Quantenquark

Marie Hoffmann

Einleitung

Quanten
Quantenwelt
Superpositionen
Qubits

QuRechner
Funktionen
Gatter

Algorithmen
Faktorisierung
QFT

Fazit
Komplexität
Simulation

Quellen

Quantenrechnung

aus "Computational Complexity - A modern approach"[1]

Marie Hoffmann

Institut für Informatik
Freie Universität zu Berlin

14. Juli 2010

[1] von S. Arora und B. Barak, Cambridge University Press, 1. Auflage 2009

Übersicht

1. Quanten
   - Quantenwelt
   - Superpositionen
   - Qubits
2. QuRechner
   - Funktionen
   - Gatter
3. Algorithmen
   - Algorithmus von Shor: Primfaktorzerlegung
   - Quanten-Fourier-Transformation
4. Fazit
   - Komplexität
   - Simulation von Quantenrechnern
5. Quellen

Church-Turing-These

Quantenquark

Marie Hoffmann

Einleitung

Quanten
Quantenwelt
Superpositionen
Qubits

QuRechner
Funktionen
Gatter

Algorithmen
Faktorisierung
QFT

Fazit
Komplexität
Simulation

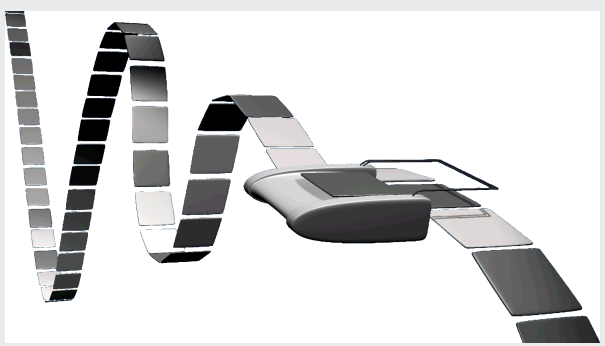
Quellen

Church-Turing-These [Church, 1936], [Turing, 1936]

Jede intuitiv berechenbare Funktion kann von einer Turingmaschine simuliert werden.

Physikalische Version der CT-These [Deutsch, 1985]

Jedes **physikalisch** realisierbare Rechenmodell, unabhängig von der ihm zugrundeliegenden Technologie, kann von einer TM simuliert werden.



Church-Turing-These

Quantenquark
Marie Hoffmann
Einleitung
Quanten
Quantenwelt
Superpositionen
Qubits
QuRechner
Funktionen
Gatter
Algorithmen
Faktorisierung
QFT
Fazit
Komplexität
Simulation
Quellen

Church-Turing-These [Church, 1936], [Turing, 1936]

Jede intuitiv berechenbare Funktion kann von einer Turingmaschine simuliert werden.

Physikalische Version der CT-These [Deutsch, 1985]

Jedes **physikalisch** realisierbare Rechenmodell, unabhängig von der ihm zugrundeliegenden Technologie, kann von einer TM simuliert werden.

Stärker formuliert (*strong form of CT thesis*)

Jedes physikalisch realisierbare Rechenmodell kann von einer TM mit höchstens polynomiellen Aufwand simuliert werden.

Was sind Quanten?
Quantelung

Quantenquark
Marie Hoffmann
Einleitung
Quanten
Quantenwelt
Superpositionen
Qubits
QuRechner
Funktionen
Gatter
Algorithmen
Faktorisierung
QFT
Fazit
Komplexität
Simulation
Quellen

lat. *quantum*: "wie groß", "wie viel"

- **nicht teilbare Portion** bezüglich einer **physikalischen Größe**, meist Energie (Quantelung der physik. Größe)
- kann nur als Ganzes verändert/abgegeben werden
- Beispiele:
  - **Photon** als Quant des **elektromagnetischen Feldes**
    - Energie des Lichts tritt in zur Frequenz propotionalen Einheiten auf
  - Quant des **Drehimpulses** $\vec{L} = \vec{r} \times \vec{p}$
    - ganz- und halbzahlige Vielfache von h([2])
  - **Elektron** bzgl. seiner **vier Quantenzahlen**
    - **Hauptquantenzahl**: Schale $n \in \{1, 2, 3, ...\}$
    - **Nebenquantenzahl**: Orbital $l \in \{0, 1, 2, ..., n-1\}$
    - **Magnetische Quantenzahl des Drehimpuls**: $m \in \{-l, -l+1, ..., l\}$
    - **Spinquantenzahl**: Orientierung des Spins $s_z \in \{-\frac{1}{2}, \frac{1}{2}\}$

