Forschungsseminar Quantenfeldtheorie
- Journal Club -

Quantum Computing Challenges

von Jozef Gruska

erschienen in:
B. Engquist, W. Schmid (Hrsg.)
Mathematics Unlimited - 2001 and Beyond

Springer 2001

vorgestellt von:
André Ewering u. Enno E. Scholz

30. Oktober 2001

Andrés Part

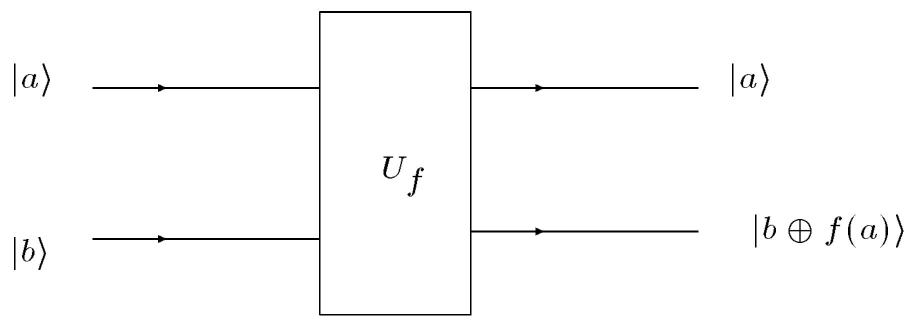
1. Prologue
2. Introduction
3. Going Quantum
4. Historical Milestones
5. Basic Mathematical Framework
6. Quantum Information Processing Resources
7. Limitations of Quantum Information Processing

Quanten Algorithmen

Notation

- Funktion $f : A \to B$ mit A, B endliche Mengen
- Hilbert-Räume $\mathcal{H}_A$, $\mathcal{H}_B$
- U_f entsprechende Unitäre Operation auf $\mathcal{H}_A \otimes \mathcal{H}_A$:

$$U_f \,|a\rangle\,|b\rangle \;=\; |a\rangle\,|b \oplus f(a)\rangle$$



- Hadamard-Transformation

$$H \;=\; \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

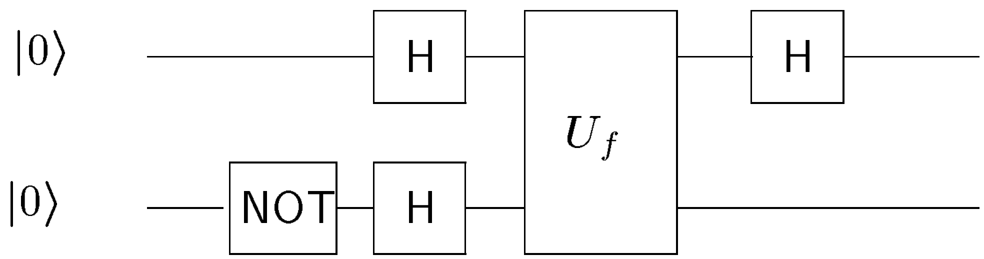
$$H\,|0\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right) \qquad H\,|1\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right)$$

$$H^2 \;=\; \mathbb{1}$$

Deutsch-Problem

- gegeben Funktion $f : \{0,1\} \rightarrow \{0,1\}$ als „black-box“
- Frage: Funktion konstant oder ausgewogen („balanced“)
- klassisch: 2 Schritte erforderlich ($f(0) = ?$, $f(1) = ?$)

Quantenalgorithmus



$$|0\rangle\,|0\rangle \stackrel{\mathbb{1}\otimes\mathrm{NOT}}{\rightarrow} |0\rangle\,|1\rangle \stackrel{H\otimes H}{\rightarrow} \frac{(|0\rangle + |1\rangle)}{\sqrt{2}}\frac{(|0\rangle - |1\rangle)}{\sqrt{2}} = \sum_{x\in\{0,1\}} \frac{|x\rangle}{\sqrt{2}}\frac{(|0\rangle - |1\rangle)}{\sqrt{2}}$$

$$U_f \; |x\rangle \left(|0\rangle - |1\rangle\right) = \begin{cases} \;\; |x\rangle \left(|0\rangle - |1\rangle\right) & , f(x) = 0 \\ -\,|x\rangle \left(|0\rangle - |1\rangle\right) & , f(x) = 1 \end{cases}$$

$$\sum_{x \in \{0,1\}} \frac{|x\rangle}{\sqrt{2}} \frac{\left(|0\rangle - |1\rangle\right)}{\sqrt{2}} \overset{U_f}{\rightarrow} \Big(\frac{1}{\sqrt{2}} \sum_{x \in \{0,1\}} (-1)^{f(x)} \, |x\rangle \Big) \Big(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\Big)$$

Betrachte oberes (input) Register:

- f konstant: $\pm \frac{|0\rangle + |1\rangle}{\sqrt{2}}$
- f ausgewogen: $\pm \frac{|0\rangle - |1\rangle}{\sqrt{2}}$
- nach Anwendung von H: $\pm\, |0\rangle$ bzw. $\pm\, |1\rangle$
- $\Rightarrow$ **eine** Berechung von U_f reicht aus!

