Seminar über Algorithmen SS 2010
Quantenrechner

Dozent: Prof. Dr. Helmut Alt, Vortragende: Marie Hoffmann*

Freie Universität Berlin

26. Juli 2010

1 Church-Turing-These

Die CT-These besagt, dass jede intuitiv berechenbare Funktion von einer Turingmaschine (TM) simuliert werden kann. Dies kann noch stärker formuliert werden[1]:

These 1 *Jedes physikalisch realisierbare Rechenmodell kann von einer TM mit höchstens polynomiellen Aufwand simuliert werden.*

Frage: Gilt das auch für Quantencomputer?

Zumindest weiß man, dass ein Quantencomputer die Primzahlfaktorisierung, die ein NP-vollständiges Problem ist, in polynomieller Zeit lösen kann. Wenn gezeigt werden könnte, dass es *keinen polynomiellen Faktorisierungsalgorithmus* für TMs[2] geben kann, und dass Quantencomputer physikalisch realisierbar sind, dann wäre die stark formulierte CT-These falsch.
In den folgenden Kapiteln wird auf die Eigenheiten von Quanten eingegangen, die als Bausteine des physikalisch realisierten Quantencomputers erst das quasi-parallele Rechnen ermöglichen. Es werden auch Grenzen aufgezeigt, die sich auf die Programmierweise auswirken. Das letzte Kapitel widmet sich dem Primzahlfaktorisierungsalgorithmus von Shor.

2 Quanten

2.1 Eigenheiten

Ein Quant ist eine **nicht teilbare Portion** bezüglich einer **physikalischen Größe**, meist Energie. Man spricht von der Quantelung einer physik. Größe. Ein Quant kann nur als Ganzes verändert oder abgegeben werden. Beispiele für Quanten:

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[3]

vier Quantenzahlen des Elektrons

- **Hauptquantenzahl**: Schale $n \in \{1, 2, 3, ...\}$, welche beschreibt auf welcher Schale sich ein Elektron mit hoher Wahrscheinlichkeit aufhält

*marie.hoffmann@fu-berlin.de

[1] *strong Church-Turing Thesis*, Verschärfung der physikalischen Formulierung durch David Deutsch [1985]

[2] weder deterministische noch probabilistische TMs

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

- **Nebenquantenzahl**: Orbital $l \in \{0, 1, 2, ..., n-1\}$, welche die Form des Orbitals beschreibt
- **Magnetische Quantenzahl des Drehimpuls**: $m \in \{-l, -l+1, ..., l\}$
- **Spinquantenzahl**: Orientierung des Spins $s_z \in \{-\frac{1}{2}, \frac{1}{2}\}$

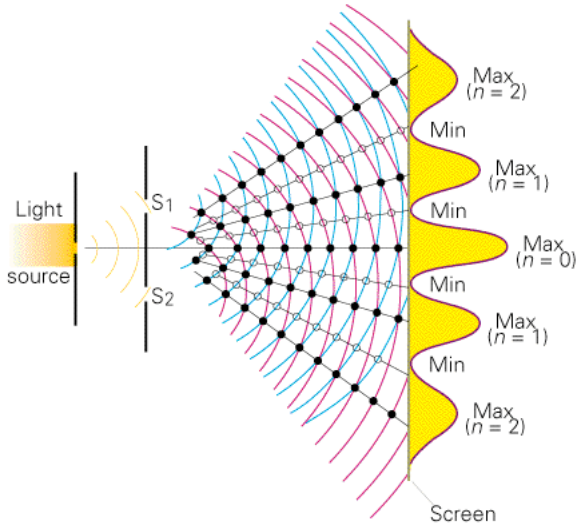
Das Beispiel des Drehimpulses verdeutlicht, dass es sich bei Quanten nicht um ein "festes" Teilchen handeln muss.