[2] Planckschen Wirkungsquantums $h \approx 6,62606896 \cdot 10^{-34} Js$

Was sind Quanten?
Dualismus Welle –Teilchen

Quantenquark

Marie Hoffmann

Einleitung

Quanten

Quantenwelt

Superpositionen

Qubits

QuRechner

Funktionen

Gatter

Algorithmen

Faktorisierung

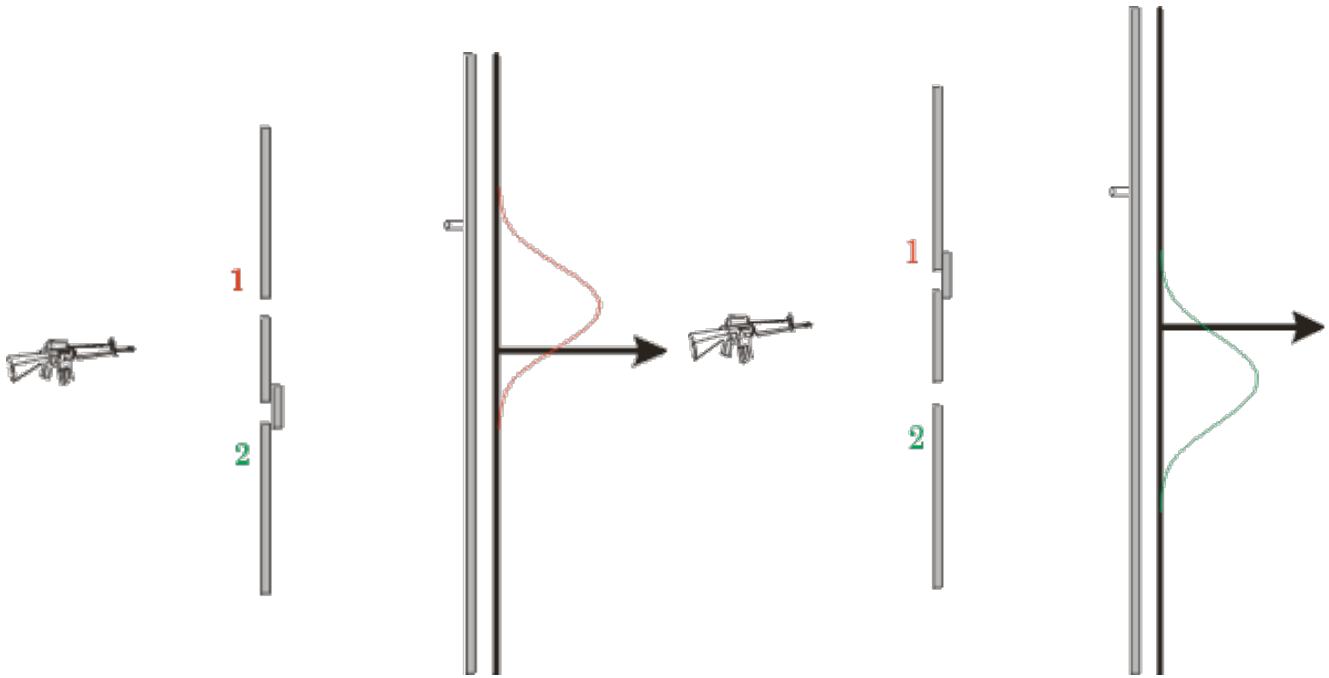
QFT

Fazit

Komplexität

Simulation

Quellen



(a) Spalt 1 geöffnet (b) Spalt 2 geöffnet

Abbildung: Beschuss durch Teilchen/Licht

Was sind Quanten?
Dualismus Welle –Teilchen

Quantenquark

Marie Hoffmann

Einleitung

Quanten

Quantenwelt

Superpositionen

Qubits

QuRechner

Funktionen

Gatter

Algorithmen

Faktorisierung

QFT

Fazit

Komplexität

Simulation

Quellen

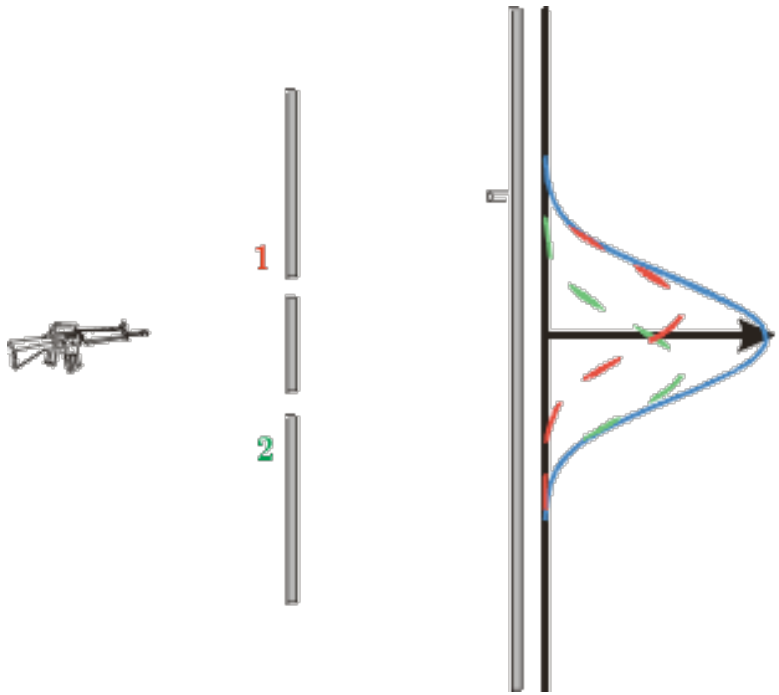


Abbildung: Teilchenbeschuss durch beide Öffnungen

Was sind Quanten?
Dualismus Welle –Teilchen

Quantenquark

Marie Hoffmann

Einleitung

Quanten

Quantenwelt

Superpositionen

Qubits

QuRechner

Funktionen

Gatter

Algorithmen

Faktorisierung

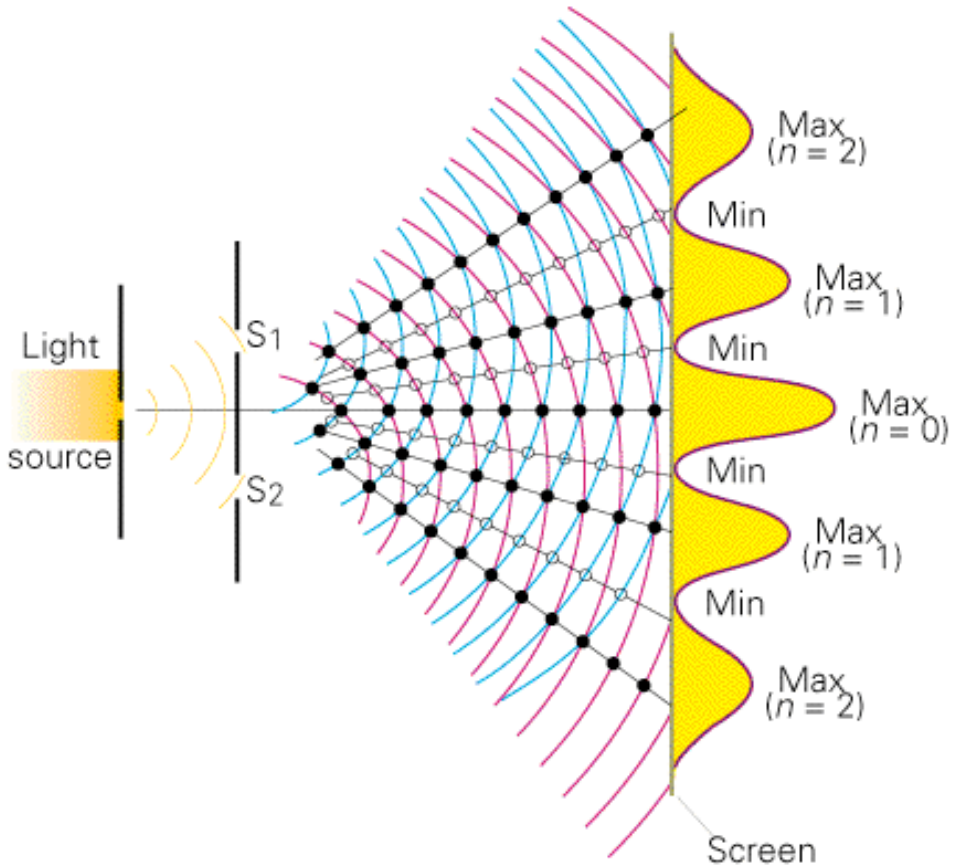
QFT

Fazit

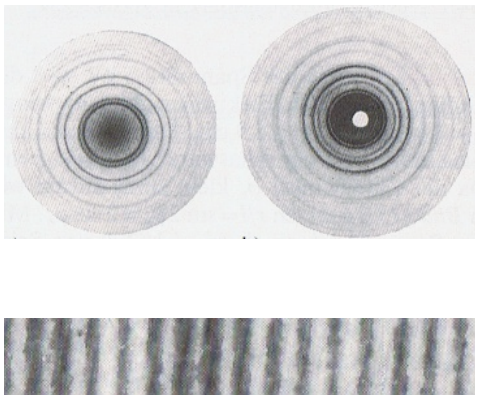
Komplexität

Simulation

Quellen



(a) Lichtbeschuss durch beide Öffnungen



(b) Beugunsbilder

Was sind Quanten?
Dualismus Welle –Teilchen

Quantenquark

Marie Hoffmann

Einleitung

Quanten
Quantenwelt
Superpositionen
Qubits

QuRechner
Funktionen
Gatter

Algorithmen
Faktorisierung
QFT

Fazit
Komplexität
Simulation

Quellen

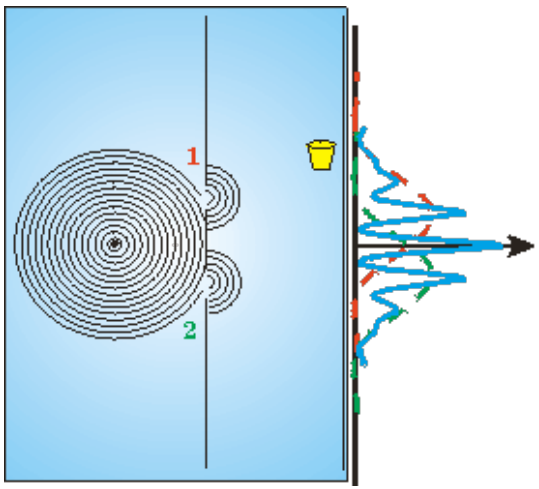


Abbildung: Beugung, Entstehung neuer Wellen

- **Beugung** und **Interferenz** führen zu einem charakteristischen Beugungsbild
- Experiment wiederholbar für Elektronen, Ionen