Deutsch-Josza-Problem

Anwenung auf Funktion $f : \{0,1\}^n \to \{0,1\}$, entweder konstant oder ausgewogen.

- klassisch: $2^{n-1} + 1$ Schritte erforderlich $\Rightarrow$ Aufwand exponentiell!
- Quantenalgorithmus: analog zum obigen Fall:
  - n input-Register $|0\rangle$, ein output-Register $|0\rangle$
  - H auf input-register, NOT, H auf output-register
  - nach Anwendung von U_f input-Register:

$$\frac{1}{\sqrt{2}^n} \sum_{x \in \{0,1\}^n} (-1)^{f(x)} |x\rangle$$

  - Zustände für f konstant bzw. ausgewogen sind orthogonal!
- nur eine Berechnung U_f
- zur Unterscheidung der Zustände wende H auf die n input-Register an, messe in Basis $\{|0\rangle, |1\rangle\}$
- Aufwand: $\mathcal{O}(n)$ (klassisch: $\mathcal{O}(2^n)$)

Shor-Algorithmus

Ziel: Faktorisierung einer gegeben Zahl N
Klassisch:

- naive Vorgehensweise: probiere Zahlen $2, \ldots, \sqrt{N}$ aus, also $\mathcal{O}\left(\exp(\log N)\right)$
- bisher bester klassischer Algorithmus: $\mathcal{O}\left(\exp((\log N)^{\frac{1}{3}}(\log\log N)^{\frac{2}{3}})\right)$

Problem läßt sich auf die Bestimmung der Periodizität einer Funktion zurückführen:

- zufällige Zahl $a < N$, teilerfremd zu N
- suche kleinstes r mit $a^r \equiv 1 \mod N$
- $f(x) = a^x \mod N$
- $f(x) = f(x+r)$
- Annahme: gefundenes r gerade

$$(a^{\frac{r}{2}} - 1)(a^{\frac{r}{2}} + 1) \equiv 0 \mod N$$

- bestimme größten gemeinsamen Teiler der Faktoren mit N

Quantenalgorithmus zur Periodenbestimmung

gegeben black-box-Funktion $f : \mathbb{Z}_N \to \mathbb{Z}$, mit $f(x+r) = f(x)$, r unbekannt
Quanten-Parallel-Computing

$$|f\rangle \;=\; \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle \, |f(x)\rangle$$

Messung des 2. Registers ergebe Wert y_0
1. Register Gleichverteilung über Zustände $|x\rangle$ mit $f(x) = y_0$

$$|\psi\rangle \;=\; \frac{1}{\sqrt{K}} \sum_{k=0}^{K-1} |x_0 + kr\rangle \qquad N = Kr$$

diskrete Fourier-Transformation (als $N \times N$-Matrix)

$$F_{ab} \;=\; \frac{1}{\sqrt{N}} e^{2\pi i \frac{ab}{N}}$$

$$F\,|\psi\rangle \;=\; \frac{1}{\sqrt{r}} \sum_{j=0}^{r-1} e^{2\pi i \frac{x_0 j}{r}} \left| j \frac{N}{r} \right\rangle$$

Messung des 1. Registers führt zu Zustand c

$$c = \lambda \frac{N}{r}$$

Aufwand: $\mathcal{O}\left(\mathrm{poly}(\log N)\right)$

Quanten-Kryptographie

Hauptproblem: Key-Distribution

$$\textbf{Alice} \xleftrightarrow{\hspace{4em}\textbf{Eve (?)}\hspace{4em}} \textbf{Bob}$$

Lösungen:

- Public-Key (klassisch)
- No-cloning
- Verschränkung
- Ein-Teilchen-Protokolle (z. Bsp. BB84, C.H. Bennett, G. Brassard (1984))

benutze polarisierte Photonen

- $|\uparrow\rangle$ für 0, $|\rightarrow\rangle$ für 1 in Basis $\oplus$
- $|\nearrow\rangle$ für 0, $|\searrow\rangle$ für 1 in Basis $\otimes$
- Alice wählt zufällig Basis und Wert
- Bob wählt zufällig Basis
- Kommunikation über „public channel“
- Test: Eve mitgehört?

