

## Quantum-Fourier-Transformation

In der letzten Vorlesung hatten wir den Zustand

$$v = \frac{1}{\sqrt{A}} \sum_{x=0}^{M-1} \delta_{\mathcal{A}}(x) |x\rangle. \quad (1)$$

erzeugt, wobei  $\delta_{\mathcal{A}}$  die charakteristische Funktion des Urbildes  $\mathcal{A} = f^{-1}(z_0)$  eines Wertes  $z_0$  unter der Funktion  $f$  mit (unbekannter) Periode  $r$  war, und  $A = \text{card } \mathcal{A}$ .

Auf diesen Zustand wenden wir jetzt die Quanten-Fourier-Transformation an, also die unitäre Abbildung

$$U : |x\rangle \mapsto \frac{1}{\sqrt{M}} \sum_{y=0}^{M-1} e^{2\pi i xy/M} |y\rangle.$$

Diese Abbildung werden wir in Zukunft mit QFT bezeichnen.

Im Ergebnis erhalten wir den Zustand

$$\frac{1}{\sqrt{MA}} \sum_{y=0}^{M-1} \left( \sum_{x=0}^{M-1} \delta_{\mathcal{A}}(x) e^{2\pi i xy/M} \right) |y\rangle = \frac{1}{\sqrt{MA}} \sum_{y=0}^{M-1} \widehat{\delta}_{\mathcal{A}}(y) |y\rangle.$$

Vor uns stehen jetzt folgende Fragen:

- Wie groß soll  $M$  gewählt werden?
- Für welche Argumente  $y$  ist  $\delta_{\mathcal{A}}(y)$  groß? Können wir für diese Werte eine untere Schranke angeben?
- Wie rekonstruieren wir die Periode  $r$  aus einem oder mehreren gemessenen Werten?
- Können wir QFTeffizient berechnen?

Wir beginnen mit den ersten drei Fragen und betrachten zunächst den einfacheren Fall, daß  $r \mid M$ , und dann die allgemeine Situation.

## Der Fall $r \mid M$

In diesem Fall läßt sich  $\mathcal{A}$  einfach schreiben als

$$\mathcal{A} = f^{-1}(z_0) = \{x \mid r \mid (x - x_0)\} = \{x_0 + kr \mid k = 0, \dots, M/r - 1\},$$

wobei  $x_0$  das kleinste Argument im Intervall  $[0, M)$  ist, welches auf  $z_0$  abgebildet wird. Es folgt  $A = M/r$ .

Also läßt sich unser Zustand schreiben als  $(MA)^{-1/2}$  multipliziert mit

$$\sum_{y=0}^{M-1} \left( \sum_{k=0}^{M/r-1} e^{2\pi i(x_0+kr)y/M} \right) |y\rangle = \sum_{y=0}^{M-1} e^{2\pi i x_0 y/M} \left( \sum_{k=0}^{M/r-1} e^{2\pi i k r y/M} \right) |y\rangle.$$

Für die Wahrscheinlichkeit,  $y$  zu messen, ist der Faktor  $e^{2\pi i x_0 y/M}$  ohne Belang, da er Betrag 1 besitzt. Wir fragen uns also, wann die rechte Summe einen großen Betrag besitzt.

Dies ist wenigstens dann der Fall, wenn  $ry/M$  ganz ist, da dann jeder Summand gleich 1 und die Summe gleich  $M/r$  ist. Die Zahl  $ry/M$  ist genau dann ganz, wenn  $y = lM/r$  mit  $l = 0, \dots, r-1$ . Die Wahrscheinlichkeit, ein solches  $y$  zu messen, ergibt sich zu

$$\frac{(M/r)^2}{MA} = \frac{M^2}{r^2} \cdot \frac{r}{M^2} = \frac{1}{r}.$$

Wir erhalten also  $r$  mögliche Werte für  $y$ , wobei jeder mit der gleichen Wahrscheinlichkeit  $1/r$  gemessen wird. Folglich sind dies auch die einzigen Werte, welche gemessen werden.