$\Rightarrow$ Quantenobjekten wird eine Wahrscheinlichkeitswelle mit **Wellenlänge** $\lambda = \frac{h}{p}$ zugeordnet

Was sind Quanten?
Dualismus Welle –Teilchen

Quantenquark

Marie Hoffmann

Einleitung

Quanten

Quantenwelt

Superpositionen

Qubits

QuRechner

Funktionen

Gatter

Algorithmen

Faktorisierung

QFT

Fazit

Komplexität

Simulation

Quellen

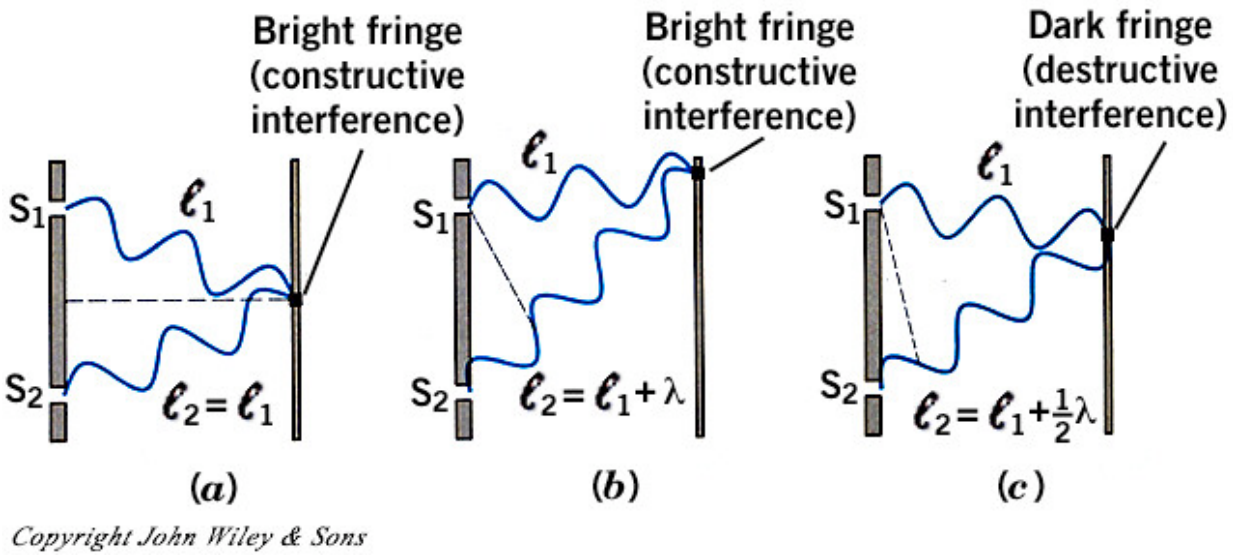


Abbildung: Interferenz, Überlagerung von Wellen

- **Beugung** und **Interferenz** führen zu einem charakteristischen Beugungsbild
- Experiment wiederholbar für Elektronen, Ionen

$\Rightarrow$ Quantenobjekten wird eine Wahrscheinlichkeitswelle mit **Wellenlänge** $\lambda = \frac{h}{p}$ zugeordnet

Von Quanten zu Qubits
Superposition

Quantenquark

Marie Hoffmann

Einleitung

Quanten
Quantenwelt
Superpositionen
Qubits

QuRechner
Funktionen
Gatter

Algorithmen
Faktorisierung
QFT

Fazit
Komplexität
Simulation

Quellen

- benötigen manipulierbares Speicherelement analog zum Bit: das **Qubit**
- Zustandsbeschreibung mithilfe des Superpositionsprinzip

Prinzip der Superposition

- zwei beliebige Zustände eines Quants werden als Grundzustände festgesetzt: $|0\rangle$ und $|1\rangle$
- beide Zustände überlagern sich, bzw. interferieren
- Quant kann alle Zustände der Form $\alpha_0|0\rangle + \alpha_1|1\rangle$ annehmen

Amplituden $\alpha_{0/1} \in \mathbb{C}$ und $|\alpha_0|^2 + |\alpha_1|^2 = 1$

- ersetze **Quant** durch **Qubit**
- Achtung: **Messung führt zum Kollaps des Quantensystems!**

Von Quanten zu Qubits

Zwei-Qubit-System

Ein-Qubit-System: $\alpha_0|0\rangle + \alpha_1|1\rangle$

$$p(|0\rangle) = \alpha_0^2 \text{ und } p(|1\rangle) = \alpha_1^2$$

Analog ein **Zwei-Qubit-System**:

$$z_{b_1 b_2} = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$$

umgeschrieben:

$$z_{b_1 b_2} = \underbrace{(|0\rangle + |1\rangle)}_{b_1}\underbrace{(|0\rangle + |1\rangle)}_{b_2}$$

$\sum_{b_1,b_2} |\alpha_{b_1 b_2}|^2 = 1$

Frage: Wie groß ist die W'keit, dass sich ein Zwei-Qubit-System im Zustand $|b_1 b_2\rangle$ befindet?

Von Quanten zu Qubits

Zwei-Qubit-System

Ein-Qubit-System: $\alpha_0|0\rangle + \alpha_1|1\rangle$

$$p(|0\rangle) = \alpha_0^2 \text{ und } p(|1\rangle) = \alpha_1^2$$

Analog ein **Zwei-Qubit-System**:

$$z_{b_1 b_2} = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$$

umgeschrieben:

$$z_{b_1 b_2} = \underbrace{(|0\rangle + |1\rangle)}_{b_1}\underbrace{(|0\rangle + |1\rangle)}_{b_2}$$

$\sum_{b_1,b_2} |\alpha_{b_1 b_2}|^2 = 1$

Frage: Wie groß ist die W'keit, dass sich ein Zwei-Qubit-System im Zustand $|b_1 b_2\rangle$ befindet?

Antwort: Antwort: $|\alpha_{b_1 b_2}|^2$

Von Quanten zu Qubits
Geometrische Veranschaulichung der Superpositionen

Quantenquark

Marie Hoffmann

Einleitung

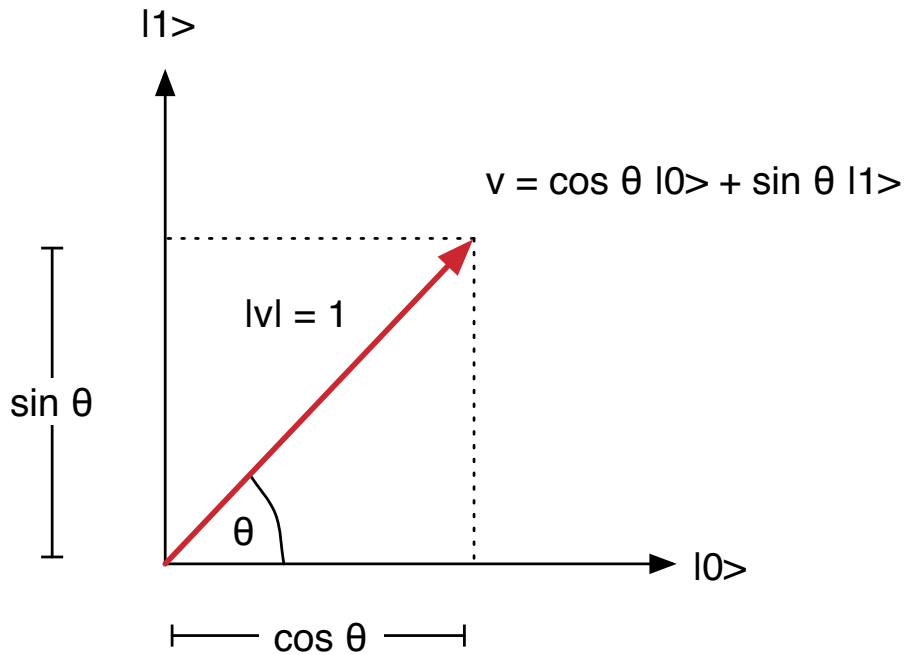
Quanten
- Quantenwelt
- Superpositionen
- Qubits