2.2 Welle-Teilchen-Dualismus

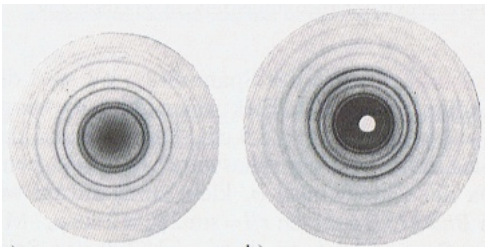
Es ist die besondere Eigenschaft Welle-Teilchen-Dualismus, die es dem Quant ermöglicht, in mehreren Zuständen zugleich zu sein. Zum Zeitpunkt der Messung wird es jedoch stets in nur einem Zustand anzutreffen sein. Der Welle- und Teilchencharakter von Photonen kann an zwei Experimente studiert werden: dem Doppelspaltexperiment und der Ablösearbeit beim photoelektrischen Effekt.

2.2.1 Doppelspaltexperiment

Eine Lichtquelle wird in einem gewissen Abstand zu einer Platte aufgestellt und bestrahlt diese. Die Platte ist mit zwei Spalten versehen, durch die Licht hindurchtreten kann. Weiter dahinter liegt eine Photoplatte auf, die die auftretenden Intensitäten aufzeichnet. Öffnet man nur einen Spalt, so tritt die stärkste Intensität senkrecht über dem Spalt auf und wird nach außen hin schwächer, entsprechend der Gaußschen Nornmalverteilung.
Öffnet man beide Spalte, so wird nicht die Summe der Interferenzen gemessen, sondern es ergeben sich charakteristische Beugungsbilder, die sich nur durch das Wirken von Beugung und Interferenz erklären lassen: An beiden Spalten werden die Wellen abgelenkt und treffen auf die Photoplatte an verschiedenen Stellen mit unterschiedlich versetzten Wellen aufeinander. Beträgt die Versetzung ein Vielfaches der ganzen Amplitude, so addieren sich die Intensitäten (konstruktive Interferenz). Treffen zwei Lichtwellen um genau die Hälfte einer Amplitude versetzt aufeinander, so löschen sie sich aus (destruktive Interferenz).



(a) Lichtbestrahlung eines Doppelspalts



(b) Beugungsbilder, punktförmige Öffnungen

Bringt man je zwei Sensoren am Spalt an, in der Hoffnung den gleichzeitigen Eintritt zweier Quanten zu detektieren, so kollabiert die Welle. Stets wird nur ein Teilchen stochastisch verteilt detektiert.
Schlussfolgerung: Die Gleichzeitigkeit der Quantenwelle lässt sich nicht messen. Jede Messung ist eine Störung und führt zum Kollaps des Systems, die Teilchen verhalten sich nur noch stochastisch, wie erwartet.

2.2.2 Photoelektrischer Effekt

Bisher haben wir gesehen, dass Quanten sich wellenförmig gemäß den ihr eigenen Wellenlängen fortbewegen. Wir wissen, dass Lichtquanten in beliebige, kontinuierliche Frequenzen versetzt werden können. Jedoch können sie ihre Lichtenergie nur portionsweise abgeben. Beim photoelektrischen Effekt wird dies evident. Um Photoelektronen aus einer Metallplatte abzulösen, muss eine bestimmte Energie W_a aufgebracht werden. Diese ist abhängig von der Art

des Metalls; bei Edelmetallen ist sie wegen der vollbesetzten, äußeren Schale höher.
Bestrahlt man die Platte mit Licht bestimmter Wellenlänge und Intensität um Elektronen herauszuschießen, so müsste es genügen die Intensität zu erhöhen, also mehr Lichtquanten auszusenden, bis die nötige Ablöseenergie erreicht ist, wenn die Energie des Lichtquants in seiner Wellenamplitude steckt. Dem ist aber nicht so, eine Erhöhung der Intensität löst nicht mehr Elektronen heraus als zuvor. Erst die Eröhung der Frequenz hat den erwünschten Effekt. Die Ablöseenergie ist proportional zur Frequenz: $W_{phot} = h \cdot f$. Damit kann die Energie des Lichtquants nur portionenweise abgegeben werden.

3 Qubits

Zur Speicherung benötigen wir dem Bit analoge Teilchen: die **Qubits**. Ihre Zustände werden durch das **Superpositionsprinzip** beschrieben.