In der Tat, nehmen wir an, daß  $e^{2\pi i r y/M} \neq 1$ . Dann ist

$$\sum_{k=0}^{M/r-1} e^{2\pi i k r y/M} = \frac{e^{2\pi i (M/r) r y/M} - 1}{e^{2\pi i r y/M} - 1} = 0.$$

Wie bestimmen wir  $r$ , wenn wir nach zweimaliger Ausführung unseres Algorithmus die Werte  $y_1 = l_1 M/r$  und  $y_2 = l_2 M/r$  vorliegen haben? Falls  $y_i = 0$  für ein  $i = 1, 2$  (geschieht mit verschwindender Wahrscheinlichkeit, falls  $r \gg 0$ ) führen wir den Algorithmus erneut durch. Sind die gemessenen Werte beide von Null verschieden, dann sind mit Wahrscheinlichkeit größer  $1/2$  die Zahlen  $l_1$  und  $l_2$  zueinander prim (d.h.  $\gcd(l_1, l_2) = 1$ ). Also genügt

es, den größten gemeinsamen Teiler von  $y_1$  und  $y_2$  (klassisch) zu berechnen, um  $M/r$  und damit  $r$  zu erhalten.

*Beispiel.* Sei  $f(x) = a^x \bmod N$  mit  $a = 4$  und  $N = 15$ . Wir wählen  $M = 8$ . Dann erhalten wir im Ablauf der Algorithmus zuerst folgenden Zustand

$$|0\rangle|0\rangle \rightarrow \frac{1}{\sqrt{8}} \sum_{x=0}^7 |x\rangle |f(x)\rangle = \frac{1}{\sqrt{8}} \left( \sum_{k=0}^3 |2k\rangle |1\rangle + \sum_{k=0}^3 |2k+1\rangle |4\rangle \right)$$

Angenommen die Messung des rechten Registers ergibt den Wert 4, dann wenden wir die QFT auf folgenden Zustand an

$$\frac{1}{2} \sum_{k=0}^3 |2k+1\rangle \xrightarrow{\text{QFT}} \frac{1}{2\sqrt{8}} \sum_{y=0}^7 \left( \sum_{k=0}^3 e^{2\pi i(2k+1)y/8} \right) |y\rangle$$

Wir berechnen die Wahrscheinlichkeit, mit der die  $y = 1$  und  $y = 4$  gemessen werden. Die erste ist

$$\frac{1}{32} \left| \sum_{k=0}^3 e^{2\pi i(2k+1)/8} \right|^2 = \frac{1}{32} \left| \sum_{k=0}^3 e^{2\pi i k/4} \right|^2 = \frac{1}{32} (1 + i + (-1) + (-i)) = 0.$$

Gleiches gilt für  $y \in \{2, 3, 5, 6, 7\}$ . Die Wahrscheinlichkeit,  $y = 4$  zu messen, ist

$$\frac{1}{32} \left| \sum_{k=0}^3 e^{2\pi i(2k+1)/2} \right|^2 = \frac{1}{32} \left| \sum_{k=0}^3 e^{2\pi i k} \right|^2 = \frac{1}{32} \cdot 4^2 = \frac{1}{2}.$$

Dies ist auch die Wahrscheinlichkeit,  $y = 0$  zu messen. Da der einzige von 0 verschiedene Wert, den der Quanten-Algorithmus ausgibt,  $y = 4$  ist, schließen wir, daß  $4 = M/r$ , also  $r = 2$ .

## Der Fall $r \nmid M$

Dies ist der Regelfall, da  $M$  eine Zweierpotenz ist, und daher nur sehr wenige Teiler besitzt. Es stellt sich heraus, daß wir genau gleich vorgehen können, jedoch diesmal nicht nur Vielfache von  $M/r$  finden – in der Tat kann es im Intervall  $[0, M)$  möglicherweise keine ganzzahligen Vielfachen von  $M/r$  geben – sondern auch (sehr gute) Annäherungen an diese Vielfache.

Untersuchen wir dies genauer. Sei also

$$M \equiv M_0 \pmod{r} \quad \text{mit } 0 < M_0 < r.$$

Die Kardinalität der Menge  $\mathcal{A}$  hängt nun davon ab, ob  $x_0 < M_0$  oder nicht. Wir betrachten den Fall  $M_0 \leq x_0 < r$ . Der andere Fall bleibt als Übung. Dann ist

$$\mathcal{A} = \{ x_0 + kr \mid k = 0, \dots, (M - M_0)/r - 1 \} .$$

und  $A = (M - M_0)/r$ .