QuRechner
- Funktionen
- Gatter

Algorithmen
- Faktorisierung
- QFT

Fazit
- Komplexität
- Simulation

Quellen



Zu einem beliebigen Zeitpunkt befindet sich das System[3]

- in Zustand $|0\rangle$ mit W'keit $\cos^2\theta$
- in Zustand $|1\rangle$ mit W'keit $\sin^2\theta$

[3] Koeffizienten aus $\mathbb{R}$

EPR-Paradoxon
Ein Gedankenexperiment

Quantenquark

Marie Hoffmann

Einleitung

Quanten
Quantenwelt
Superpositionen
Qubits

QuRechner
Funktionen
Gatter

Algorithmen
Faktorisierung
QFT

Fazit
Komplexität
Simulation

Quellen

Das **EPR-Paradoxon**[4] veranschaulicht wie zwei Systeme[5] mithilfe der Quantenmechanik zeitgleich ihre Aktionen koordinieren können.

- zunächst nur Gedankenspiel [1935]
- paradox: nichts ist schneller als Licht
- John Bell [1964] macht daraus ein reales Experiment

Version von Bells Experiment: **Paritätsspiel**

- Ratespiel
- Spielleiter und zwei Spieler Alice (A) und Bob (B)

[4] benannt nach Einstein, Podosky und Rosen
[5] räumlich getrennte

Quantenquark

Marie Hoffmann

Einleitung

Quanten
Quantenwelt
Superpositionen
Qubits

QuRechner
Funktionen
Gatter

Algorithmen
Faktorisierung
QFT

Fazit
Komplexität
Simulation

Quellen

Spielablauf

1. Spielleiter wählt zufällig zwei Bits $x, y \in_R \{0, 1\}]$
2. x wird Alice und y Bob gezeigt[4]
3. Alice und Bob entscheiden[5] mit welchen Bit a bzw. b sie dem Spielleiter antworten, $a, b \in \{0, 1\}$
4. Alice und Bob gewinnen $\Leftrightarrow x \wedge y = a \oplus b$

x	y	$x \wedge y$
0	0	0
0	1	0
1	0	0
1	1	1

a	b	$a \oplus b$
0	0	0
0	1	1
1	0	1
1	1	0

[4] keiner kennt das andere Bit

[5] ohne Informationsaustausch mit dem anderen Spieler

Quantenquark
Marie Hoffmann
Einleitung
Quanten
Quantenwelt
Superpositionen
Qubits
QuRechner
Funktionen
Gatter
Algorithmen
Faktorisierung
QFT
Fazit
Komplexität
Simulation
Quellen

Versuchsaufbau 1: kein gemeinsames Quantensystem

- falls $f(x) = a$ und $g(y) = b$[4], dann Gewinnw'keit $p = \frac{1}{2}$
- beste Strategie: beide antworten unabhängig von der Eingabe immer mit 0, dann $p = \frac{3}{4}$

x	y	$x \wedge y$
0	0	**0**
0	1	**0**
1	0	**0**
1	1	1

a	b	$a \oplus b$
0	**0**	**0**
0	1	1
1	0	1
1	1	0

$$p = \underbrace{p(x \wedge y = 0)}_{\frac{3}{4}} * \underbrace{p(a \oplus b = 0 | a = b = 0)}_{1}$$

[4] Antwort abhängig von Eingabe

Quantenquark
Marie Hoffmann
Einleitung
Quanten
Quantenwelt
Superpositionen
Qubits
QuRechner
Funktionen
Gatter
Algorithmen
Faktorisierung
QFT
Fazit
Komplexität
Simulation
Quellen

Versuchsaufbau 2: gemeinsames Quantensystem im Zustand $z_{EPR} = |00\rangle + |11\rangle$

- A bekommt das erste Qubit q_A, B das zweite Qubit q_B
- einigen sich vorher:
  1. A: $x = 1$, dann $rotate(q_A, \frac{\pi}{8})$
  2. B: $y = 1$, dann $rotate(q_B, -\frac{\pi}{8})$
  3. $x = 0 \vee y = 0$, dann tun sie nichts
  4. Antwort: Lesen ihr Qubit $q_{A,B} = \alpha_{A/B,0}|0\rangle + \alpha_{A/B,1}|1\rangle$ und antworten mit den W'keiten $f(q_{A,0}) = \alpha_{A,0}^2$ für $|0\rangle$ und $f(q_{A,1}) = \alpha_{A,1}^2$ für $|1\rangle$, B analog
- drei grundsätzliche Fälle
  1. $p_{xy}(x = y = 0) = 1/4$
  2. $p_{xy}(x \neq y) = 1/2$
  3. $p_{xy}(x = y = 1) = 1/4$

Quantenquark
Marie Hoffmann
Einleitung
Quanten
Quantenwelt
Superpositionen
Qubits
QuRechner
Funktionen
Gatter
Algorithmen
Faktorisierung
QFT
Fazit
Komplexität
Simulation
Quellen

Fall 1: $x = y = 0$, Aktion: beide **rotieren** nicht ihre Qubit und **messen** es

- zum Zeitpunkt der Messung $q_{EPR}(t) = |00\rangle \vee |11\rangle$

  $\underline{q_{EPR}(t) = |00\rangle, \theta = 0}$

  $$f(q_A) = \begin{pmatrix} \cos^2 0 \\ \sin^2 0 \end{pmatrix} = f(q_B) = \begin{pmatrix} \cos^2 0 \\ \sin^2 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

  Auswertung: $\underbrace{x \wedge y}_{0 \wedge 0 = 0} = \underbrace{a \oplus b}_{0 \oplus 0 = 0} \equiv 1$

  $\underline{q_{EPR}(t) = |11\rangle, \theta = \pi/2}$

  $$f(q_A) = \begin{pmatrix} \cos^2 \frac{\phi}{2} \\ \sin^2 \frac{\theta}{2} \end{pmatrix} = f(q_B) = \begin{pmatrix} \cos^2 \frac{\theta}{2} \\ \sin^2 \frac{\theta}{2} \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

  Auswertung: $\underbrace{x \wedge y}_{0 \wedge 0 = 0} = \underbrace{a \oplus b}_{1 \oplus 1 = 0} \equiv 1$

- $p(x = y = 0) = 1$

Quantenquark
Marie Hoffmann
Einleitung
Quanten
Quantenwelt
Superpositionen
Qubits
QuRechner
Funktionen
Gatter
Algorithmen
Faktorisierung
QFT
Fazit
Komplexität
Simulation
Quellen

Fall 2: $x \neq y$, Aktion: **einer rotiert**, der **andere tut nichts**, o.B.d.A. A: $x = 0$ und B: $y = 1$ und **messen**

- zum Zeitpunkt der Messung $q_{EPR}(t) = |00\rangle \vee |11\rangle$

  $\underline{q_{EPR}(t) = |00\rangle, \theta = 0}$

$$f(q_A) = \begin{pmatrix} \cos^2 0 \\ \sin^2 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

