Quanten Fourier Transformation & Shors Faktorisierungs Algorithmus

Peter Kaufmann

Universität Siegen

4. Juli 2006

Inhaltsverzeichnis

1. Quantenfouriertransformation
   - Rechnen mit Qubits
   - diskrete Fourier Transformation
   - Quanten Fourier Transformation
2. Shor Algorithmus
   - mathematische Grundlagen
   - Quantenalgorithmus

Qubit

Definition: Qubit

Ein Qubit $|\psi\rangle$ ist ein Quantensystem mit nur zwei linear unabhängigen Basiszuständen $|0\rangle$ und $|1\rangle$:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \text{ mit } |\alpha|^2 + |\beta|^2 = 1$$

$|\psi\rangle$ ist ein Element des zweidimensionalen Hilbertraumes $\mathcal{H}_2$, der von den beiden Basiszuständen aufgespannt wird.
Mögliche physikalische Realisierungen:

- Spin
- (zwei) Energieniveaus eines Ions
- Polarisation von Photonen
- ...

Quantenregister

Definition: Quantenregister

Ein Quantenregister setzt sich aus L Qubits zusammen:

$$|a\rangle = |a_{L-1}, a_{L-2}, ..., a_0\rangle \text{ mit } a_j \in \{0, 1\}$$

$$a = \sum_{j=0}^{L-1} a_i 2^i \Rightarrow 0 \leq a < 2^L$$

$|a\rangle$ beschreibt einen Punkt im 2^L dimensionalen Hilbertraum: $|a\rangle \in \mathcal{H}_2^L$. Die 2^L Basisvektoren lassen sich von 0 bis $2^L - 1$ nummerieren $|0\rangle, |1\rangle, \ldots |2^L - 1\rangle$.

Quantengatter

Aus der Schrödingergleichung $i\hbar\frac{d}{dt}|\psi\rangle = H|\psi\rangle$ folgt der zu H gehörige Zeitenentwicklungsoperator $U(t)$:

$$|\psi(t)\rangle = U(t)\psi(t=0)$$

U ist unitär:

$$1 = \langle\psi(t)|\psi(t)\rangle = \langle U(t)\psi|U(t)\psi\rangle = \langle\psi|U^\dagger(t)U(t)|\psi\rangle$$

$$\Rightarrow U^\dagger(t)U(t) = 1$$

Definition: Quantengatter

Unter einem Quantengatter versteht man die unitäre Operation, die mit Hilfe eines geigneten Hamiltonenoperators den Zustand eines Quantengatter nach einer gewissen Zeit von einem in einen anderen Zustand überführt.

Hadamard Gatter

Das Hadamard Gatter

Definition: Hadamard Gatter

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

operiert auf das $j$te Qubit des Quantenregisters und vermittelt eine unitäre Transformation in der Basis $|a_j\rangle$.

