Protokoll zur Vorlesung Quantencomputing WS 23/24

W. Bley

1. Februar 2024

1 Die Quanten-Fourier-Transformation

Definition 1.0.1 Sei $n \in \mathbb{N}$ und $\{|j\rangle^n : 0 \leq j < 2^n\}$ die Rechenbasis des ${}^q\mathbb{H}^{\otimes n}$. Weiter sei

$$\omega := \exp(2\pi i/2^n).$$

Dann ist die Quanten-Fourier-Transformation F gegeben durch

$$|j\rangle^n \overset{F}{\mapsto} \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} \omega^{jk} |k\rangle^n.$$

Remark 1.0.2 Für ein beliebiges Element

$$|x\rangle = \sum_{j=0}^{2^n-1} x_j |j\rangle^n \in {}^q\mathbb{H}^{\otimes n}$$

erhält man

$$F|x\rangle = \sum_{k=0}^{2^n-1} y_k |k\rangle^n.$$

mit

$$y_k = \frac{1}{\sqrt{2^n}} \sum_{j=0}^{2^n-1} x_j \omega^{jk}.$$

Die Zahlen $y_0, \ldots, y_{2^n-1}$ sind gerade die diskreten Fouriertransformierten der komplexen Zahlen $x_0, \ldots, x_{2^n-1}$.

Lemma 1.0.3 *Die Quanten-Fourier-Transformation ist unitär. Für die Inverse F^{-1} gilt:*

$$|k\rangle^n \overset{F^{-1}}{\mapsto} \frac{1}{\sqrt{2^n}} \sum_{s=0}^{2^n-1} \omega^{-sk} |s\rangle^n.$$

Definition 1.0.4 Für $a_1, \ldots, a_m \in \{0, 1\}$ setzen wir

$$0.a_1 a_2 \ldots a_m := \frac{a_1}{2} + \frac{a_2}{2^2} + \ldots + \frac{a_m}{2^m} = \sum_{l=1}^{m} \frac{a_l}{2^l}.$$

Lemma 1.0.5 *Sei $|x\rangle^n$ ein Element der Rechenbasis und $x = \sum_{j=0}^{n-1} x_j 2^j$ mit $x_j \in \{0, 1\}$ seine 2-adische Entwicklung. Dann gilt:*

$$F|x\rangle^n = \frac{1}{\sqrt{2^n}} \bigotimes_{j=0}^{n-1} \left[|0\rangle + e^{2\pi i 0.x_j \ldots x_0} |1\rangle\right].$$

Definition 1.0.6 Sei $n \in \mathbb{N}$.
a) Für $0 \leq j < n$ setzen wir

$$H_j := \mathrm{id}^{\otimes(n-1+j)} \otimes H \otimes \mathrm{id}^{\otimes j}$$

mit der Hadamardtransformation H.
b) Für $j, k \in \{0, \ldots, n-1\}$ mit $j > k$ setzen wir $\theta_{jk} := \pi/2^{j-k}$ und definieren den bedingten Phasenschieber durch

$$\begin{aligned} P_{jk} &= \mathrm{id}^{\otimes(n-1-k)} \otimes |0\rangle\langle 0| \otimes \mathrm{id}^{\otimes k} + \\ &\quad \mathrm{id}^{\otimes(n-1-j)} \otimes \left[|0\rangle\langle 0| + e^{i\theta_{jk}}|1\rangle\langle 1|\right] \otimes \mathrm{id}^{\otimes(j-k-1)} \otimes |1\rangle\langle 1| \otimes \mathrm{id}^{\otimes k}. \end{aligned}$$

Satz 1.0.7 *Für die Quanten-Fourier-Transformation gilt*

$$\begin{aligned} F &= S^{(n)} \prod_{j=0}^{n-1} \left(\left[\prod_{k=0}^{j-1} P_{jk} \right] H_j \right) \\ &= S^{(n)} H_0 P_{10} H_1 P_{20} P_{21} H_2 P_{30} P_{31} P_{32} H_3 \cdots P_{n-1,0} P_{n-1,1} \cdots P_{n-1,n-2} H_{n-1}. \end{aligned}$$

Hierbei ist $S^{(n)}$ eine einfache Transformation, die die Reihenfolge der qBits umkehrt.