B rotiert $q_B = \cos\frac{\pi}{8}|0\rangle - \sin\frac{\pi}{8}|1\rangle$ und gibt aus

$$f(q_B) = \begin{pmatrix} \cos^2 \frac{\pi}{8} \\ \sin^2 \frac{\pi}{8} \end{pmatrix}$$

um zu gewinnen müssen beide Bits gleich sein
$p(x \neq y \wedge |00\rangle) = 1 \cdot \cos^2 \frac{\theta}{8}$

Quantenquark
Marie Hoffmann
Einleitung
Quanten
Quantenwelt
Superpositionen
Qubits
QuRechner
Funktionen
Gatter
Algorithmen
Faktorisierung
QFT
Fazit
Komplexität
Simulation
Quellen

Fall 2: $x \neq y$, Aktion: **einer rotiert**, der **andere tut nichts**, o.B.d.A. A: $x = 0$ und B: $y = 1$ und **messen**

- zum Zeitpunkt der Messung $q_{EPR}(t) = |00\rangle \vee |11\rangle$
  $\underline{q_{EPR}(t) = |11\rangle, \theta = \frac{\pi}{2}}$

$$f(q_A) = \begin{pmatrix} \cos^2 \frac{\pi}{2} \\ \sin^2 \frac{\pi}{2} \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

B rotiert
$q_B = \cos(\frac{\pi}{2} - \frac{\pi}{8})|0\rangle + \sin(\frac{\pi}{2} - \frac{\pi}{8})|1\rangle = \sin\frac{\pi}{8}|0\rangle + \cos\frac{\pi}{8}$
und gibt aus

$$f(q_B) = \begin{pmatrix} \sin^2 \frac{\pi}{8} \\ \cos^2 \frac{\pi}{8} \end{pmatrix}$$

um zu gewinnen müssen beide Bits gleich sein
$p(x \neq y \wedge |11\rangle) = 1 \cdot \cos^2 \frac{\theta}{8}$

Quantenquark
Marie Hoffmann
Einleitung
Quanten
Quantenwelt
Superpositionen
Qubits
QuRechner
Funktionen
Gatter
Algorithmen
Faktorisierung
QFT
Fazit
Komplexität
Simulation
Quellen

Fall 3: $x = y = 1$, Aktion **beide rotieren** ihr Qubit und **messen**, gewinnen g.d.w. $a \neq b$

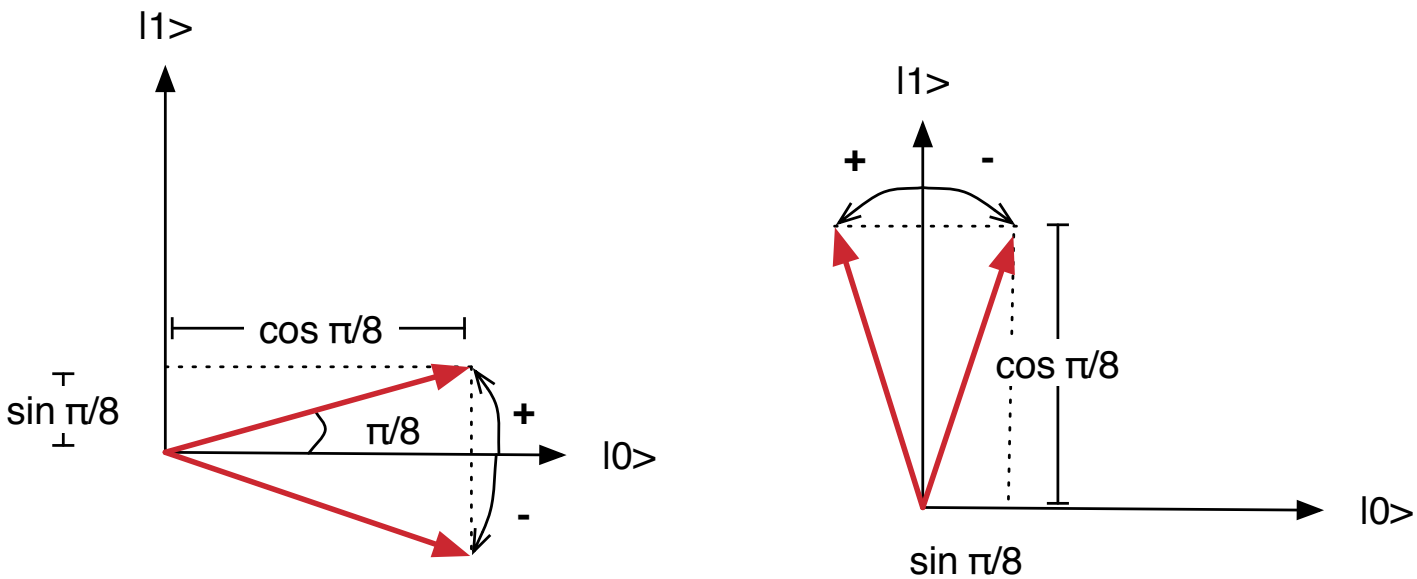


Abbildung: Rotation aus $|0\rangle$ und $|1\rangle$

Quantenquark
Marie Hoffmann
Einleitung
Quanten
Quantenwelt
Superpositionen
Qubits
QuRechner
Funktionen
Gatter
Algorithmen
Faktorisierung
QFT
Fazit
Komplexität
Simulation
Quellen

Fall 3: $x = y = 1$, Aktion **beide rotieren** ihr Qubit und **messen**, gewinnen g.d.w. $a \neq b$

$$
\begin{aligned}
q_{AB} &= q_{AB}^{|00\rangle} + q_{AB}^{|11\rangle} \\
&= \underbrace{(\cos\frac{\pi}{8}|0\rangle + \sin\frac{\pi}{8}|1\rangle)}_{q_A^{|0\rangle}} \underbrace{(\cos\frac{\pi}{8}|0\rangle - \sin\frac{\pi}{8}|1\rangle)}_{q_B^{|0\rangle}} \\
&\quad + \\
&\quad \underbrace{(-\sin\frac{\pi}{8}|0\rangle + \cos\frac{\pi}{8}|1\rangle)}_{q_A^{|1\rangle}} \underbrace{(\sin\frac{\pi}{8}|0\rangle + \cos\frac{\pi}{8}|1\rangle)}_{q_B^{|1\rangle}} \\
&= (\cos^2\frac{\pi}{8} - \sin^2\frac{\pi}{8})|00\rangle - 2\sin\frac{\pi}{8}\cos\frac{\pi}{8}|01\rangle + \\
&\quad 2\sin\frac{\pi}{8}\cos\frac{\pi}{8}|10\rangle + (\cos^2\frac{\pi}{8} - \sin\frac{\pi}{8})|11\rangle
\end{aligned}
$$

Alle Koeffizienten betragen $\frac{1}{\sqrt{2}} \Longrightarrow$ alle Zustände gleichwahrscheinlich mit Normalisierungsfaktor $(\frac{1}{\sqrt{2}} \cdot \frac{1}{\sqrt{2}})^2 = \frac{1}{4}$.