Beispiel: $A_j A_j |0\rangle$

$$A_j \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) = |0\rangle$$

kontrolliertes Rotationsgatter

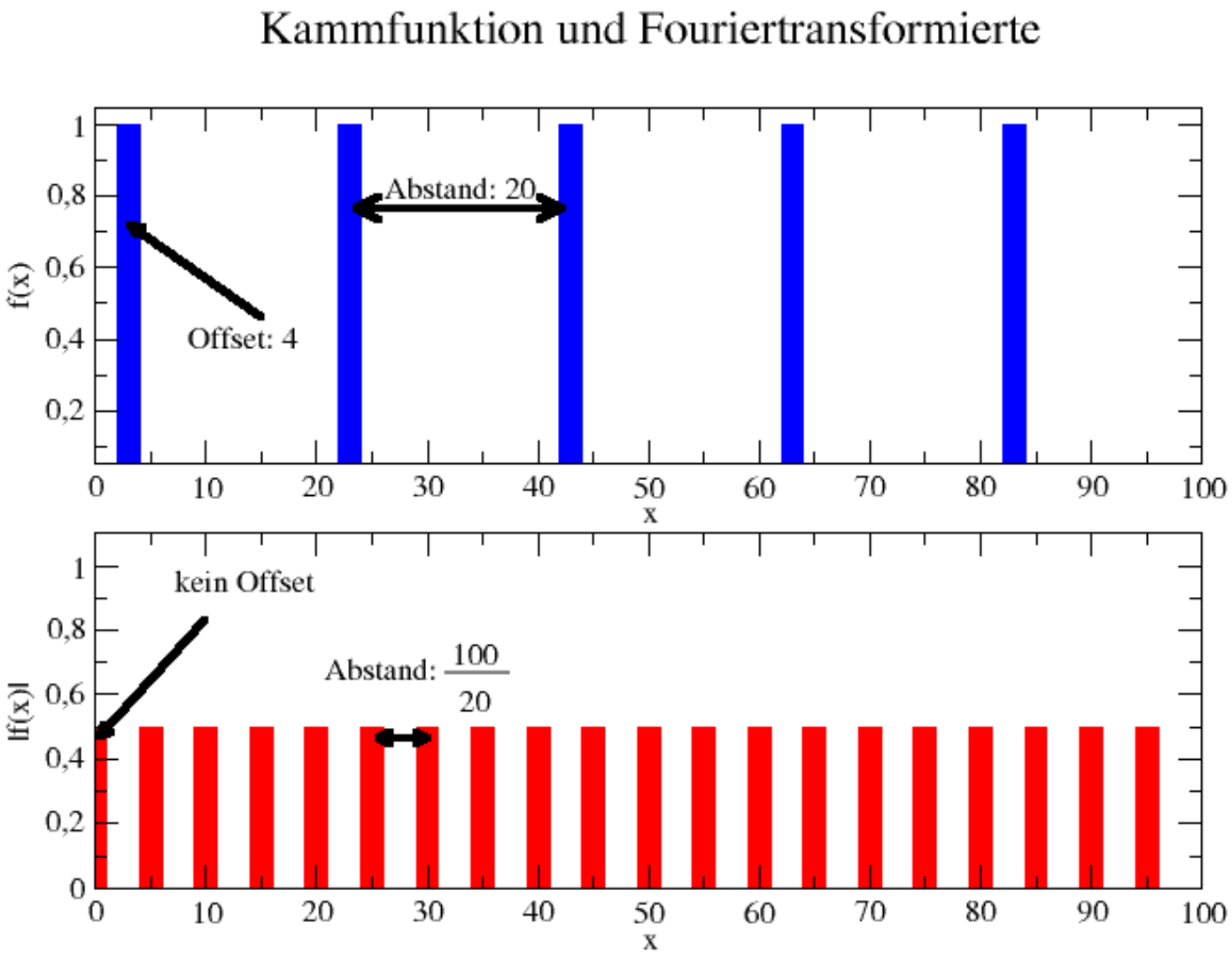
Das B_{jk} Gatter

Definiton: kontrolliertes Rotationsgatter

$$B_{jk} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{i\Theta_{jk}} \end{pmatrix} \text{ mit } \Theta_{jk} = \frac{\pi}{2^{k-j}}$$

operiert auf die Qubits j und k und ist in der Basis $|a_j, a_k\rangle$ definiert.
B_{jk} liefert im Fall $|a_j = 1, a_k = 1\rangle$ einen Phasenfaktor Θ, der von dem Abstand der beiden Qubits im Quantenregister abhängt.

Diskrete Fourier Transformation



Quanten Fourier Transformation

Die Quanten Fourier Transformation (QFT) wird analog zur diskreten Fouriertransformation (DFT) definiert:

Definition: QFT

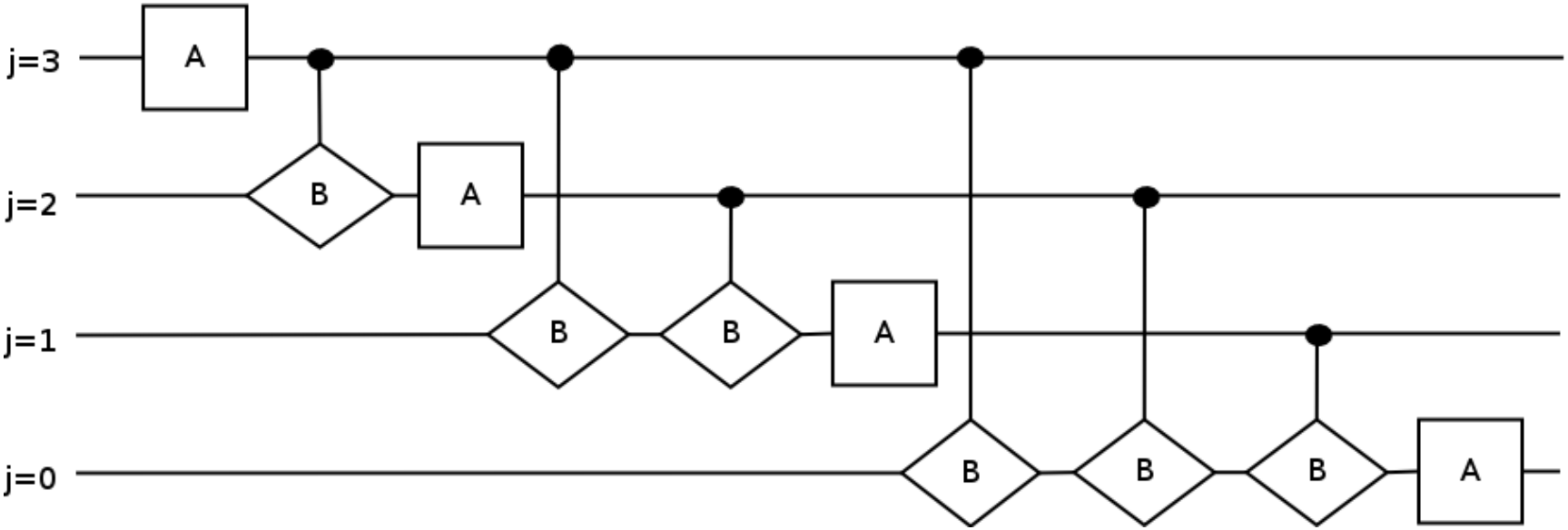
$$QFT_q : |a\rangle \rightarrow \frac{1}{\sqrt{q}} \sum_{c=0}^{q-1} e^{2\pi i \frac{ac}{q}} |c\rangle$$

Also:

$$QFT_q : \sum_a f(a)|a\rangle \rightarrow \sum_c \tilde{f}(c)|c\rangle \text{ mit } \tilde{f}(c) = \frac{1}{\sqrt{q}} \sum_a e^{2\pi i \frac{ac}{q}}$$

QFT_q Quantengatter

Die Quantenfouriertransformation für $L = 4$ wird durch das Quantengatter



vermittelt. Das Ergebnis ist allerdings „im Register falsch herum“. Allgemein gilt:

$$QFT_{2^L} = (A_{L-1})\,(B_{L-2,L-1}A_{L-2})\ldots(B_{0,L-1}\ldots B_{0,2}B_{0,1}A_0)$$

Quanten Fourier Transformation

Beispiel: Quantengatter für $L = 2$

- Hadamard Gatter A_1:

$$A_1|a_1\rangle = \frac{1}{\sqrt{2}} \sum_{k=0}^{1} (-1)^{a_1 k} |k\rangle = \frac{1}{\sqrt{2}} \left(|0\rangle + e^{i\pi a_1}|1\rangle\right)$$

- Rotationsgatter $B_{1,0}$:

$$B_{1,0} \frac{1}{\sqrt{2}} \left(|0\rangle + e^{i\pi a_1}|1\rangle\right) \otimes |a_0\rangle = \frac{1}{\sqrt{2}} \left(|0\rangle + e^{i\pi(a_1 + \frac{a_0}{2})}|1\rangle\right) \otimes |a_0\rangle$$

- Hadamard Gatter A_0:

$$A_0(\dots) = \frac{1}{2} \left(|0\rangle + e^{i\pi(a_1 + \frac{a_0}{2})}|1\rangle\right) \otimes \left(|0\rangle + e^{i\pi a_0}|1\rangle\right)$$