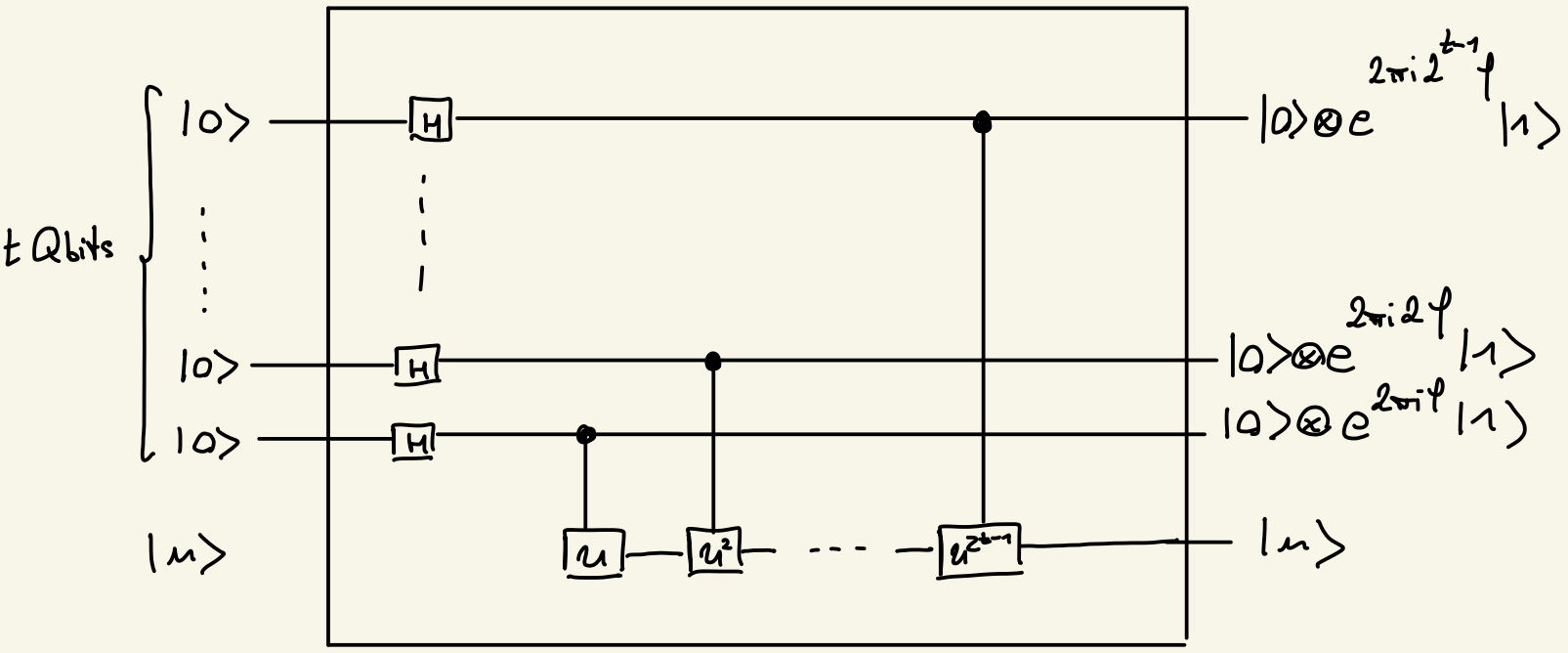
Folgerung 1.0.8 *Zur Berechnung der Quanten-Fourier-Transformation benötigt man $O(n^2)$ elementare Rechenschritte.*

2 Die wichtigsten Quantenalgorithmen

2.1 Der Phasenschätzer

Sei $U\colon {}^q\mathbb{H}^{\otimes n} \longrightarrow {}^q\mathbb{H}^{\otimes n}$ ein unitärer Operator und $|u\rangle$ ein Eigenvektor. Sei $U|u\rangle = e^{2\pi i\varphi}|u\rangle$ mit $0 \leq \varphi < 1$. Es sei $\varphi = 0.\varphi_1\varphi_2\varphi_3\ldots$ mit $\varphi_j \in \{0, 1\}$. Ziel des Phasenschätzers ist die Berechnung einer guten Approximation an φ.
Wir setzen voraus, dass wir über zwei schwarze Schachteln verfügen:
Black Box 1 präpariert den Eigenzustand $|u\rangle$.
Black Box 2 berechnet ein kontrolliertes U^{2^j} für $j \in \mathbb{N}_0$.

Der Algorithmus nutzt zwei Register: ein t-Qbit-Register, das zu Anfang auf $|0\rangle^t$ gesetzt wird sowie ein n-Qbit-Register, dass zu Anfang den Eigenzustand $|u\rangle$ enthält.
Schritt 1 Durchlaufe den folgenden Schaltkreis.


t Qbits
|0>
|0>
|0>
|u>
H
H
H
U
U²
U^(2^(t-1))
|0>⊗e^(2πi2^(t-1)φ)|1>
|0>⊗e^(2πi2φ)|1>
|0>⊗e^(2πiφ)|1>
|u>

Schritt 2 Führe eine inverse Quanten-Fourier-Transformation im ersten Register durch.
Schritt 3 Miss das erste Register.