Nachdem wir QFT auf den Zustand (1) anwenden, hat der Basisvektor  $|y\rangle$  die Amplitude

$$\frac{1}{\sqrt{AM}} e^{2\pi i x_0 / M} \sum_{k=0}^{(M-M_0)/r-1} e^{2\pi i k r y / M} . \quad (2)$$

Angenommen,  $y$  ist die nächste ganze Zahl zu  $lM/r$  für ein ganzes  $l$  in  $[0, r)$ , also

$$-\frac{1}{2} < y - \frac{lM}{r} \leq \frac{1}{2} . \quad (3)$$

Wir gehen in der Folge davon aus, daß die Differenz  $y - lM/r$  positiv ist. Ist  $y = lM/r$ , dann können wir die Analyse aus dem vorigen Abschnitt anwenden. Der Fall negativer Differenz läßt sich analog zu dem positiven Fall entwickeln. In letzterem gilt

$$0 \leq \frac{kry}{M} - kl \leq \frac{kr}{2M} < \frac{1}{2}$$

für alle  $k = 0, \dots, K = (M - M_0)/r - 1$ . Also liegen alle Summanden  $e^{2\pi i kry/M}$  oberhalb der  $x$ -Achse auf dem Einheitskreis, und zwar gleichverteilt mit steigendem Argument von  $1 = e^{2\pi i 0ry/M}$  bis  $e^{2\pi i Kry/M}$ . (Ist die Differenz  $y - lM/r$  hingegen negativ, dann haben wir die analoge Situation unterhalb der  $x$ -Achse.)

Damit ist bereits klar, daß die Summe für derartiges  $y$  großen Betrag besitzt. Dies quantifizieren wir jetzt.

Wir betrachten zwei Fälle, je nachdem, ob  $K(ry/M - l)$  größer oder kleiner als  $1/4$  ist. Ist dieses Produkt größer als  $1/4$ , dann ist

$$|e^{2\pi i Kry/M} - 1| > \sqrt{2} .$$

Dies nutzen wir, indem wir die Summe in (2) als geometrische Reihe aufsummieren. Wir erhalten

$$\frac{e^{2\pi i Kry/M} - 1}{e^{2\pi i ry/M} - 1} .$$

Den Nenner schätzen wir ab über

$$|e^{i\omega} - 1| \leq \omega$$

(Beweis: Übung) und erhalten

$$|e^{2\pi i y r / M} - 1| = |e^{2\pi i (y r / M - l)} - 1| \leq 2\pi \cdot \frac{r}{2M} = \frac{\pi r}{M}.$$

wegen (3).

Im Ergebnis erhalten wir, daß die Wahrscheinlichkeit ein  $y$  mit (3) zu finden, von unten durch

$$\frac{1}{AM} \cdot \frac{2}{(\pi r / M)^2} = \frac{2}{\pi^2} \cdot \frac{1}{A} \cdot \frac{M}{r^2} > \frac{2}{\pi^2} \cdot \frac{r}{M} \cdot \frac{M}{r^2} = \frac{2}{\pi^2} \frac{1}{r}$$

beschränkt ist.

Im zweiten Fall ist  $K(ry/M - l)$  kleiner als  $1/4$ . Dann gilt auch

$$0 \leq k(ry/M - l) < 1/4 \quad \text{für alle } 0 \leq k < K. \quad (4)$$

Wir schreiben den  $k$ -te Summanden  $e^{2\pi i k r y / M}$  als Linearkombination  $\alpha_k(1 + i) + \beta_k(1 - i)$  der orthogonalen Vektoren  $(1 + i)$  und  $1 - i$  in  $C$ . Aus (4) folgt dann, daß  $\alpha_k \geq 1/2$ . In der Konsequenz ist

$$\begin{aligned} \left| \sum_{k=0}^{(M-M_0)/r-1} e^{2\pi i k r y / M} \right| &= \left| (1 + i) \sum_{k=0}^{(M-M_0)/r-1} \alpha_k + (1 - i) \cdot \sum_{k=0}^{(M-M_0)/r-1} \beta_k \right| \\ &\geq \frac{M - M_0}{2r}. \end{aligned}$$

Wie zuvor erhalten wir für die Wahrscheinlichkeit  $Ws_y$ , ein  $y$  zu messen, das (3) erfüllt,

$$Ws_y > \frac{1}{AM} \cdot \frac{(M - M_0)^2}{4r^2} > \frac{M - M_0}{4rM} > \frac{1}{4r} - \frac{1}{4M}.$$

Wir schlußfolgern, daß wir im Ergebnis eines Durchlaufs des beschriebenen Quanten-Algorithmus mit Wahrscheinlichkeit größer  $1/5$  ein  $y$  finden, das (3) erfüllt (jedenfalls, wenn  $4M \geq 5r$ ).

In der nächsten Vorlesung werden wir die Methode behandeln, wie wir aus dem Ergebnis zweier Läufe des Quanten-Algorithmus die Periode  $r$  berechnen, und die Frage beantworten, wie groß  $M$  sein muß, damit dies mit konstanter von  $r$  unabhängiger Wahrscheinlichkeit gelingt.