Beweis: QFT_q

- Vorfaktor: L Anwendungen von A_j liefern einen Faktor $\left(\frac{1}{\sqrt{2}}\right)^L = \frac{1}{\sqrt{2^L}} = \frac{1}{\sqrt{q}}$
- Phase:
  - A_j: Für $a_j = b_j = 1$ liefert A_j einen Phasenfaktor π
  - B_{jk}: Für $a_j = b_k = 1$ liefert B_{jk} einen Phasenfaktor $\frac{\pi}{2^{k-j}}$

$$\varphi = \sum_{j=0}^{L-1} \pi a_j b_j + \sum_{j=0}^{L-1} \sum_{k=j+1}^{L-1} \frac{\pi}{2^{k-j}} a_j b_k = \sum_{j=0}^{L-1} \sum_{k=j}^{L-1} \frac{\pi}{2^{k-j}} a_j b_k$$

Mit $b_k = c_{L-1-k}$ folgt weiter:

$$\varphi = \sum_{j=0}^{L-1} \sum_{k=j}^{L-1} \frac{\pi}{2^{k-j}} a_j c_{L-1-k}$$

Beweis: QFT_q

Subsitution: $\tilde{k} = L - 1 - k$

$$\varphi = \sum_{j=0}^{L-1} \sum_{\tilde{k}=0}^{L-1-j} 2\pi \frac{2^j 2^{\tilde{k}}}{2^L} a_j c_{\tilde{k}}$$

$$\tilde{\varphi} = \underbrace{\frac{2\pi}{2^L}}_{=\frac{2\pi}{q}} \underbrace{\sum_{j=0}^{L-1} 2^j a_j}_{=a} \underbrace{\sum_{\tilde{k}=0}^{L-1} 2^{\tilde{k}} c_{\tilde{k}}}_{=c}$$

$$= 2\pi \frac{ac}{q}$$

Primfaktoren und Modulo

Die Primfaktorzerlegung

$$x = p_1^{x_1} p_2^{x_2} \dots p_n^{x_n}$$

jeder natürlichen Zahl x ist eindeutig (Fundamentalsatz der Arithmetik).
Die Operation *Modulo* liefert den Rest der Ganzahldivision zweier Zahlen. Zwei Zahlen nennt man *kongruent bzgl. eines Moduls*, wenn die Operation Modulo den selben Wert liefert.

Beispiel: Rechnung kongruent 7

$$\text{mod}\ (19, 7) = 5 \wedge \quad \text{mod}\ (5, 7) = 5$$

$$\Rightarrow 19 \equiv 5 \pmod 7$$

Primfaktorzerlegung

Wähle $c > N$ und $d > N$, die nicht durch durch N teilbar sind, und für ein beliebiges m die Gleichung

$$\frac{cd}{N} = m$$

erfüllen.
Alle Primfaktoren von N lassen sich somit im obigen Bruch gegen Primfaktoren von c und d kürzen:

$$\frac{\prod_i p_i^{c_i} \prod_j p_j^{d_j}}{\prod_k p_k^{N_k}} = \prod_l p_l^{m_l}$$

Primfaktorzerlegung

Beispiel: Faktoren von $N = 21$

$$\frac{6 \cdot 35}{21} = 10$$

$$\frac{2 \cdot 3 \quad \cdot \quad 5 \cdot 7}{3 \cdot 7} = 2 \cdot 5$$

- Mit ggT(c,N) und ggT(d,N) sind zwei Faktoren von N bekannt.
- Sukzessive Anwendung des Verfahrens liefert die Primfaktorzerlegung von N.
- Die geignete Wahl von c und d ist aber i.A. schwierig.

Faktorisierung $\longrightarrow$ Periodensuche

Wähle ein (zufälliges) $a \in \mathbb{N}$ mit $1 < a < N$ mit $ggT(a, N) = 1$.
Definiere die Funktion

$$f(x) := a^x \mod N$$

und ihre Peridode r

$$f(x + r) = f(x), \quad r \text{ minimal}$$

Faktorisierung $\longrightarrow$ Periodensuche

Aus $f(x+r) \equiv f(x) \pmod{N} \Leftrightarrow a^{x+r} \equiv a^x \pmod{N}$ folgt $a^r \equiv 1 \pmod{N}$ und somit

$$a^r - 1 \equiv 0 \pmod{N}$$

Falls r gerade ist und $a^{\frac{r}{2}} + 1 \not\equiv 0 \pmod{N}$ gilt:

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

$$\Rightarrow \exists m \in \mathbb{N} : \frac{(a^{\frac{r}{2}} + 1)(a^{\frac{r}{2}} - 1)}{N} = m$$

- $ggT(a^{\frac{r}{2}} + 1, N)$ und $ggT(a^{\frac{r}{2}} - 1, N)$ sind nicht triviale Faktoren von N.