Quantenquark

Marie Hoffmann

Einleitung

Quanten
Quantenwelt
Superpositionen
Qubits

QuRechner
Funktionen
Gatter

Algorithmen
Faktorisierung
QFT

Fazit
Komplexität
Simulation

Quellen

Zusammengefasst:

$$p_q = \underbrace{\frac{1}{4}}_{x=y=0} \cdot 1 + \underbrace{\frac{1}{2}}_{x \neq y} \cdot \cos^2 \frac{\pi}{8} + \underbrace{\frac{1}{4}}_{x=y=1} \cdot \frac{1}{2} \geq 0.8 > 0.75 = p_{notq}$$

$\Longrightarrow$ mit einem Qubit-System erhöht sich die Gewinnwahrscheinlichkeit im Ratespiel ohne Informationsaustausch[4]

[4] dieser fand vor Spielbeginn statt

Quantenrechnung

Quantenquark

Marie Hoffmann

Einleitung

Quanten
Quantenwelt
Superpositionen
Qubits

QuRechner
Funktionen
Gatter

Algorithmen
Faktorisierung
QFT

Fazit
Komplexität
Simulation

Quellen

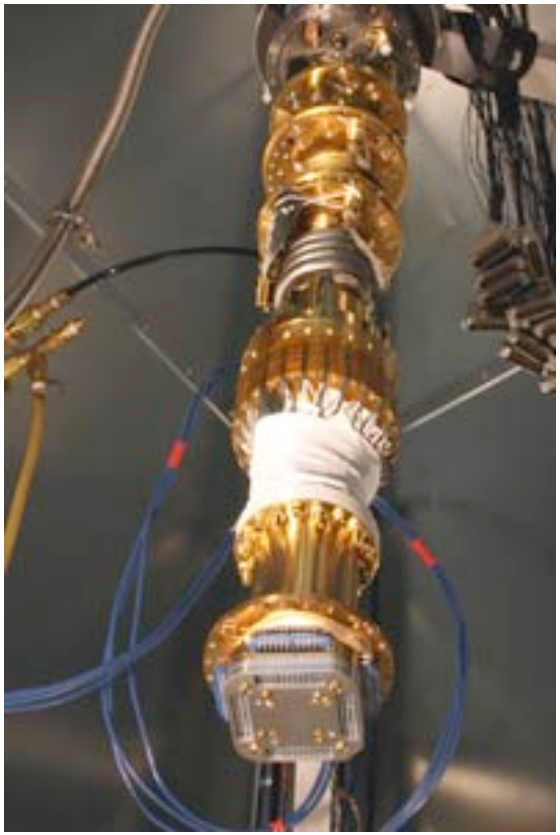


Abbildung: 16-Qubit-Quantencomputer der Firma D-Wave

Lineare Algebra
zur Erinnerung

Quantenquark
Marie Hoffmann
Einleitung
Quanten
Quantenwelt
Superpositionen
Qubits
QuRechner
Funktionen
Gatter
Algorithmen
Faktorisierung
QFT
Fazit
Komplexität
Simulation
Quellen

komplexe Zahl $z = a + ib$, dann ist $\bar{z} = a - ib$ die *komplex Konjugierte* zu z, $i = \sqrt{-1}$

Norm $||u||_2 = ||u|| = \sqrt{< u, u >}$

Orthogonalität $< u, v >= 0 \Leftrightarrow u, v$ sind orthogonal

Orthonormalbasis $\{v^i\}_{i \in [1..m]} \in \mathbb{C}^m$ ist Orthonormalbasis von $\mathbb{C}^m$ g.d.w. $< v^i, v^j >_{i \neq j}= 0$ und $< v^i, v^j >_{i=j}= 1$

konjugiert Transponierte A^* zu $A \in \mathbb{C}^{m \times m}$ mit $A^*_{ij} = \bar{A}_{ji}, \forall i, j \in [1..m]$

unitäre Matrix eine Matrix $A \in \mathbb{R}^{m \times m}$ ist unitär, wenn $AA^* = I$

Quantenregister

Quantenquark

Marie Hoffmann

Einleitung

Quanten
Quantenwelt
Superpositionen
Qubits

QuRechner
Funktionen
Gatter

Algorithmen
Faktorisierung
QFT

Fazit
Komplexität
Simulation

Quellen

Speicher

- ein m-**Qubit-Quantenregister** ist zusammengesetzt aus m Qubits

- Zustandsraum: alle Superpositionen über die $\{0,1\}^m = 2^m$ Grundzustände
- Zustandsvektor $v = \langle v_{0^m}, v_{0^{m-1}1}, ..., v_{1^m} \rangle$, $\sum_x |v_x|^2 = 1$
- Messung: $p(|x\rangle) = v_x^2$ und $v_{x \neq y} = 0$ [5]

[5] Kollaps: alle anderen Koeffizienten werden Null

Quantenoperationen

Quantenquark
Marie Hoffmann
Einleitung
Quanten
Quantenwelt
Superpositionen
Qubits
QuRechner
Funktionen
Gatter
Algorithmen
Faktorisierung
QFT
Fazit
Komplexität
Simulation
Quellen

Quantenoperation F

Eine Quantenoperation ist eine Funktion F, die für ein m-Qubit-Register einen Zustandswechsel durchführt

$$F : \mathbb{C}^{2^m} \mapsto \mathbb{C}^{2^m}$$

und den Bedingungen genügt:

Linearität $F(v) = \sum_x v_x F(|x\rangle),\ \forall v \in C^{2^m}$

Normerhaltung $||v|| = 1 \Rightarrow ||F(v)|| = 1$

1. F kann durch eine *unitäre* $2^m \times 2^m$-Matrix A beschrieben werden
2. da $AA^* = I$[6], hat jede Funktion eine Inverse

[6] also unitär ist

Quantenquark

Marie Hoffmann

Einleitung

Quanten
Quantenwelt
Superpositionen
Qubits

QuRechner
Funktionen
Gatter

Algorithmen
Faktorisierung
QFT

Fazit
Komplexität
Simulation

Quellen

Definition: elementar

Eine Quantenoperation[a] ist *elementar*, wenn sie auf höchstens **drei** Qubits des Registers rechnet.

[a] oder auch mehrere Quantengatter

Definition: Quantenberechnung

Eine Quantenberechnung ist eine Sequenz von Elementaroperationen angewandt auf ein Quantenregister.

Quantenoperationen

BQP: *bounded error quantum polynomial time*

Quantenquark

Marie Hoffmann

Einleitung

Quanten
Quantenwelt
Superpositionen
Qubits

QuRechner
Funktionen
Gatter

Algorithmen
Faktorisierung
QFT

Fazit
Komplexität
Simulation

Quellen

Definition: BQP

Ein Boolesche Funktion $f : \{0,1\}^* \mapsto \{0,1\}$ ist in **BQP**, wenn es ein Polynom $p : \mathbb{N} \mapsto \mathbb{N}$ gibt, so dass f in $p(n)$-Zeit quantenberechenbar ist.

No-Cloning-Theorem

Quantenquark

Marie Hoffmann

Einleitung

Quanten
Quantenwelt
Superpositionen
Qubits

QuRechner
Funktionen
Gatter

Algorithmen
Faktorisierung
QFT

Fazit
Komplexität
Simulation

Quellen

No-Cloning-Theorem

Resultat der Quantenphysik: Das **Kopieren** von einem Qubit auf ein anderes ist **nicht möglich** ohne das ursprüngliche zu verändern.

$\Rightarrow$ Kopieren ist nicht umkehrbar, also keine gültige Funktion[a]

$$\cancel{x := y}, \text{ aber } x := \underbrace{x}_{=0} \vee y$$

b

---

[a] keine unitäre Matrix bildbar

[b] es dürfen auch keine neuen Qubits hinzugenommen werden

No-Cloning-Theorem

Quantenquark

Marie Hoffmann

Einleitung

Quanten
Quantenwelt
Superpositionen
Qubits

QuRechner
Funktionen
Gatter

Algorithmen
Faktorisierung
QFT

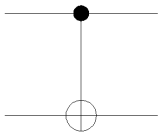
Fazit
Komplexität
Simulation

Quellen

Beispiele:

1. $CNOT(x)$[7]

$$|xy\rangle \mapsto |x(x \oplus y)\rangle$$



x	$y = x \oplus 0$
0	0
1	1

x	$y = x \oplus 1$
0	1
1	0

2. $AND(b_1, b_2)$

$$|b_1\rangle|b_2\rangle|b_3\rangle \mapsto |b_1\rangle|b_2\rangle|b_3 \oplus (b_1 \wedge b_2)\rangle$$

3. $FLIP(x, y)$, $|0\rangle \mapsto |1\rangle$ und $|1\rangle \mapsto |0\rangle$

! y, b_3 müssen unberührte Qubits im Zustand $|0\rangle$ bzw. $|1\rangle$ sein!

