

Die Berechnung der Periode

Wir gehen davon aus, daß wir mit dem in der vergangenen Vorlesung angegebenen Algorithmus zwei von Null verschiedene Werte y_i erhalten haben, für die

$$-\frac{1}{2} < y_i - \frac{l_i M}{r} \leq \frac{1}{2}, \quad i = 1, 2. \quad (1)$$

mit ganzen $0 < l_1 < l_2 < r$ gilt. Wie wir gesehen haben, gelingt uns das mit Wahrscheinlichkeit größer $1/25$. Weiterhin setzen wir voraus, daß $\gcd(l_1, l_2) = 1$, was unter den gegebenen Voraussetzungen mit Wahrscheinlichkeit größer $1/2$ eintritt.

Wie berechnen wir aus y_1 und y_2 nun die Periode r ? Wir müssen den erweiterten Euklidischen Algorithmus, den wir im Fall $r \mid M$ benutzt haben, ersetzen.

Wir betrachten die Menge L aller Linearkombinationen der Vektoren

$$v_1 = \begin{pmatrix} 1 \\ 0 \\ y_1 \end{pmatrix} \quad \text{und} \quad v_2 = \begin{pmatrix} 0 \\ 1 \\ y_2 \end{pmatrix}.$$

Eine solche Menge wird *Gitter* genannt. In L liegt der Vektor

$$v = l_2 v_1 - l_1 v_2 = \begin{pmatrix} l_2 \\ -l_1 \\ l_2 y_1 - l_1 y_2 \end{pmatrix}.$$

Lemma 1 Falls $M > 2\sqrt{3}r^2$, ist v kürzer als jeder von Null und $\pm v$ verschiedene Vektor in L .

BEWEIS Zunächst schätzen wir die Länge von v ab. Die ersten beiden Einträge von v haben Betrag kleiner r . Gleiches gilt auch für den dritten Eintrag

$$\begin{aligned} |l_2 y_1 - l_1 y_2| &= \left| l_2 y_1 - l_2 \frac{l_1 M}{r} + l_1 \frac{l_2 M}{r} - l_1 y_2 \right| \\ &\leq l_2 \left| y_1 - \frac{l_1 M}{r} \right| + l_1 \left| y_2 - \frac{l_2 M}{r} \right| \leq \frac{1}{2}(l_1 + l_2) < r. \end{aligned}$$

Es folgt $\|v\| < \sqrt{3}r$.

Angenommen für $w = a_1 v_1 - a_2 v_2$ gelte $0 < \|w\| < \|v\|$. Damit muß für die ersten beiden Einträge von w , also für a_1 und a_2 gelten, daß $a_i < \sqrt{3}r$. Wir

betrachten den letzten Eintrag w_3 von w .

$$a_1 y_1 - a_2 y_2 = (a_1 l_1 - a_2 l_2) \frac{M}{r} + a_1 \left(y_1 - \frac{l_1 M}{r} \right) - a_2 \left(y_2 - \frac{l_2 M}{r} \right).$$

Ist $a_1 l_1 \neq a_2 l_2$, dann ist diese Zahl vom Betrag größer als

$$\frac{M}{r} - |a_1| \left| y_1 - \frac{l_1 M}{r} \right| - |a_2| \left| y_2 - \frac{l_2 M}{r} \right|.$$

Da nach Voraussetzung $M/r > 2\sqrt{3}r$, würde aus $|a_i| < \sqrt{3}r$ und (1) für diesen Fall folgen, daß $|w_3| > \sqrt{3}r$ im Widerspruch zu $\|w\| < \|v\|$.

Also ist $a_1 l_1 = a_2 l_2$. Wegen $\gcd(l_1, l_2) = 1$ gilt daher $a_1 = k l_2$ und $a_2 = k l_1$ und $w = kv$ mit ganzem k , wiederum im Widerspruch zu $\|w\| < \|v\|$. \square

Wie finden wir den kürzesten Vektor in L ? Dazu dient der Gaußsche Reduktionsalgorithmus.