Periodenbestimmung per Quantenalgorithmus

Wir haben die Faktorisierung von N auf die Suche nach der Periode von $f(x)$ zurückgeführt.

- Die Bestimmung der Periode r von $f(x)$ ist i.A. schwierig.
- Im Prinzip kann die Periode aus vielen Wertepaaren $(x_i, f(x_i))$ abgelesen werden.

Periodensuche mit dem Quantencomputer

Idee: *Berechne alle Wertepaare* $(x_i, f(x_i))$ *parallel und lese die Periode* r *von* $f(x)$ *geschickt ab.*
Verwende zwei Quantenregister mit den Zuständen $|\phi\rangle \in \mathcal{H}_2^n$ $(q = 2^n)$ und $|\chi\rangle \in \mathcal{H}_2^m$ $(m \in \mathbb{N} : 2^m \geq N)$. Der Gesamtzustand des Systems ist:

$$|\psi\rangle = |\phi\rangle|\chi\rangle \in \mathcal{H}_2^n \otimes \mathcal{H}_2^m$$

Beispiel: Shor Algorithmus für $N = 15$

Zu faktorisieren:

$$N = 15$$

Mögliche Werte für a: $a \in \{2, 4, 7, 8, 11, 13, 14\}$. Wähle

$$a = 11 \quad (\Rightarrow f(x) = 11^x \mod N)$$

$n = 3$ und $m = 4$.

Initalisierung

Bring das erste Register in die gleichgewichtige Superposition aller Basiszustände:

$$|\psi\rangle = \frac{1}{\sqrt{q}} \sum_{x=0}^{q-1} |x\rangle|0\rangle$$

Beispiel: Shor Algorithmus für $N = 15$

$$|\psi\rangle = \frac{1}{\sqrt{8}} \left(|0\rangle + |1\rangle + |2\rangle + \cdots + |7\rangle\right)|0\rangle$$

Berechnung von $f(x)$ im zweiten Register

Berechne $f(x)$ im zweiten Register:

$$|\psi\rangle = \frac{1}{\sqrt{q}} \sum_{x=0}^{q-1} |x\rangle |a^x \mod N\rangle$$

- Messung im zweiten Register: $y = a^l \mod N$.
- Die Messung selektiert im ersten Register Werte: $x = l, l+r, l+2r, \ldots, l+Ar$ mit $A \leq \frac{q-1-l}{r} \Rightarrow A = \lfloor \frac{q-l}{r} \rfloor$:

$$|\phi\rangle = \frac{1}{A+1} \sum_{j=0}^{A} |jr+l\rangle$$

Berechnung von $f(x)$ im zweiten Register

Beispiel: Shor Algorithmus für $N = 15$

$$|\psi\rangle = \frac{1}{\sqrt{8}}\left(|0\rangle|1\rangle + |1\rangle|11\rangle + |2\rangle|1\rangle + \cdots + |6\rangle|1\rangle|7\rangle|11\rangle\right)$$

$$|\psi\rangle = \frac{1}{\sqrt{8}}\left(\left[|0\rangle + |2\rangle + |4\rangle + |6\rangle\right]|1\rangle + \left[|1\rangle + |3\rangle + |5\rangle + |7\rangle\right]|11\rangle\right)$$

Nach der Messung von $y = 11$:

$$|\psi\rangle = \frac{1}{2}\left(|1\rangle + |3\rangle + |5\rangle + |7\rangle\right)|11\rangle$$

Berechnung von $f(x)$ im zweiten Register

Vereinfachung

Um die folgenden Erläuterungen einfacher zu halten nehmen wir an, daß q ein Vielfaches von r ist:

$$A = A = \lfloor \frac{q-l}{r} \rfloor = \frac{q}{r} - 1$$

$$|\phi\rangle = \sqrt{\frac{r}{q}} \sum_{j=0}^{\frac{q}{r}-1} |jr+l\rangle = \sum_{x=0}^{q-1} g(x)|x\rangle$$

Mit $g(x) = \sqrt{\frac{r}{q}}$ falls $(x-l)$ Vielfaches von r, sonst $g(x) = 0$.