[7] controlled NOT

Hadamard-Gatter

Quantenquark

Marie Hoffmann

Einleitung

Quanten
Quantenwelt
Superpositionen
Qubits

QuRechner
Funktionen
Gatter

Algorithmen
Faktorisierung
QFT

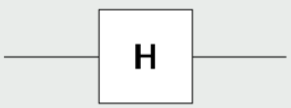
Fazit
Komplexität
Simulation

Quellen

Hadamard-Gatter

einstellige Funktion, die Zustände $|0\rangle, |1\rangle$ in überlagerte Zustände überführt

$$\begin{pmatrix}|0\rangle\\|1\rangle\end{pmatrix} \mapsto \frac{1}{\sqrt{2}}\begin{pmatrix}|0\rangle + |1\rangle\\|0\rangle - |1\rangle\end{pmatrix}, \text{ Matrix: } \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\1 & -1\end{pmatrix}$$

Schaltsymbol: 

, allgemein: $|b\rangle \mapsto |0\rangle + (-1)^b|1\rangle$

Hadamard-Gatter auf ein m-Qubit-Register angewandt:

$$|b\rangle \text{ —H— } \frac{1}{\sqrt{2^m}} \sum_{x\in\{0,1\}^m} (-1)^{xb}|x\rangle = \frac{1}{\sqrt{2^m}} \sum_{x\in\{0,1\}^m} (-1)^{x\odot b}|x\rangle$$

Hadamard-Gatter

Quantenquark

Marie Hoffmann

Einleitung

Quanten
Quantenwelt
Superpositionen
Qubits

QuRechner
Funktionen
Gatter

Algorithmen
Faktorisierung
QFT

Fazit
Komplexität
Simulation

Quellen

Beispiele:

1. $m = 1$

$$\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} v_1 \\ v_2 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} v_1 + v_2 \\ v_1 - v_2 \end{pmatrix}$$

2. $m = 2$

$$|01\rangle \text{ —[H]— } \frac{1}{\sqrt{2^m}} \sum_{x \in \{0,1\}^m} (-1)^{x \cdot b} |x\rangle = \frac{1}{2} \sum_{x \in \{0,1\}^2} (-1)^x |x\rangle$$

$$= \frac{1}{2} \left[|00\rangle - |01\rangle + |10\rangle - |11\rangle \right]$$

Quantenquark
Marie Hoffmann
Einleitung
Quanten
Quantenwelt
Superpositionen
Qubits
QuRechner
Funktionen
Gatter
Algorithmen
Faktorisierung
QFT
Fazit
Komplexität
Simulation
Quellen

Primfaktorzerlegung

Gegeben ein $N \in \mathbb{N}$

Finde Menge aller Primzahlfaktoren von N

Bisher bester klassische Algorithmus: $2^{(\log N)^{1/3}}$ Schritte

Algorithmus von Shor: Faktorisierung in **BPQ**

Es gibt ein Quantenalgorithmus, der ein gegebenes N die Primzahlzerlegung in $poly(\log N))$ Zeit ausgibt.

Der Algorithmus von Shor [1994]

- gehört zur Klasse der Monte-Carlo-Algorithmen

$\Rightarrow$ ist in wenigen Fällen falsch

- zwei Teile: klassischer Teil (Reduktion) und Quantenteil

Quantenquark
Marie Hoffmann
Einleitung
Quanten
Quantenwelt
Superpositionen
Qubits
QuRechner
Funktionen
Gatter
Algorithmen
Faktorisierung
QFT
Fazit
Komplexität
Simulation
Quellen

Behauptung

Problem der Primzahlfaktorisierung kann auf das Problem der Ordnungsbestimmung reduziert werden

Definition: Ordnung

Die Ordnung r ist die kleinste natürliche Zahl mit der ein Element a einer Gruppe G mit sich selber verknüpft werden muss, damit gilt: $a^r = e$. e sei das neutrale Element von G.

- im Fall der Primfaktorzerlegung einer Zahl N gilt:

$$a^r \equiv 1(\mod N)$$

- es reicht **einen Faktor** zu finden und die Anwendung zu **wiederholen**

Algorithmus von Shor

Klassischer Teil – Reduktion auf Bestimmung der Ordnung

Sei dies vom Algorithmus sicher gestellt[8]:

1. wähle zufällig $1 < A < N$
2. Bestimme Ordnung r, so dass

$$A^r \equiv 1(\mod N) \Longleftrightarrow A^r - 1 \equiv 0$$

3. r gerade und $A^{r/2} + 1 \not\equiv 0$

$k_{1-5} \in \mathbb{N}$, betrachte

$$(\underbrace{A^{r/2} - 1}_{k_4 \cdot N + k_5 \not\equiv 0 \text{ aus 2.}})(\underbrace{A^{r/2} + 1}_{k_2 \cdot N + k_3 \not\equiv 0}) = \underbrace{A^r - 1}_{k_1 \cdot N \equiv 0}$$

$$\Rightarrow \quad k_4 N k_2 N + k_4 N k_3 + k_v k_2 N + k_5 k_3 \equiv 0$$

$$= \underbrace{N \cdot Rest}_{\equiv 0} + \underbrace{k_5 k_3}_{\Rightarrow \equiv 0} \equiv 0 \Longrightarrow A^{r/2} - 1 \text{ enthält Teiler}$$

[8] falls nicht wieder zu Schritt 1

Quantenquark
Marie Hoffmann
Einleitung
Quanten
Quantenwelt
Superpositionen
Qubits
QuRechner
Funktionen
Gatter
Algorithmen
Faktorisierung
QFT
Fazit
Komplexität
Simulation
Quellen

Shor's Algorithm

Eingabe: $N \in \mathbb{N}$, Ausgabe: ein Primfaktor

1. Wähle ein A zufällig aus $[2..N-1]$
2. Bestimme $g = ggT(A, N)$ mit euklidischen Algorithmus[a]
   (a) falls $g \neq 1$ gebe g zurück und terminiere
   (b) sonst weiter 3
3. Bestimme mit **Quantenteil** Ordnung r von A [b]
4. zurück zu 1. falls[c]
   (a) r ungerade
   (b) $A^{r/2} \equiv -1(\%N)$
5. gebe $ggT(A^{r/2} - 1, n)$ zurück

---

[a] siehe Anhang im Handout
[b] kleinstes r, so dass $A^r \equiv 1(\%N)$
[c] W'keit $< 3/4$

Algorithmus von Shor
Quantenteil – QFT

Quantenquark
Marie Hoffmann
Einleitung
Quanten
Quantenwelt
Superpositionen
Qubits
QuRechner
Funktionen
Gatter
Algorithmen
Faktorisierung
QFT
Fazit
Komplexität
Simulation
Quellen

Kernstück ist die Quanten-Fourier-Transformation (**QFT**, analog zur FFT)

- jedes sich wiederholende Ereignis f lässt sich durch Sinus/Kosinuswellen darstellen[9]

$$\hat{f}(x) = \frac{1}{\sqrt{M}} \sum_{y \in \mathbb{Z}_M} f(x)\omega^{xy} \text{ mit } \omega = e^{2\pi i/M}$$