Im ersten Schritt geht der Zustand $|0\rangle^t \otimes |u\rangle$ über in den Zustand

$$\frac{1}{\sqrt{2^t}} \bigotimes_{k=t-1}^{0} \left(|0\rangle + e^{2\pi i 2^k \varphi} |1\rangle \right) \otimes |u\rangle.$$

Das erste Register ist also im Zustand

$$|v\rangle = \frac{1}{\sqrt{2^t}} \bigotimes_{k=t-1}^{0} \left(|0\rangle + e^{2\pi i 2^k \varphi} |1\rangle \right).$$

Man beachte, dass

$$e^{2\pi i 2^k \varphi} = e^{2\pi i 0.\varphi_{k+1}\varphi_{k+2}\varphi_{k+3}\cdots}$$

gilt. Im Fall $\varphi = 0.\varphi_1\varphi_2\ldots\varphi_{t-1}$ bewerkstelligt die inverse Quantenfouriertransformation nun gemäß Lemma 1.0.5 in einem polynomiellen Schritt die Zustandsänderung $|v\rangle \mapsto |x\rangle^t$ mit

$$x = \sum_{j=0}^{t-1} \varphi_j 2^j.$$

Wir erhalten also durch $x/2^t$ den exakten Wert φ.

Im Allgemeinen messen wir ein $|x\rangle$ und setzen $\tilde{\varphi} := x/2^t$. Sei nun $m \in \mathbb{N}$ und $\varepsilon > 0$ gegeben. Um φ mit einer Erfolgswahrscheinlichkeit $\geq 1 - \varepsilon$ und einem Fehler $|\varphi - \tilde{\varphi}| \leq 1/2^m$ zu berechnen, muss man

$$t = m + \left\lceil \log_2 \left(2 + \frac{1}{2\varepsilon} \right) \right\rceil$$

wählen.

2.2 Simons Algorithmus

Sei $f\colon \{0,1\}^n \longrightarrow \{0,1\}^n$ eine Funktion, die folgender Bedingung genügt. Sie ist entweder bijektiv (Typ **B**) oder es gibt ein $s \in \{0,1\}^n$ mit $s \neq 0$, so dass gilt:

$$f(x) = f(x') \iff x \oplus s = x' \text{ oder } x = x'.$$

f ist dann periodisch (Typ **P**) mit Periode s.

Ziel von Simons Algorithmus ist die Bestimmung des Typs und gegebenenfalls der Periode s.
Wir brauchen zwei n-Qbit-Register H^A und H^B sowie ein Quantenorakel

$$\begin{aligned} U_f\colon H^A \otimes H^B &\longrightarrow H^A \otimes H^B, \\ |a\rangle^n \otimes |b\rangle^n &\mapsto |a\rangle^n \otimes |b \oplus f(a)\rangle^n. \end{aligned}$$

Schritt 1: Präpariere den Zustand $|\Psi_1\rangle = |0\rangle^n \otimes |0\rangle^n$.
Schritt 2: Wende die n-fache Hadamardtransformation $H^{\otimes n}$ auf das erste Register H^A an. Wir erhalten dadurch den Zustand

$$|\Psi_2\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle^n \otimes |0\rangle^n.$$

Schritt 3: Wende das Quantenorakel U_f an. Wir erhalten

$$|\Psi_3\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle^n \otimes |f(x)\rangle^n.$$

Schritt 4: Miss das zweite Register H^B.
Schritt 5: Wende nochmals $H^{\otimes n}$ auf das erste Register H^A an.
Schritt 6: Miss das erste Register H^A.

Schritt 6 liefert ein $z \in \{0,1\}^n$. Wir wiederholen die Schritte 1 - 6 solange, bis wir $n-1$ linear unabhängige Vektoren $z_1, \ldots, z_{n-1}$ gefunden haben. Dies ist der Quantenteil des Algorithmus. Es folgt ein klassischer Teil.

Schritt 7: Löse das lineare Gleichungssystem

$$z_1 \cdot t \equiv 0 \pmod 2, \ldots, z_{n-1} \cdot t \equiv 0 \pmod 2.$$

Dieses lineare Gleichnugssystem hat einen eindimensionalen Lösungsraum, also eine zweielementige Lösungsmenge $\{0, s\}$.
Schritt 8: Falls $f(0) = f(s)$ gilt, so ist f vom Typ P mit Periode s. Andernfalls ist f vom Typ B.

Wir beginnen die Analyse des Algorithmus mit der Messung in Schritt 4. Sei $|y\rangle^n \in H^B$ das Messergebnis und x ein Urbild von y, d.h. $f(x) = y$.
Falls f vom Typ P ist, so projeziert die Messung das Quantensystem in den Zustand

$$|\Psi_4\rangle = \frac{1}{\sqrt{2}} \left(|x\rangle^n + |x \oplus s\rangle^n\right) \otimes |f(x)\rangle^n.$$

In Schritt 5 wird $|\Psi_4\rangle$ in den Zustand

$$|\Psi_5\rangle = \sum_{z=0}^{2^n-1} \alpha_z \left(|z\rangle^n \otimes |f(x)\rangle^n\right)$$

transformiert, wobei die Amplitude α_z von $|z\rangle^n \otimes |f(x)\rangle^n$ durch

$$\alpha_z = \begin{cases} \frac{\pm 1}{\sqrt{2^n}}, & \text{falls } z \cdot s \equiv 0 \pmod 2, \\ 0, & \text{falls } z \cdot s \equiv 1 \pmod 2 \end{cases}$$

gegeben ist. Wir messen in Schritt 6 also stets ein z mit der Eigenschaft $z \cdot s \equiv 0 \pmod 2$, d.h. wir finden eine nicht-triviale Gleichung für s.