Quantenfouriertransformation im ersten Register

Wende die QFT auf das erste Register an:

$$QFT_q|\phi\rangle = \sum_{c=0}^{\frac{q}{r}-1} \tilde{g}(c)|c\rangle$$

Die Amplituden $\tilde{g}(c)$ sind die Fouriertransformierten von $g(x)$:

$$\tilde{g}(c) = \frac{\sqrt{r}}{q} \sum_{j=0}^{\frac{q}{r}-1} \exp\left(\frac{2\pi i(jr+l)c}{q}\right)$$

$$= \frac{\sqrt{r}}{q} \underbrace{\sum_{j=0}^{\frac{q}{r}-1} \exp\left(\frac{2\pi ijrc}{q}\right)}_{\text{geom. Reihe}} \underbrace{exp\left(2\pi i\frac{lc}{q}\right)}_{\text{Phase}}$$

Quantenfouriertransformation im ersten Register

Auswertung der geom. Reihe:

$$\sum_{j=0}^{\frac{q}{r}-1} \exp\left(\frac{2\pi ijrc}{q}\right) = \frac{\exp\left(2\pi ic\right)-1}{\exp\left(2\pi i\frac{rc}{q}\right)-1} = \begin{cases} \frac{q}{r} & \text{für} \quad c = d\frac{q}{r} \\ 0 & \text{sonst} \end{cases}$$

Damit folgt für den Zustand des ersten Registers:

$$|\phi\rangle = \frac{1}{\sqrt{r}} \sum_{d=0}^{r-1} \exp\left(\frac{2\pi ild}{r}\right) |d\frac{q}{r}\rangle$$

Quantenfouriertransformation im ersten Register

Beispiel: Shor Algorithmus für $N = 15$

$$|\psi\rangle = \frac{1}{\sqrt{2}} \left(|0\rangle + e^{i\pi} |4\rangle \right) |11\rangle$$

Die Messung im ersten Register liefert $x \in \{0, 4\}$. Der Zustand ist also wie von der DFT bekannt mit $M = \frac{2^3}{2} = 4$ periodisch.

Bestimmung der Periode

Die Messung im ersten Register liefert einen Wert $x = d\frac{q}{r}$ mit $d \in \{0, \ldots, r-1\}$:

$$\frac{r}{d} = \frac{q}{x}(\text{ für } d, x \neq 0)$$

Hier sind q und x bekannt, r wird gesucht. Wenn d und r teilerfremd sind, kann r durch kürzen von q und x auf einen irreduziblen Bruch abgelesen werden. Die Wahrscheinlichkeit für $ggT(d, r) = 1$ ist für große r größer $\frac{1}{\ln r}$.