3.1 Prinzip der Superposition

Zwei beliebige[4] Zustände eines Quants werden als Grundzustände festgesetzt und bezeichnet mit $|0\rangle$ und $|1\rangle$. Beide Zustände sind ständig überlagert, bzw. interferieren mit den ihnen zugordneten Wellenlängen α_0 und α_1. Der Raum der Zustände ergibt sich allen Linearkombinationen der Form $\alpha_0|0\rangle + \alpha_1|1\rangle$ mit Amplituden $\alpha_{0/1} \in \mathbb{C}$ und der Invariante $|\alpha_0|^2 + |\alpha_1|^2 = 1$
Niemals wird man die gleichzeitigige Existenz der Superpositionen messen können, sondern das Qubit mit Wahrscheinlichkeit α_0^2 im Zustand $|0\rangle$ und mit Wahrscheinlichkeit α_1^2 im Zustand $|1\rangle$ antreffen.

Analog ein **Zwei-Qubit-System**: zwei miteinander verschränkte Qubits erzeugen vier Basiszustände, die je nach vorgenommener Manipulation mit gewissen Amplituden auftreten:

$$\alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle \text{ und der Invariante } \sum_{b_0,b_1} |\alpha_{b_0 b_1}|^2 = 1$$

Wie im 1-Qubit-System ist die Wahrscheinlichkeit das System im Zustand $b_0 b_1$ anzutreffen gleich $\alpha^2_{b_0 b_1}$. Unter Missachtung des Normalisierungsfaktors schreiben wir das 2-Qubit-System um als ein Produkt zweier 1-Qubit-Systeme:

$$\underbrace{(|0\rangle + |1\rangle)}_{b_0}\underbrace{(|0\rangle + |1\rangle)}_{b_1} \text{ mit}$$

3.2 Geometrische Veranschaulichung

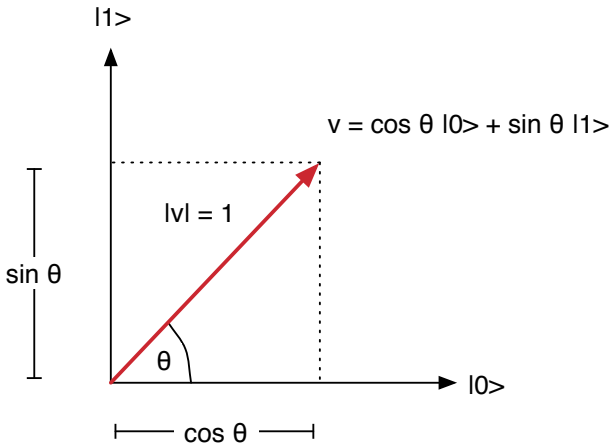


Abbildung 1: geometrische Veranschaulichung

[4] zueinander orthogonale

Sei v der Zustandsvektor eines 1-Qubit-Systems[5] und θ der Winkel zur $|0\rangle$-Achse, so lassen sich die Zustandswahrscheinlichkeiten nach den Elementarsätzen der Geometrie mit $\cos^2\theta|0\rangle$ und $\sin^2\theta|1\rangle$ bestimmen (siehe Abbildung 1). Wir wählen diese vereinfachte Darstellung ohne die Imaginärkomponente um eine Variante des Einstein-Podosky-Rosen-Paradoxons im nachfolgenden Abschnitt leichter rechnerisch nachvollziehen zu können.
Unter Hinzunahme der komplexen Zahlebene erhielten wir eine Kugel. Diese Darstellung wurde vom Physiker Felix Bloch entwickelt und nach ihm benannt: die Bloch-Kugel.

3.3 EPR-Paradoxon

Das Einstein-Podosky-Rosen-Paradoxon (EPR) ist ein Gedankenexperiment [1935], welches verdeutlicht wie mithilfe eines gemeinsamen Quantensystems zwei entfernte Systeme ohne Zeitverzögerung kommunizieren können. Dies widersprach Einsteins Axiom der speziellen Relativitätstheorie, nach der nichts schneller als Licht reisen kann. John Bell [1964] machte daraus ein Experiment, welches inzwischen nachgestellt worden ist: das Paritätsspiel.