2.3 Shors Faktorisierungsalgorithmus

2.3.1 Motivation

Sei N eine natürliche Zahl, die wir faktorisieren wollen. Gute Faktorisierungsalgorithmen versuchen eine ganze Zahl x zu finden, so dass

$$x^2 \equiv 1 \pmod N \tag{1}$$

gilt. Falls dann $x \not\equiv \pm 1 \pmod N$ ist, so liefert $\mathrm{ggT}(N, x \pm 1)$ einen echten Teiler von N.
Um Kongruenzen der Form (1) zu finden, wählen wir zufällig $a \in \{1, \ldots, N-1\}$ mit $\mathrm{ggT}(a, N) = 1$ und schreiben $\bar{a} \in (\mathbb{Z}/N\mathbb{Z})^\times$ für die Nebenklasse von a modulo N. Wir berechnen nun die Ordnung $r := \mathrm{ord}(\bar{a})$ und falls r gerade ist, so setzen wir $x := a^{r/2}$. (Natürlich rechnen wir an jeder Stelle modulo N.) Mit einer gewissen Wahrscheinlichkeit ist r gerade und es gilt zusätzlich $x \not\equiv \pm 1 \pmod N$.
Die Quantenkomponente in Shors Algorithmus beschränkt sich auf die Berechnung der Ordnung $r = \mathrm{ord}(\bar{a})$.

2.3.2 Ordnungsbestimmung

Sei $N \in \mathbb{N}$ und $G = (\mathbb{Z}/N\mathbb{Z})^\times$. Sei $0 \leq x < N$ und es gelte $\mathrm{ggT}(x, N) = 1$. Dann ist $\bar{x} \in G$ und wir wollen $\mathrm{ord}(\bar{x})$ bestimmen.
Sei $L := \lceil \log_2(N) \rceil$. Wir betrachten den unitären Operator

$$\begin{aligned} U\colon\ {}^q\mathbb{H}^{\otimes L} &\longrightarrow {}^q\mathbb{H}^{\otimes L}, \\ |y\rangle^L &\mapsto \begin{cases} |xy \bmod N\rangle^L, & \text{falls } 0 \leq y \leq N-1, \\ |y\rangle^L, & \text{sonst.} \end{cases} \end{aligned}$$

Lemma 2.3.1 *Für $0 \leq s \leq r-1$ sei*

$$|u_s\rangle := \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} \exp(-2\pi i s k/r) |x^k \bmod N\rangle^L.$$

a) Für $0 \leq s \leq r-1$ ist $|u_s\rangle$ ein Eigenzustand von U mit Eigenwert $\exp(2\pi i s/r)$.
b) Es gilt

$$\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |u_s\rangle = |1\rangle^L.$$

Wendet man nun den Phasenschätzer auf den Zustand $|0\rangle^t \otimes |1\rangle^L$ an, so erhält man einen Zustand

$$\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |x_s\rangle^t \otimes |u_s\rangle.$$

Setzt man $\tilde{\varphi}_s := x_s/2^t$, so ist $\tilde{\varphi}_s$ mit einer positiven Wahrscheinlichkeit eine gute Approximation an die Phase s/r. Genauer kann man zeigen: Setzt man $t = (2L+1) + \left\lceil \log_2(2 + \frac{1}{2\varepsilon}) \right\rceil$ und fixiert s, so misst man $\tilde{\varphi}_s$ mit Wahrscheinlichkeit $1/r$ und mit einer Erfolgswahrscheinlichkeit $\geq (1-\varepsilon)$ ist $\tilde{\varphi}_s$ eine Approximation an s/r mit einer Genauigkeit von $2L+1$ Bits, d.h. $|\tilde{\varphi}_s - \frac{s}{r}| < \frac{1}{2^{2L+1}}$ (vgl. Aufgabe 1, Blatt 10).
Mit Hilfe der Theorie der Kettenbruchentwicklung kann man nun aus der Kenntnis der Approximation $\tilde{\varphi}_s$ die Ordnung r berechnen. Es gilt (vgl. Aufgabe 4, Blatt 7):

Satz 2.3.2 *Sei $\frac{s}{r} \in \mathbb{Q}$ und es gelte $|\frac{s}{r} - \tilde{\varphi}_s| \leq \frac{1}{2r^2}$. Dann ist s/r ein Teilbruch in der Kettenbruchentwicklung von $\tilde{\varphi}_s$.*

Falls wir also eine gute Approximation an s/r haben, so produziert uns die Kettenbruchentwicklung von $\tilde{\varphi}_s$ endlich viele Zahlen $p_0, q_0, p_1, q_1, \ldots$ so dass für ein i gilt

$$\frac{s}{r} = \frac{p_i}{q_i}.$$

Man beachte, das der Bruch $\frac{p_i}{q_i}$ stets gekürzt ist. Wir durchlaufen nun die endliche Liste $q_0, q_1, \ldots$ und testen, ob $x^{q_i} \equiv 1 \pmod{N}$ erfüllt ist.
Im wesentlichen können zwei Dinge schief gehen.
1) Mit einer gewissen Wahrscheinlichkeit wird ein schlechter Schätzwert für die Phase s/r berechnet. In diesem Fall starten wir einen neuen Versuch (eventuell sogar mit dem gleichen x).
2) Falls wir ein s messen, so dass s/r nicht gekürzt ist, so liefert der Kettenbruchalgorithmus einen echten Teiler r' von r. Auch in diesem Fall starten wir von neuem.

