quantensystems

Zur Veranschaulichung betrachten wir ein System aus N Spin 1/2 Teilchen mit Basiszuständen $\{|0\rangle, |1\rangle\}$. Die Dimension des Hilbertraumes ist $d = 2^N$. Sei der Anfangszustand $|\Psi(t_0)\rangle$ ein Produkt

$$(1) \qquad |\Psi(t_0)\rangle = \underbrace{|0\rangle|1\rangle|0\rangle \cdots |0\rangle|1\rangle}_{\text{N binäre Zahlen} \qquad \text{N bit}}$$

$$(2) \qquad |\Psi(t)\rangle = \sum_{i=0}^{2^N-1} \alpha_i(t)\, |i\rangle$$

wobei

$$(3) \qquad |i\rangle \hat{=} \left\{ \begin{array}{l} |10000\ldots0\rangle \\ |11000\ldots0\rangle \\ |10100\ldots0\rangle \\ \vdots \\ |11111\ldots1\rangle \end{array} \right\} \; 2^N \text{ verschiedene Zustände}$$

Die klassische Simulation der Quantendynamik erfordert Speicherung und Verarbeitung von 2^N komplexen Zahlen

mit einer bestimmten Genauigkeit! Für $N=100$ Teilchen ist $2^{100} \sim 10^{30}$!!!

> klassische Computer können Quantenprobleme (insbesondere Vielteilchenprobleme) i.A. nur sehr ineffizient berechnen ☹

Umkehrung: (Feynman) Ein quantenmechanisches Experiment ersetzt eine exponentiell aufwendige klassische Rechnung!

⇒ eine Rechenmaschine die physikalisch ein Quantensystem ist könnte klass. Rechenmaschinen überlegen sein!

0.2. Potentiale der Quanteninformationsverarbeitung

(i) sichere Informationsübertragung (Kryptographie)
- BB84 Protokoll (Bennett, Brasad 1984)
- Deutsch-Ekert Protokoll (Ekert et al 1992)

- nutzt Eigenschaften des quantenmechanischen Meßprozesses aus (Messung verändert i.A. Zustand)
- no-cloning Theorem

$$|\psi\rangle|0\rangle \xrightarrow{\text{i.A.}} \not\rightarrow |\psi\rangle|\psi\rangle$$

(ii) Datensuperkompression ("dense coding")

mit einem sog. quantenbit (qubit) zwei klassische bit übertragbar

(iii) Quantenalgorithmen

- Grovers Suchalgorithmus L. Grover PRL 78, 325 (1997)

Suche in unsortierter Liste (Telephonbuch rückwärts)

- klassisch: $N/2$ Tests nötig
- qm: $\sqrt{N}$ Tests nötig

Bem: $N = 2^{\log N}$ $\quad \sqrt{N} = 2^{\frac{1}{2}\log N}$

beides exponentielle Skalierung mit $\log N \equiv \log_2 N$ = Anzahl der bits die nötig sind um die Zahl N darzustellen

- Shor's Faktorisierungsalgorithmus (1994)

gegeben: $N \in \mathbb{N}$ gesucht: $k \in \mathbb{N}$, $k \neq 1, N$
k teilt N

- naives Verfahren: Durchtesten von $k=1$ bis $k = \sqrt{N}$

im Mittel $\sqrt{N}/2$ Schritte nötig: $\sim 2^{\frac{1}{2}\log N}$

- bestes klass. Primzahlsieb

$\sim \exp\{(\log N)^{1/3} (\log\log N)\}$

- Shor $\quad \mathcal{O}(\text{poly}(\log N))$

Shor's Verfahren macht aus einem NP Problem ein P Problem

NP Problem: Lösung schwierig (= exponentieller Aufwand = kein effizienter Algorithmus)

Verifizierung einfach

Beispiel: $5 \times 7 \Rightarrow \boxed{35}$ $\quad 49 = \boxed{7} \times \boxed{7}$

$17 \times 29 \Rightarrow \boxed{435}$ $\quad 589 = \boxed{}_{19} \times \boxed{}_{31}$

einfach $\qquad$ schwierig

Mit dem Shor Algorithmus können gegenwärtige Kryptosysteme geknackt werden.

0.8. Probleme der Quanteninformationsverarbeitung

- erfordert kontrollierte kohärente Manipulation einer großen Anzahl mikroskopischer Systeme $\Rightarrow$ schwierig!

- Rolf Landauers Dekohärenzargument:
Die Verarbeitung von Quanteninformation erfordert die Kopplung eines Quantensystems an seine Umgebung. Damit handelt man sich aber automatisch ungewollte Wechselwirkungen mit der Umwelt ein = Dekohärenz

Es ist dabei zu beachten, daß (wie wir noch sehen werden) eine "Verstärkung" von Quanteninformation nicht möglich ist. Der Ausweg aus diesem Problem besteht in der

⇒ Quantenfehlerkorrektur

- Literatur

Literatur schnell veraltet

- Review Artikel:

A.M. Steane "Quantum computing"
quant-ph 9708022

A. Ekert, R. Josza Rev. Mod. Phys 68, 733 (1996)

- Bücher:

D. Bouwmeester, A. Ekert, A. Zeilinger (eds.)
"The Physics of Quantum Information" Springer 2000

S. Braunstein (eds.)
"Quantum Computing: Where do we want to go tomorrow?" J. Wiley 1999

M.A. Nielsen, I.L. Chuang
"Quantum Computation and Quantum Information"
Cambridge Univ. Press 2000
(