3.4 Paritätsspiel

Die Teilnehmer des Spiels sind zwei Spieler Alice (A) und Bob (B) und ein Spielleiter. Zum Vergleich werden zwei Varianten durchgespielt: eine ohne und eine mit einem gemeinsamen 2-Qubit-System. Der Spielablauf ist wie folgt:

1. Spielleiter wählt zufällig zwei Bits $x, y \in_R \{0,1\}]$
2. x wird Alice und y Bob gezeigt[6]
3. Alice und Bob entscheiden[7] 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

Tabelle 1: Wahrheitstabellen für AND und XOR

Versuchsaufbau 1 kein gemeinsames Qubit-System Ein Blick auf die Wahrheitstabelle zeigt, dass mit die beste Strategie[8] hier wäre, unabhängig vom erhaltenen Bit eine Null zu senden, denn in $\frac{3}{4}$ aller Fälle ergibt die Konjunktion von x und y Null. Das exklusive Oder der beiden gesendeten Nullen ist ebenfalls Null, beide gewinnen. Mit der zuvor überlegten Strategie liegt die Gewinnwahrscheinlichkeit bei 75%.

Versuchsaufbau 2 Beide Teilnehmer teilen sich ein 2-Qubit-System, welches sie initial in den Zustand

$$z_{EPR} = |00\rangle + |11\rangle$$

versetzen[9]. Mit der Wahrscheinlichkeit $\frac{1}{2}$ treffen sie es zum Zeitpunkt der Messung entweder im Zustand $|00\rangle$ (beide Bits auf Null) oder im Zustand $|11\rangle$ (beide Bits auf Eins) an. Bevor sich beide Spieler trennen, nimmt jeder ein Qubit an sich. Alice erhält das erste Qubit q_A und Bob das zweite Qubit q_B. Beide einigen sich auf folgende Strategie:

1. Wenn Alice ein $x = 1$ erhält, dann rotiert sie ihr Qubit um $\frac{\pi}{8}$ im mathematisch positiven Sinne.
2. Wenn Bob ein $y = 1$ erhält, dann rotiert er sein Qubit um $-\frac{\pi}{8}$.
3. Erhalten beide eine Null ($x = 0 \vee y = 0$), dann tun sie nichts.

[5] Koeffizienten aus $\mathbb{R}$
[6] keiner kennt das andere Bit
[7] ohne Informationsaustausch mit dem anderen Spieler
[8] Alice und Bob dürfen sich vorher absprechen
[9] Normalisierungsfaktor $\frac{1}{\sqrt{2}}$ ist beiseite gelassen

4. Die Antworten fallen so aus: Beide nehmen an ihrem Qubit $q_{A,B} = \alpha_{A/B,0}|0\rangle + \alpha_{A/B,1}|1\rangle$ eine Messung vor und antworten mit korrespondierenden Wahrscheinlichkeiten $f(q_{A,0}) = \alpha_{A,0}^2$ für $|0\rangle$ und $f(q_{A,1}) = \alpha_{A,1}^2$ für $|1\rangle$, B analog.

Bezogen auf die Aktionen von Bob und Alice unterscheiden wir drei Fälle:

1. $p_{xy}(x = y = 0) = 1/4$: keiner rotiert
2. $p_{xy}(x \neq y) = 1/2$: einer rotiert
3. $p_{xy}(x = y = 1) = 1/4$: beide rotieren

Fall 1 Zum Zeitpunkt der Messung ist das System in einen der beiden Zustände $q_{EPR}(t) = |00\rangle \vee |11\rangle$

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

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

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

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

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

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

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

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 befindet sich das System wieder gleichwahrscheinlich in einem der beiden Grundzustände $q_{EPR}(t) = |00\rangle \vee |11\rangle$.

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

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

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 $p(x \neq y \wedge |00\rangle) = 1 \cdot \cos^2\frac{\theta}{8} + 0 \cdot sin^2\frac{\pi}{8}$