2.3.3 Der Faktorisierungsalgorithmus im Überblick

Eingabe: Eine zusammengesetzte Zahl N mit mindestens zwei Primfaktoren.
Ausgabe: Ein nicht-trivialer Teiler von N.
Laufzeit: $O\left((\log_2(N))^3\right)$.

Schritt 1: Wähle $b \in \mathbb{N}$ mit $1 < b < N$ und bestimme $d := \mathrm{ggT}(b, N)$. Falls $d > 1$, so gib d aus und beende den Algorithmus.
Schritt 2: Bestimme $r := \mathrm{ord}(\bar{b})$ mit dem Quanten-Algorithmus zur Ordnungsberechnung. Falls r ungerade ist, so gehe zu Schritt 1. Andernfalls gehe zu Schritt 3.
Schritt 3: Berechne $d := \gcd(N, b^{r/2} \pm 1)$. Falls $1 < d < N$, so gib d aus. Andernfalls gehe zu Schritt 1.

2.3.4 Ordnungsbestimmung mit Fouriersampling

Sei $1 < b < N$ mit $\mathrm{ggT}(b, N) = 1$ gegeben. Betrachte die Abbildung $f = f_{b,N} \colon \mathbb{N}_0 \longrightarrow \mathbb{N}_0$ gegeben durch $f(n) = b^n \pmod N$. Sei $L := \lfloor 2\log_2(N) \rfloor + 1$ und $K \geq \lceil \log_2(N) \rceil$. Sei $H^A := {}^qH^{\otimes L}$ und $H^B := {}^qH^{\otimes K}$. Sei weiter U_f das Gatter, dass durch

$$U_f \colon H^A \otimes H^B \longrightarrow H^A \otimes H^B, \quad |x\rangle^L \otimes |y\rangle^K \mapsto |x\rangle^L \otimes |y \oplus f(x)\rangle^K,$$

gegeben ist.
Schritt 1: Präpariere $|\Psi_0\rangle := |0\rangle^L \otimes |0\rangle^K$ und wende im Register H^A die L-fache Hadamard-Transformation $H^{\otimes L}$ an. Wir erhalten

$$|\Psi_1\rangle := \frac{1}{\sqrt{2^L}} \sum_{x=0}^{2^L-1} |x\rangle^L \otimes |0\rangle^K.$$

Schritt 2: Wende U_f an. Dies liefert

$$|\Psi_2\rangle := \frac{1}{\sqrt{2^L}} \sum_{x=0}^{2^L-1} |x\rangle^L \otimes |f(x)\rangle^K.$$

Schreibt man $x = jr + k$ mit $j \in \mathbb{N}_0$ und $0 \leq k < r$, so erhält man

$$|\Psi_2\rangle := \frac{1}{\sqrt{2^L}} \sum_j \sum_k |jr + k\rangle^L \otimes |f(k)\rangle^K.$$

Schritt 3: Wende die Quanten-Fourier-Transformation auf H^A an. Man erhält

$$|\Psi_3\rangle := \frac{1}{2^L} \sum_k \sum_j \sum_{l=0}^{2^L-1} \exp(2\pi i(jr + k)l/2^L) |l\rangle^L \otimes |f(k)\rangle^K.$$

Schritt 4: Miss das erste Register H^A.

Mit genügend großer Wahrscheinlichkeit messen wir ein $z \in \{0, \ldots, 2^L - 1\}$, so dass ein $l = l_z$ mit der Eigenschaft $|zr - 2^L l| \leq r/2$ existiert. Für solch ein z gilt

$$\left| \frac{z}{2^L} - \frac{l_z}{r} \right| < \frac{1}{2r^2}.$$

Man kann also aus der Kenntnis von $\frac{z}{2^L}$ mit der Kettenbruchmethode die Ordnung r berechnen.

3 Das versteckte Untergruppenproblem (Hidden Subgroup Problem (HSP))

Sei G eine Gruppe und $H \leq G$ eine Untergruppe. Sei S eine endliche Menge und $f\colon G \longrightarrow S$ eine Abbildung. Man sagt, "f versteckt die Untergruppe H", falls für alle $g_1, g_2 \in G$ gilt:

$$f(g_1) = f(g_2) \iff g_1 H = g_2 H.$$

Die Abbildung f induziert also eine injektive Abbildung $G/H \hookrightarrow S$. Man beachte aber, dass im Allgemeinen G/H keine Gruppe ist.
Das HSP ist nun das Problem, zu gegebenem f die versteckte Untergruppe H zu bestimmen. Falls G abelsch ist, so sprechen wir vom AHSP (Abelian Hidden Subgroup Problem).