Input: Vektoren v_1 und v_2 mit $\|v_1\| < \|v_2\|$

Output: Kürzester Vektor in $L = \mathbb{Z}v_1 + \mathbb{Z}v_2$

- (1) **while** $\|v_1\| < \|v_2\|$
- (2) Ersetze v_2 durch den kürzesten Vektor der Form
 $v_2 + av_1$ mit $a \in \mathbb{Z}$.
- (3) Tausche $v_1 \leftrightarrow v_2$.
- (4) **return** v_2 .

Beispiel. Wir berechnen die Periode $r = 5$ der Funktion $f(x) = 4^x \bmod 11$. Dazu wählen wir $M = 128$. Nach $H_n \otimes \text{Id}$ und U_f haben wir

$$2^{-7/2} \sum_{x=0}^{127} |x\rangle |4^x \bmod 11\rangle.$$

Wir messen die rechte Seite und erhalten, sagen wir, 4 und den Zustand

$$\frac{1}{\sqrt{26}} \sum_{k=0}^{25} |1 + 5k\rangle.$$

QFT transformiert diesen Zustand in

$$\frac{1}{2^{7/2} \sqrt{26}} \sum_{y=0}^{127} \left(\sum_{k=0}^{25} e^{2\pi i(1+5k)y/128} \right) |y\rangle$$

Wir messen erneut und erhalten den Wert $y_1 = 51$. Die Wahrscheinlichkeit dafür war

$$\frac{1}{2^7 26} \left| \sum_{k=0}^{25} e^{2\pi i(1+5k)51/128} \right|^2 = \frac{1}{2^7 26} \frac{|e^{-2\pi i 26/128}|}{|e^{-2\pi i/128}|}.$$

Dies ist größer als $1/6$. In einem zweiten Durchlauf erhalten wir $y_2 = 77$ (mit der gleichen Wahrscheinlichkeit).

In der Gaußschen Reduktion finden wir die Vektoren

$$v_{2,\text{neu}} = v_2 - 2v_1 = \begin{pmatrix} -2 \\ 1 \\ -25 \end{pmatrix}$$

und nach dem Tausch $v'_1 = v_{2,\text{neu}}, v'_2 = v_1$ in der zweiten Iteration

$$v'_{2,\text{neu}} = v'_2 - 2v'_1 = 5v_1 - 2v_2 = \begin{pmatrix} -3 \\ 2 \\ 1 \end{pmatrix}.$$

Dies ist der kürzeste Vektor in L . Wir lesen ab $l_1 = 2$ und $l_2 = -3$. Schließlich erhalten wir aus

$$\left| 51 - \frac{2 \cdot 128}{r} \right| \leq \frac{1}{2},$$

daß $r = 5$.

Berechnung der QFT

Wir betrachten zunächst die QFT für $m = 1$ und 2 .

Für $m = 1$ haben wir

$$\sqrt{2} \cdot \text{QFT}_1|x\rangle = \sum_{y=0}^1 e^{2\pi i xy/2} |y\rangle = |0\rangle + e^{2\pi ix/2} |1\rangle.$$

Da $e^{2\pi ix/2} = (-1)^x$ erkennen wir, daß QFT_1 nichts anderes als die bekannte Hadamard-Transformation ist.