A Basis	$\otimes$	$\oplus$	$\oplus$	$\otimes$	...
A Wert	0	0	1	1	...
gesendet	$\|\nearrow\rangle$	$\|\uparrow\rangle$	$\|\rightarrow\rangle$	$\|\searrow\rangle$	...
B Basis	$\otimes$	$\otimes$	$\oplus$	$\oplus$	...
B gemessen	0	1	1	1	...

Error-Correcting-Codes

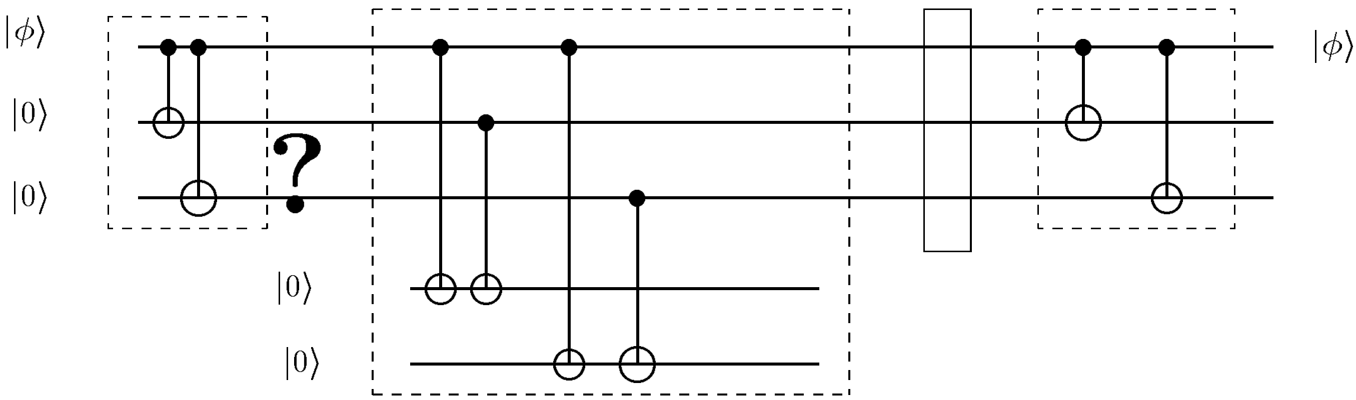
Dekohärenz bewirkt Übertragungsfehler

- mögliche Übertragungsfehler:
  - Bit-Error $\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
  - Phase-Error $\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$
  - Bit-Phasen-Error $\sigma_y = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \sigma_x \sigma_z$
- Probleme:
  - No-Clone-Theorem
  - keine Messung vor Abschluß der gesamten Operation
- Lösungsansatz:
  - Verteilen der Information auf verschränkte qubit-Systeme
  - auftauchende, unterschiedliche Fehler führen zu Entwicklung in paarweise orthogonale Sub-Hilberträume
  - Projektion auf diese ergibt Information über Fehler
  - Behebung möglich

Beispiel: Behebung eines Bit-Errors mit Hilfe eines 3qubit-codes

- $\phi = \alpha |0\rangle + \beta |1\rangle$ übertragen
- verschränkter Zustand $\alpha |000\rangle + \beta |111\rangle$
- Übertragungsfehler: Bit-error
- „Syndrom“mit zwei weiteren Zuständen bestimmen
- Anwendung der entsprechenden Korrektur, hier:

Syndrom	Fehler
00	kein
11	1. Bit
10	2. Bit
01	3. Bit



Literatur

- J. Gruska, *Quantum Computing Challenges*, in: B. Engquist, W. Schmid (Hrsg.), *Mathematics Unlimited - 2001 and Beyond*, Springer 2001
- J. Gruska, *Quantum Computing*, McGraw-Hill 1999
- Vorlesung „Quantum Computing“ von J. Gruska: `http://www.fi.muni.cz/usr/gruska/wien/`
- D. Bouwmester, A. Ekert, A. Zeilinger (Hrsg.), *The Physics of Quantum Information*, Springer 2000
  sehr ausführliches Literaturverzeichnis!
- H. Weinfurter, *Quanteninformatik*, in: Verhandlungen der 120. Tagung der Gesellschaft deutscher Naturforscher u. Ärzte, Berlin, September 1998
- weiteres Material unter:
  `http://www.qubit.org/Intros_Tuts.html`