3.1 Das abelsche versteckte Untergruppenproblem (AHSP)

Ab jetzt sei G endlich und abelsch. Sei $G = \{g_1, \ldots, g_{|G|}\}$ und sei $n := \lceil \log_2 |G| \rceil$. Wir wählen eine Teilmenge der Rechenbasis des ${}^q\mathbb{H}^{\otimes n}$ der Kardinalität $|G|$ und taufen ihre Elemente $|g_1\rangle, \ldots, |g_{|G|}\rangle$, d.h.

$$\{|g_1\rangle, \ldots, |g_{|G|}\rangle\} \subseteq \{|x\rangle^n : 0 \leq x < 2^n\} \subseteq {}^q\mathbb{H}^{\otimes n}.$$

Setze $H^A := \langle |g_1\rangle, \ldots, |g_{|G|}\rangle\rangle_{\mathbb{C}} \subseteq {}^q\mathbb{H}^{\otimes n}$. Dann ist H^A ein Hilbertraum mit ONB $|g_1\rangle, \ldots, |g_{|G|}\rangle$.
Sei $m := |S|$ und $H^B := {}^qH^{\otimes m}$. Sei $S = \{s_0, \ldots, s_{m-1}\}$. Wir definieren

$$\tilde{}\colon S \longrightarrow \{0, \ldots, m-1\}, \quad s_j \mapsto j,$$

und identifizieren s_j mit $|\tilde{s_j}\rangle = |j\rangle^m \in H^B$.

1.Schritt im AHSP-Algorithmus Präpariere den Zustand

$$|\Psi_0\rangle := \frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle \otimes |0\rangle^m \in H^A \otimes H^B.$$

Remark 3.1.1 Dieser Schritt hängt von der Gruppe G ab. Wir nehmen an, dass die Präparation von $|\Psi_0\rangle$ polynomial in n ist.

2.Schritt im AHSP-Algorithmus Wir nehmen nun an, dass wir ein Gatter

$$\begin{aligned} U_f\colon H^A \otimes H^B &\longrightarrow H^A \otimes H^B, \\ |g\rangle \otimes |y\rangle^m &\mapsto |g\rangle \otimes |y \oplus \widetilde{f(g)}\rangle^m, \end{aligned}$$

zur Verfügung haben, das ebenfalls in polynomial (in n) vielen "elementaren Rechenschritten" realisiert werden kann.
Wir wenden nun U_f auf $|\Psi_0\rangle$ an und erhalten den neuen Zustand

$$|\Psi_1\rangle := U_f |\Psi_0\rangle = \frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle \otimes |\widetilde{f(g)}\rangle^m.$$

Nach dem zweiten Rechenschritt ignorieren wir das zweite Register H^B. Das Teilsystem H^A wird durch den Dichteoperator ρ^A beschrieben. Bezüglich der ONB $\{|g_1\rangle, \ldots, |g_{|G|}\rangle\}$ hat die darstellende Matrix die Koeffizienten

$$\rho^A_{g_1, g_2} = \begin{cases} \frac{1}{|G|}, & \text{falls } g_1 H = g_2 H, \\ 0, & \text{sonst.} \end{cases}$$

Im Folgenden schreiben wir $[g] = gH$ für die Nebenklasse von $g \in G$ nach H und setzen

$$\Psi^A_{[g]} := \frac{1}{\sqrt{|H|}} \sum_{t \in [g]} \langle t| = \frac{1}{\sqrt{|H|}} \sum_{h \in H} \langle gh|.$$

Es gilt dann:

$$\rho^A = \frac{|H|}{|G|} \sum_{[g] \in G/H} |\Psi^A_{[g]}\rangle\langle\Psi^A_{[g]}|.$$

Wir wenden nun im ersten Register H^A die Fouriertransformation

$$F_G = \frac{1}{\sqrt{|G|}} \sum_{g \in G} \sum_{\chi \in \hat{G}} \chi(g)|\chi\rangle\langle g|$$

an. Hierzu schreiben wir $\hat{G} = \{|\chi_1\rangle, \ldots, |\chi_{|G|}\rangle\}$ und identifizieren die Mengen $\{|\chi_1\rangle, \ldots, |\chi_{|G|}\rangle\}$ und $\{|g_1\rangle, \ldots, |g_{|G|}\rangle\}$. Die Anwendung von F_G auf Register H^A transformiert den gemischten Zustand ρ^A in den Zustand $F_G \rho^A F_G^*$.
Wieder nehmen wir an, dass sich auch die Anwendung von F_G in polynomial (in n) vielen elementaren Rechenschritten realisieren läßt.
Die Berechnung des Dichteoperators $F_G \rho^A F_G^*$ liefert

$$F_G \rho^A F_G^* = \frac{|H|}{|G|} \sum_{[g] \in G/H} \frac{|H|}{|G|} \left(\sum_{\chi|_H = 1} \chi(g)|\chi\rangle \right) \left(\sum_{\xi|_H = 1} \bar{\xi}(g)\langle\xi| \right)$$