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

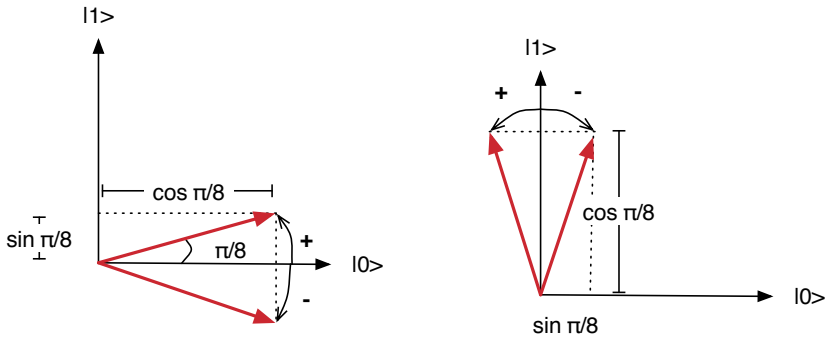


Abbildung 2: Rotationen in $|00\rangle$ und $|11\rangle$

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

Alle Koeffizienten betragen $\frac{1}{\sqrt{2}}$. Damit sind alle Zustände gleichwahrscheinlich mit Normalisierungsfaktor $(\frac{1}{\sqrt{2}} \cdot \frac{1}{\sqrt{2}})^2 = \frac{1}{4}$. Die Wahrscheinlichkeit für unterschiedliche Antworten beträgt demnach $\frac{1}{2}$.

Zusammengefasst: $\frac{1}{4} \cdot 1 + \frac{1}{2} \cdot \cos^2\frac{\pi}{8} + \frac{1}{4} \cdot \frac{1}{2} \geq 0.8$

Die Analyse zeigt, dass mit der besten Strategie (immer 0 senden) die Gewinnwahrscheinlichkeit nicht höher ist als 75% im Erwartungswert. Teilen sich beide aber ein Qubitsystem, so steigt die Wahrscheinlichkeit auf über 80%.

4 Quantenrechner

Ein Quantenrechner $\mathcal{Q}$ ist zunächst formal ein Rechenmodell bestehend aus einem Prozessor und einem m-Qubitregister aus m miteinander verschränkten Qubits, die der Invariante gehorchen. Das Register dient zur Speicherung und reflektiert zu jedem Zeitpunkt den Zustand des Quantenrechners. Der Zustandsraum sind alle Superpositionen über die Grundzustände $\{0,1\}^m = 2^m$. Der Zustandsvektor $v = \langle v_{0^m}, v_{0^{m-1}1}, ..., v_{1^m}\rangle$ mit $\sum_x |v_x|^2 = 1$ speichert die den Zuständen korrespondierenden Koeffizienten. Wie immer führt eine Messung zum Kollaps. Mit Wahrscheinlichkeit $p(|x\rangle) = v_x^2$ wird ein beliebiger möglicher Zustand vorgefunden, für die restlichen Koeffizienten ist dann $v_{x\neq y} = 0$.

Abbildung 3: Qubitregister

4.1 Quantenoperation

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

Gemäß obiger Definition kann F kann durch eine *unitäre* $2^m \times 2^m$-Matrix A beschrieben werden und hat eine Inverse.

Definition 2 (Elementaroperation) *Eine Quantenoperation[a] ist elementar, wenn sie auf höchstens* **drei** *Qubits des Registers rechnet.*

[a] oder auch mehrere Quantengatter

Analog zu den Elementargattern für herkömmliche Rechner, gibt es einen Satz von Elementargattern oder -operationen, die auf einer kleinen, konstanten Zahl von Qubits rechnen. Die Zahl drei ist hier beliebig, es könnte auch ein anderer Wert größer oder gleich 2 sein.

Definition 3 (Quantenberechnung) *Eine Quantenberechnung ist eine Sequenz von Elementaroperationen angewandt auf ein Quantenregister.*

Nun haben wir das Handwerkzeugs um die Klasse **BQP** (*bounded error quantum polynomial time*) zu definieren.

Definition 4 (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.*

4.2 No-Cloning-Theorem

Eine wichtige Einschränkung, die sich aus Ergebnissen der Quantenphysik ergeben, sind das **No-Cloning-Theorem** und dass keine neuen Qubits während des Programmierens hinzugenommen werden dürfen.