  Transformation von f in die Fourier-Basis $\{\chi_x\}_{x \in \mathbb{Z}_M}$
- wenn f periodisch ist, dann werden die Koeffizienten zur Amplitude korrespondierender Basen groß
- Bestimmung der hauptsächlich vorkommenden Frequenzen im Signal und deren Amplituden

$\Rightarrow$ erlaubt Detektion der Perioden von Quantenzuständen

[9] $e^{i\phi} = \cos\phi + i\sin\phi$

Quantenquark
Marie Hoffmann
Einleitung
Quanten
Quantenwelt
Superpositionen
Qubits
QuRechner
Funktionen
Gatter
Algorithmen
Faktorisierung
QFT
Fazit
Komplexität
Simulation
Quellen

Lemma zur Quanten-Fourier-Transformation

Für jedes m und $M = 2^m$ gibt es einen Quantenalgorithmus, der $O(m^2)$ elementare Quantenoperationen benötigt und eine Quantenregister vom Zustand $f = \sum_{x \in \mathbb{Z}_m} f(x)|x\rangle$ nach $\hat{f} = \sum_{y \in \mathbb{Z}_m} \hat{f}(x)|x\rangle$ mit $\hat{f}(x) = \frac{1}{\sqrt{M}} \sum_{y \in \mathbb{Z}_m} \omega^{xy} f(x)$

$\mathbb{Z}_M = \{0, 1, 2, ..., M-1\}$

Begründung: FT_M lässt sich in zwei Teilprobleme der Größe $M/2$ trennen.

Quantenquark
Marie Hoffmann
Einleitung
Quanten
Quantenwelt
Superpositionen
Qubits
QuRechner
Funktionen
Gatter
Algorithmen
Faktorisierung
QFT
Fazit
Komplexität
Simulation
Quellen

Zwei Gatter reichen zur Durchführung einer **QFT**

1. **Hadamard-Gatter** operierend auf dem j-ten Qubit

$$R_j = \begin{array}{c|cc} |0\rangle & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ |1\rangle & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{array}$$

2. **Phasengatter**, operierend auf Qubits j und k

$$S_{j,k} = \begin{array}{c|cccc} |00\rangle & 1 & 0 & 0 & 0 \\ |01\rangle & 0 & 1 & 0 & 0 \\ |10\rangle & 0 & 0 & 1 & 0 \\ |11\rangle & 0 & 0 & 0 & e^{i\theta_{k-j}} \end{array}$$

$$\theta_{k-j} = \pi/2^{k-j}$$

Quantenquark
Marie Hoffmann
Einleitung
Quanten
Quantenwelt
Superpositionen
Qubits
QuRechner
Funktionen
Gatter
Algorithmen
Faktorisierung
QFT
Fazit
Komplexität
Simulation
Quellen

Algorithmus zur Ordnungsbestimmung

Eingabe: N und $A < N$, Ausgabe: Ordnung r, Register: $m + polylog(N)$ Qubits mit $m = \lceil 5 \log N \rceil$

1. Wende die QFT auf die ersten m Qubits an
2. Berechne $|x\rangle|y\rangle \mapsto |x\rangle y \oplus (A^x(\%N))\rangle$
3. Miss das zweite Register um y_0 zur erhalten
4. Wende die QFT auf das erste Register an
5. Miss das erste Register $x \in \mathbb{Z}_M$ und finde rationale Approximierung a/b für die Zahl $\frac{x}{M}$, falls $A^b = 1(\%N)$, gebe b aus

Quantenquark
Marie Hoffmann
Einleitung
Quanten
Quantenwelt
Superpositionen
Qubits
QuRechner
Funktionen
Gatter
Algorithmen
Faktorisierung
QFT
Fazit
Komplexität
Simulation
Quellen

Algorithmus

1. QFT der ersten m Qubits
2. $|x\rangle|y\rangle \mapsto |x\rangle|y \oplus (A^x(\%N))\rangle$
3. y_0 aus Messung von 2. Register
4. QFT auf ersten m Qubits
5. Messung auf erstem Register

Zustand, initial: $|0^{m+n}\rangle$

1. $\frac{1}{\sqrt{M}} \sum_{x \in \mathbb{Z}_M} |x\rangle|0^n\rangle$
2. $\frac{1}{\sqrt{M}} \sum_{x \in \mathbb{Z}_M} |x\rangle|A^x(\%N))\rangle$
3. $\frac{1}{\sqrt{K}} \sum_{l=0}^{K-1} \underbrace{|x_0 + lr\rangle}_{\text{stark period. Signal}} |y_0\rangle$, mit
   $K = \lfloor (M - 1 - x_0)/r \rfloor$
4. $$\frac{1}{\sqrt{MK}} \Big(\sum_{x \in \mathbb{Z}_n} \sum_{l=0}^{K-1} \omega^{(x_0+lr)x} |x\rangle \Big) |y_0\rangle$$

Stärker formuliert (*strong form of CT thesis*)

Jedes physikalisch realisierbare Rechenmodell kann von einer TM mit höchstens polynomiellen Aufwand simuliert werden.

Realisierbarkeit von $\mathcal{Q}$

Nur wenn Bauanleitung für $\mathcal{Q}$ vorhanden

$\Rightarrow$ Entscheidung treffen, ob $\mathcal{Q}$ effizient simulierbar durch TM

Stärker formuliert (*strong form of CT thesis*)

Jedes physikalisch realisierbare Rechenmodell kann von einer TM mit höchstens polynomiellen Aufwand simuliert werden.

Realisierbarkeit von $\mathcal{Q}$

Nur wenn Bauanleitung für $\mathcal{Q}$ vorhanden

$\Rightarrow$ Entscheidung treffen, ob $\mathcal{Q}$ effizient simulierbar durch TM

Ja

$\Rightarrow$ TM bleibt bisher mächtigstes Rechenmodell

Nein

$\Rightarrow$ CT-These widerlegt

$\Rightarrow$ Verschlüsselungsalgorithmen der Klasse QMA[a] müssen her

[a] analog zu NP für TMs

Und wann gibt's den ersten Quantenrechner bei Saturn?

Steuerung von Qubits

Quantenquark

Marie Hoffmann

Einleitung

Quanten
Quantenwelt
Superpositionen
Qubits

QuRechner
Funktionen
Gatter

Algorithmen
Faktorisierung
QFT

Fazit
Komplexität
Simulation

Quellen

Kandidaten

Ionenfallen optische/magnetische Felder um Ionen einzufangen

Optische Fallen Lichtwellen um Partikel einzufangen und zu steuern

Quantenpunkte verwenden Halbleitermaterialen, die Elektronen enthalten

Stickstoff-Fehlstellen im Diamanten (NV-Zentren), eingeschlossenes Stickstoffatom

Simulation von Quantenrechnung

Quantenquark

Marie Hoffmann

Einleitung

Quanten
Quantenwelt
Superpositionen
Qubits

QuRechner
Funktionen
Gatter

Algorithmen
Faktorisierung
QFT

Fazit
Komplexität
Simulation

Quellen

- Quantenrechnungen können auf einem herkömmlichen PC simuliert werden, siehe C-Bibliothek Libquantum
- $\Rightarrow$ Halteproblem auch mit Quantencomputer nicht lösbar
- Klasse der Simulationen auf einer TM ist **PSPACE**, also

Theorem

BQP $\subseteq$ **PSPACE** Idee: Berechnung der Koeffizienten mittels Rekursion (Wiederverwendung von Speicherplatz)

Shor:1994 P. W. Shor, "Polynomial Time Algorithms For Prime Factorization And Discrete Logarithms On A Quantum Computer," SIAM J. Sci. Statist. Comput. **26** (1997) 1484 [arXiv:quant-ph/9508027].