Sei nun $H^\perp := \{\chi \in \hat{G} : \chi|_H = 1\}$. Nach den Gesetzen der Quantenmechanik berechnet sich die Wahrscheinlichkeit P_ζ ein festes $\zeta \in \hat{G}$ zu messen nach der Formel

$$P_\zeta = \mathrm{Tr}\left(|\zeta\rangle\langle\zeta| F_G \rho^A F_G^*\right) = \sum_a \langle e_a|\zeta\rangle\langle\zeta|F_G \rho^A F_G^* e_a\rangle,$$

wobei hier $\{e_a\} \subseteq H^A$ eine ONB von H^A bezeichnet. Wir nehmen hier oE $\{e_a\} = \{|\chi_1\rangle, \ldots, |\chi_{|G|}\rangle\}$. Man sieht leicht, dass stets ein $\zeta \in H^\perp$ gemessen wird, und die Rechnung zeigt für $\zeta \in H^\perp$

$$P_\zeta = \frac{|H|}{|G|}.$$

Wir durchlaufen nun den Algorithmus L mal (L geeignet, siehe unten) und messen $\zeta_1, \ldots, \zeta_L \in H^\perp$. Sei $P(\langle\zeta_1, \ldots, \zeta_L\rangle = H^\perp)$ die Wahrscheinlichkeit, dass $\zeta_1, \ldots, \zeta_L$ die Gruppe $H^\perp$ erzeugen. Dann gilt:

$$P(\langle\zeta_1, \ldots, \zeta_L\rangle = H^\perp) \geq 1 - \frac{|G|}{2^L |H|}.$$

Setzen wir also zu gegebenem $\varepsilon > 0$ für die Rechengenauigkeit $L \geq \left\lceil \log_2 \left(\frac{|G|}{|H|\varepsilon} \right) \right\rceil$ an, so erhält man $P(\langle\zeta_1, \ldots, \zeta_L\rangle = H^\perp) \geq 1 - \varepsilon$. Abschließend beachte man, dass unter der Voraussetzung $\langle\zeta_1, \ldots, \zeta_L\rangle = H^\perp$ gilt:

$$\bigcap_{i=1}^{L} \ker(\zeta_i) = H.$$

Mit Wahrscheinlichkeit $\geq 1 - \varepsilon$ können wir also mit diesem Algorithmus die versteckte Untergruppe H berechnen. Unter geeigneten Voraussetzungen ist das Verfahren polynomial in $n = \lceil \log_2(|G|) \rceil$.

3.2 Darstellungstheorie endlicher Gruppen

Sei G eine endliche Gruppe. Eine Darstellung von G ist ein Gruppenhomomorphismus

$$\sigma\colon G \longrightarrow \mathrm{Gl}(V),$$

wobei V ein endlich dimensionaler $\mathbb{C}$-Vektorraum ist. Durch Wahl einer Basis von V erhält man einen Homomorphismus

$$A_{\sigma,v_1,\ldots,v_n}\colon G \longrightarrow \mathrm{Gl}_n(\mathbb{C}), \quad n := \dim_{\mathbb{C}}(V).$$

Vermöge σ wird V zu einem G-Modul: für $x \in G$ und $v \in V$ setzt man $xv := \sigma(x)(v)$. Man beachte, dass die Wirkung von G auf V linear ist. Sei umgekehrt V ein endlich-dimensionaler $\mathbb{C}$-Vektorraum mit einer linearen G-Wirkung. Dann ist die Abbildung $x \overset{\sigma}{\mapsto} (v \mapsto xv)$ eine Darstellung. Wählt man eine Basis $v_1, \ldots, v_n$ von V und definiert $A_\sigma(x) \in \mathrm{Gl}_n(\mathbb{C})$ durch $(xv_1, \ldots, xv_n) = (v_1, \ldots, v_n)A_\sigma(x)$, so erhält man

$$A_{\sigma,v_1,\ldots,v_n}\colon G \longrightarrow \mathrm{Gl}_n(\mathbb{C}), \quad n := \dim_{\mathbb{C}}(V).$$

Wir machen im Weiteren keine Unterscheidung zwischen der Darstellung σ und der basisabhängigen Matrixdarstellung A_σ und benennen beides mit σ. Es ist stets aus dem Kontext klar, was gemeint ist. Den Vektorraum V nennen wir den Darstellungsraum von σ.

Definition 3.2.1 Sei σ eine Darstellung. Dann nennt man $d_\sigma := \dim_{\mathbb{C}}(V)$ den Grad der Darstellung.