Theorem 1 (No-Cloning-Theorem) *Resultat der Quantenphysik: Das* **Kopieren** *von einem Qubit auf ein anderes ist* **nicht möglich** *ohne das ursprüngliche zu verändern.*
⇒ Kopieren ist nicht umkehrbar, also keine gültige Funktion[a]

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

[a] keine unitäre Matrix bildbar

Praktische Bedeutung des No-Cloning-Theorems: keine Einschränkung der Mächtigkeit eines Quantencomputers, jedoch Behutsamkeit beim Programmieren. In jedem Rechenschritt eines Algorithmus, sollte man wissen, wie die Wahrscheinlichkeiten der Zustände verteilt sind um ein "determiniertes" Ergebnis zu erhalten.

5 Algorithmus von Shor

Der Algorithmus von Shor löst das Ganzzahlfaktorisierungsproblem. Sei N eine gegebene, ganze Zahl, so gilt es die Menge aller Primfaktoren zu finden.
Das Problem der Primfaktorzerlegung einer Zahl N ist äquivalent zur Bestimmung **eines** Primfaktors von N. Zum Finden aller Primfaktoren kann der Lösungsalgorithmus mehrfach durchlaufen werden.

Der Algorithmus von Shor teilt sich auf in einen klassischen Teil, welcher von einem herkömmlichen Rechner nach dem Turingmaschinen-Modell berechnet werden kann und einen Quantenteil.

5.1 Klassischer Teil

Der klassische Teil reduziert das Problem des Findens **eines Primfaktors** auf die Bestimmung der **Ordnung** r. Die Ordnung ist die kleinste Anzahl von Verknüpfungen einer Zahl, die das neutrale Element einer Gruppe ergibt. Bezogen auf das Problem der Primfaktorzerlegung ist der Verknüpfungsoperator $'*'$ und das neutrale Element alle zur 1 semantisch äquivalenten Zahlen aus $\mathbb{Z}_N$.

Die eigentliche Bestimmung des kleinsten r, welches $A^r = 1 \mod N$ erfüllt, wird vom Quantenteil erledigt, welcher A und N als Eingabe erhält.

Agorithmus 1 (Algorithmus von Shor) *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 $< 3/4$

Dass für gültige Werte von A r tatsächlich die Ordnung ist, lässt sich aus den Nebenbedingungen folgern (siehe Vortrag, betrachte hierfür $(A^{r/2}-1)(A^{r/2}+1) = A^r - 1$).
$A^{r/2}-1$ und N besitzen schließlich einen gemeinsamen, nicht-trivialen Teiler, der effizient mit dem euklidischen Algorithmus ggT bestimmt werden kann. Warum aus einem zufälligen A und seiner Ordnung ein Primfaktor bestimmt werden kann und wieviel Zufallswerte in Schritt 4 verworfen werden müssen, besagen diese zwei Lemmata:

Lemma 1 *Für jede Nichtprimzahl N, die keine Primzahlpotenz ist, ist die Wahrscheinlichkeit, dass ein zufälliges X aus der Menge $\mathbb{Z}_N^* = \{X \in [N-1] : gcd(X, N) = 1\}$ eine gerade Ordnung r hat und $X^{r/2} \neq -1 \mod N$ ist wenigstens $1/4$.*

Beweis im Buch [1] Kapitel 10.6.4.

Lemma 2 *Für jedes N und Y mit $Y^2 = 1 \mod N$ und $Y \mod N \notin \{-1, +1\}$ ist $ggT(Y-1, N) \notin \{1, N\}$.*

Begründung: Nach Vorraussetzung teilt N $Y^2 - 1 = (Y-1)(Y+1)$, aber weder $(Y-1)$ noch $(Y+1)$. Folglich ist der $ggT(Y-1, N) > 1$, denn wäre er doch 1, so müsste N $(Y+1)$ teilen, was es aber nicht tut. Da $Y - 1 < N$ ist außerdem $ggT(Y-1, N) < N$.

Zusammen besagen beide Lemmata, dass zu einer gegebenen, zusammengesetzten Zahl N, die keine Primzahlpotenz ist, wir mit einer guten Wahrscheinlichkeit für ein zufälliges $A \in [N-1]$ entweder $ggT(A, N)$ oder $ggT(A^{r/2}-1, N)$ einen nicht-trivialen Faktor von N erzielen.