Für $m = 2$ haben wir

$$\begin{aligned}
 2 \cdot \text{QFT}_2|x\rangle &= \sum_{y=0}^3 e^{2\pi i xy/4} |y\rangle \\
 &= |00\rangle + e^{2\pi i x/4} |01\rangle + e^{2\pi i x/2} |10\rangle + e^{2\pi i 3x/4} |11\rangle \\
 &= |0\rangle \otimes (|0\rangle + e^{2\pi i x/4} |1\rangle) + |1\rangle \otimes (e^{2\pi i x/2} |0\rangle + e^{2\pi i 3x/4} |1\rangle) \\
 &= (|0\rangle + e^{2\pi i x/2} |1\rangle) \otimes (|0\rangle + e^{2\pi i x/4} |1\rangle)
 \end{aligned}$$

Dies führt uns zu der Vermutung, daß

$$2^{m/2} \text{QFT}_m|x\rangle = (|0\rangle + e^{2\pi i(x/2)}|1\rangle) \otimes \dots \otimes (|0\rangle + e^{2\pi i(x/2^m)}|1\rangle)$$

Beweis: Übung. Die QFT überführt die Basisvektoren also in unverschränkte Zustände. Die Transformation des ersten Qubits

$$\sqrt{2} \cdot |x_0\rangle \mapsto (|0\rangle + e^{2\pi i x_0/2}|1\rangle) = (|0\rangle + e^{2\pi i \sum_{i=0}^{m-1} x_i 2^{i-1}}|1\rangle) = (|0\rangle + e^{2\pi i x_0/2}|1\rangle)$$

ist wieder die Hadamard-Transformation. Das j -te Qubit $|x_j\rangle$ wird auf

$$\frac{1}{\sqrt{2}} (|0\rangle + e^{2\pi i x_j/2^{j+1}}|1\rangle) = \frac{1}{\sqrt{2}} (|0\rangle + e^{2\pi i \sum_{i=0}^j x_i 2^{i-j-1}}|1\rangle)$$

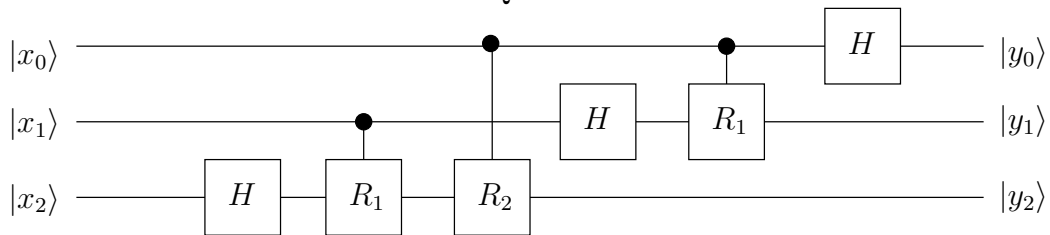
abgebildet, welches wir durch den Operator

$$\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 \\ 0 & e^{2^{-j}\pi i} \end{pmatrix}^{x_0} \dots \begin{pmatrix} 1 & 0 \\ 0 & e^{2^{-1}\pi i} \end{pmatrix}^{x_j} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

aus $|x_{m-1} \dots x_0\rangle$ erhalten. Zur Berechnung der QFT werden also kontrollierte R_k -Gatter benötigt, wobei

$$R_k = \begin{pmatrix} 1 & 0 \\ 0 & e^{2^{-k}\pi i} \end{pmatrix} .$$

Für $m = 3$ erhalten wir damit den Quantenschaltkreis



Dieser Schaltkreis läßt sich leicht für größere m verallgemeinern. Der resultierende Schaltkreis hat m Hadamard-Gatter und $m(m - 1)/2$ kontrollierte R_k -Gatter.

Bemerkung. Die R_k -Gatter sind für große k aus Präzisionsgründen voraussichtlich schwer zu implementieren. Lassen wir sie weg, entsteht auch nur ein kleiner Fehler, da $\|R_k - I\| < e^{1-k\pi}$ (Übung). Bei der Komposition unitärer Operatoren addieren sich die Fehler. Daher genügt es, wenn wir einen Fehler von ϵ tolerieren können, nur die Gatter R_i mit i in $O(\log(m/\epsilon))$ zu berechnen. Die Komplexität der QFT ist daher quasi-linear in m und linear in $\log 1/\epsilon$.