Periode $\longrightarrow$ Faktoren

Beispiel: Shor Algorithmus für $N = 15$

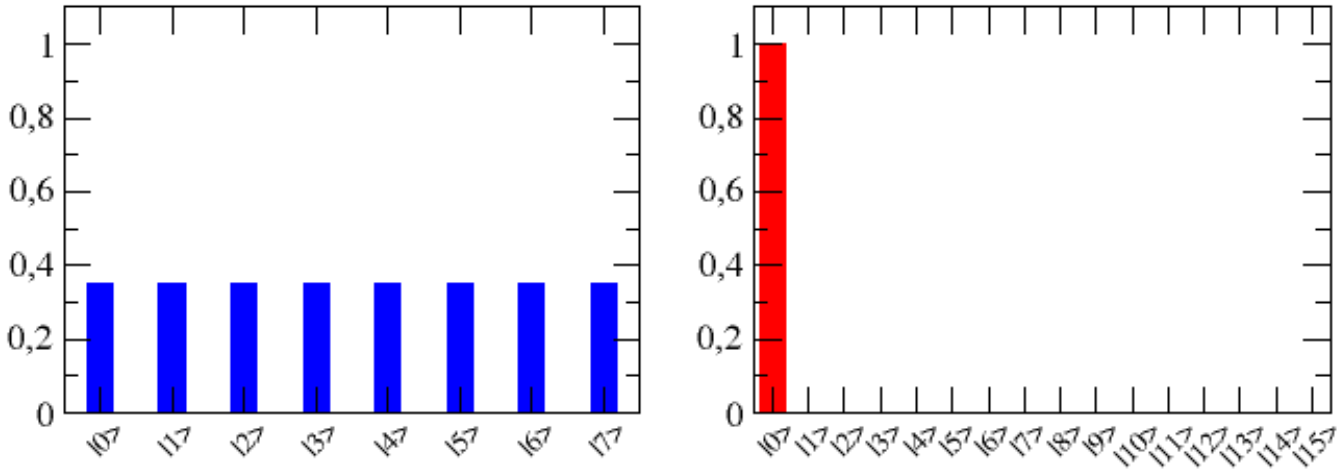
Periode von $f(x) = 11^x \mod 15$ ist $r = 2$

$$p_0 = ggT(11^{\frac{2}{2}} - 1, 15) = 5\text{: erster Primfaktor von 15}$$

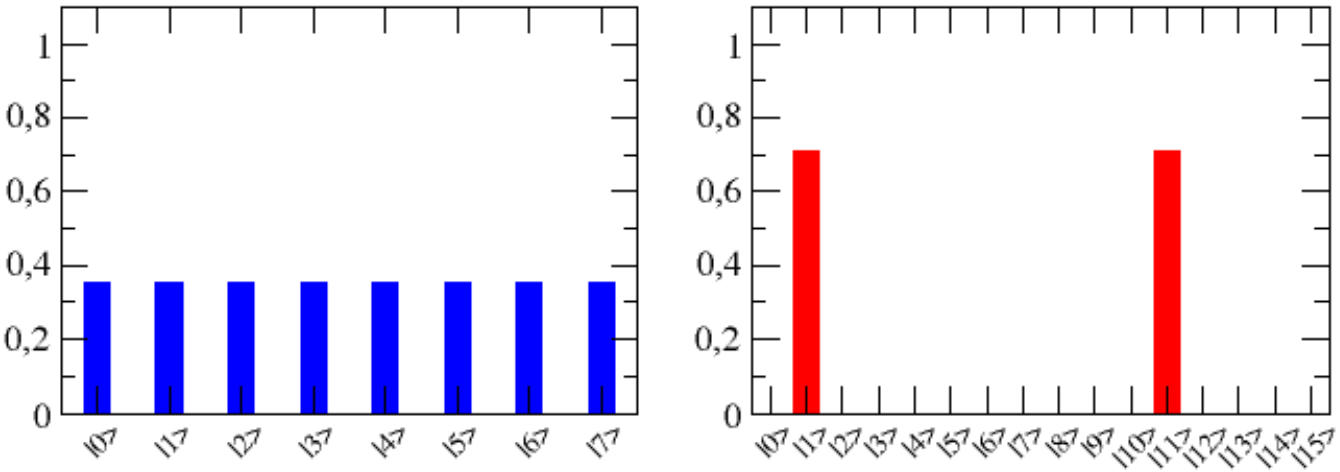
$$p_1 = ggT(11^{\frac{2}{2}} + 1, 15) = 3\text{: zweiter Primfaktor von 15}$$

Der Quantenalgorithmus für $N = 15$ im Überblick

Initialisierung beider Register:

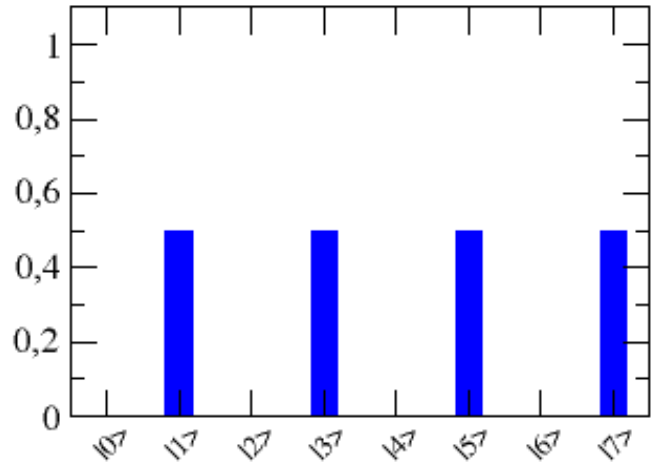


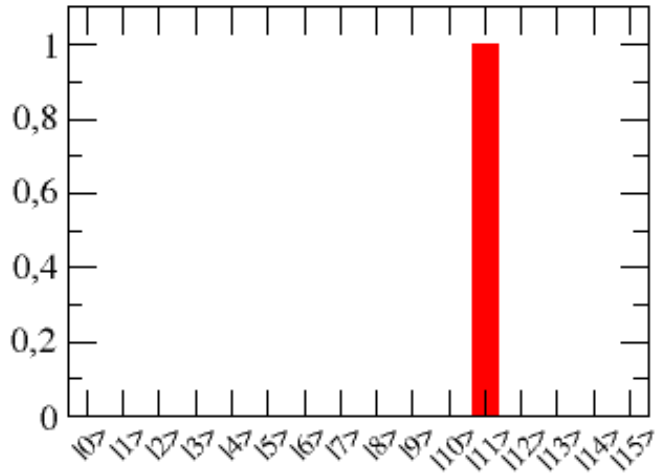
Berechne $f(x) = 11^x \mod 15$ im zweiten Register:



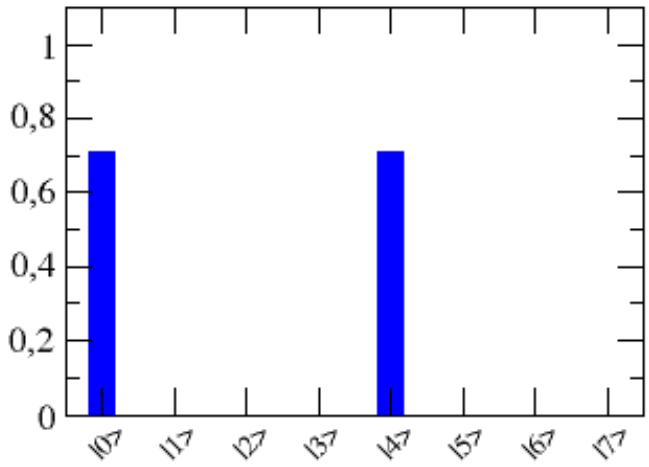
Der Quantenalgorithmus für $N = 15$ im Überblick

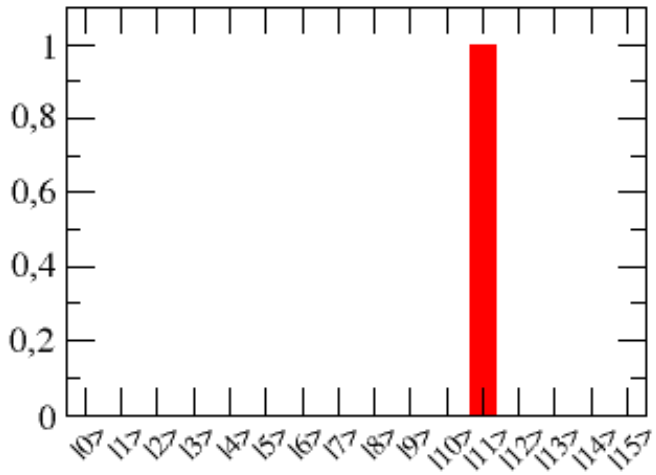
Messung im zweiten Register ($y = 11$):





Quantenfouriertransformation im ersten Register:





Literatur

- Peter W. Shor: Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer (25.01.1996) [arXiv:quant-ph/9508027 v2]
- Artur Ekert and Richard Jozsa: Quantum computation and Shor's factoring algorithm (July 1996) [Reviews of modern Physics, Vol. 68 No. 3]
- Jürgen Audretsch: Verschränkte Systeme - Die Quantenphysik auf neuen Wegen [Wiley-VCH Verlag GmbH & Co. KGaA Weinheim, 2005]