5.2 Quantenteil

Zur Bestimmung der Ordnung einer zufälligen Zahl $A \in [N-1]$ ist noch kein effizienter Algorithmus für TMs bekannt. Daher erledigt dies ein Quantenrechner. Herzstück des Quantenteils ist die Quanten-Fourier-Transformation (QFT) über den diskreten Zahlenraum $\mathbb{Z}_M$, welche zweimal ausgeführt wird.

5.2.1 Quanten-Fourier-Transformation über $\mathbb{Z}_M$

Die Quanten-Fourier-Transformation ist ein Algorithmus, der den Zustand $f \in \mathbb{C}^M$ eines Quantenregisters in seine Fourier-Transformation $\hat{f}$ überführt.

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

Die Fourier-Transformation ist in der Lage periodische Signale auf diskrete Werte abzubilden. Ein solches Signal kann auch eine Reihe sein, die sich nach einem bestimmten Muster bilden lässt. Bezogen auf das m-Qubit-Register bildet sie einen Zustand $|x\rangle$ auf $\omega^x = \omega^{\sum_{i=0}^{m-1} 2^i x_i}$ ab, in dem jedes Qubit der Stellen $i \in \{0, .., m-1\}$ folgendermaßen transformiert wird: $|0\rangle \mapsto |0\rangle$ und $|1\rangle \mapsto \omega^{2^i}|1\rangle$.

Lemma 3 *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 $\hat{f}(x) = \frac{1}{\sqrt{M}} \sum_{y\in\mathbb{Z}_m} \omega^{xy} f(x)$*

Begründung: Die Transformation kann auf zwei Teilprobleme von geraden und ungeraden Eingabevektoren für f zurückgeführt werden (je $M/2$), die iterativ der Fourier-Transformation unterworfen werden.

Für die Fourier-Transformation eines ganzen Registers sind nur zwei elementare Rechenoperationen notwendig, welche nach dem Muster

$$R_{m-1}S_{m-2,m-1}R_{m-2}S_{m-3,m-1}S_{m-3,m-2}R_{m-3}...R_1S_{0,m-1}S_{0,m-2}...S_{0,2}S_{0,1}R_0$$

angewandt werden. Insgesamt werden $m(m-1)/2$ Elementaroperation ausgeführt bei einem Eingabevektor der Länge m.

Hadamard-Gatter , operierend auf dem j-ten Qubit

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

Phasengatter , operierend auf Qubits j und k

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

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

Für eine detaillierte Erklärung wie diese Gatter die Quanten-Fourier-Transformation für ein Signal durchführen, das von $|a\rangle$ nach $|b\rangle$ reicht, sei auf das Originalpaper von Peter W. Shor [3] Kapitel 4 verwiesen.

5.2.2 Algorithmus

Agorithmus 2 (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*

Bemerkung: es handelt sich im obigen Algorithmus um **ein** Register, welches lediglich gedanklich in zwei Register aufgeteilt wird.

1. Nach der QFT auf den ersten m Qubits befindet sich das System im Zustand
$$\sum_{x=0}^{2^m-1} |x, f(x)\rangle$$
2. Die Messung des zweiten Registers führt auf einen Zufallswert y_0 von f, welcher an sich unbedeutend ist. Wesentlich ist die Auswirkung der Messung. Sie bewirkt, dass das System nur noch aus Werten für x und $f(x)$ superponiert mit Amplituden, die von x abhängen.
3. x lässt sich als Reihenentwicklung $x = x_0 + r \cdot l$ darstellen. Das Signal dieser Reihe wird durch die letzte QFT detektiert durch Transformation der Amplitude in ein scharfes Signal.

A Anhang

A.1 Euklidischer Algorithmus zur Bestimmung des ggT

Eingabe zwei natürliche Zahlen

Ausgabe größter gemeinsamer Teiler

Listing 1: euclid

```
1  EUCLID(a, b):
2      if a == 0:
3          return b
4      while (b ≠ 0):
5          if a > b:
6              a = a-b
7          else
8              b = b-a
9      return a
```

B Quellen

Literatur

[1] Sanjeev Arora, Boaz Barak, *Computational Complexity – A Modern Approach*, Cambridge University Press, 2009

[2] Franz Dorn, Friedrich Bader, *Physik, Oberstufe Gesamtband 12/13*, Schroedel, 1986

[3] Peter W. Shor, *Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*, 1996