Definition 3.2.2 Zwei Darstellungen $\sigma\colon G \longrightarrow V$ und $\sigma'\colon G \longrightarrow V'$ heißen isomorph, falls es einen Vektorraumisomorphismus $f\colon V \longrightarrow V'$ gibt, der verträglich mit der G-Wirkung ist, d.h. $f(xv) = xf(v)$ für alle $x \in G, v \in V$.

Man beachte, dass isomorphe Darstellungen stets denselben Grad haben. Wählt man Basen in V und V' und betrachtet σ und σ' als Homomorphismen $G \longrightarrow \mathrm{Gl}_n(\mathbb{C})$, so gilt:

$$V \simeq V' \text{ als } G\text{-Moduln} \iff \exists M \in \mathrm{Gl}_n(\mathbb{C}) \forall g \in G\colon \sigma(g)M = M\sigma'(g).$$

Eine erste Tatsache: Zu einer Darstellung σ kann man kann stets eine invertierbare Matrix S finden, so dass $S^{-1}\sigma(x)S$ für alle $x \in G$ unitär ist. Wir setzen daher ab jetzt voraus, das $\sigma(x)$ eine unitäre Abbildung bzw. Matrix ist.

Darstellungen kann man addieren: Falls V und V' zwei Darstellungsräume sind, so ist auch $V \oplus V'$ ein Darstellungsraum. In Matrizen:

$$(\sigma \oplus \sigma')(g) = \left(\begin{array}{c|c} \sigma(g) & 0 \\ \hline 0 & \sigma'(g) \end{array}\right)$$

Definition 3.2.3 Eine Darstellung σ heißt irreduzibel, wenn man σ nicht als Summe von Darstellungen schreiben kann.

Einige weitere Tatsachen:

- Es gibt bis auf Isomorphie nur endlich viele irreduzible Darstellungen. Genauer: Die Anzahl der irreduziblen Darstellungen (modulo Isomorphie) ist gleich der Anzahl der Konjugationsklassen von G. Wir bezeichnen mit $\hat{G}$ die Menge der irreduziblen Darstellungen (modulo Isomorphie).
- Jede Darstellung ist isomorph zu $\bigoplus_{\sigma \in \hat{G}} n_\sigma \sigma$ mit eindeutig bestimmten $n_\sigma \in \mathbb{N}_0$.

Definition 3.2.4 Sei σ eine Darstellung. Dann nennt man $\chi_\sigma\colon G \longrightarrow \mathbb{C}, \chi_\sigma(g) := \mathrm{Tr}(\sigma(g))$ den Charakter von σ.

Man beachte, dass isomorphe Darstellungen denselben Charakter haben.

Eine weitere Tatsache:

- $\sigma \simeq \sigma' \iff \chi_\sigma = \chi_{\sigma'}$.

Ferner gilt:

- $\chi_\sigma(1) = d_\sigma$.
- $\chi_\sigma(x^{-1}) = \overline{\chi_\sigma(x)}$.
- $\chi_{\sigma\oplus\sigma'} = \chi_\sigma + \chi_{\sigma'}$.

Lemma 3.2.5 *(Schur) Seien σ und σ' zwei irreduzible Darstellungen und $M \in \mathbb{C}^{d_\sigma \times d_{\sigma'}}$ erfülle*

$$\sigma(x)M = M\sigma'(x), \forall x \in G.$$

Dann gilt:
(a) $\sigma \not\simeq \sigma' \implies M = 0$,
(b) $\sigma = \sigma' \implies M = \alpha I_{d_\sigma}, \alpha \in \mathbb{C}$.

Schurs Lemma impliziert die Identitäten des folgenden Satzes.

Satz 3.2.6 *Sei $\sigma, \sigma' \in \hat{G}$.*
a) Für alle $1 \le i, j \le d_\sigma$ und $1 \le i', j' \le d_{\sigma'}$ gilt

$$\frac{d_\sigma}{|G|} \sum_{x\in G} \sigma(x)^*_{ij}\sigma'(x)_{i'j'} = \begin{cases} 1, & \text{falls } \sigma = \sigma', i = i', j = j', \\ 0, & \text{sonst.} \end{cases}$$

b)

$$(\chi_\sigma, \chi_{\sigma'}) := \frac{1}{|G|} \sum_{x\in G} \overline{\chi_\sigma(x)}\chi_{\sigma'}(x) = \begin{cases} 1, & \text{falls } \sigma = \sigma', \\ 0, & \text{sonst.} \end{cases}.$$

Wichtige Beispiele für Darstellungen sind die links- und die rechtsreguläre Darstellung. Sie sind definiert durch

$$L(x)|y\rangle := |xy\rangle, \quad R(x)|y\rangle := |yx^{-1}\rangle.$$

für $x, y \in G$.

Satz 3.2.7

$$\text{a)} \qquad L \simeq \bigoplus_{\sigma\in\hat{G}} (\sigma \otimes I_{d_\sigma}).$$

$$\text{b)} \qquad R \simeq \bigoplus_{\sigma\in\hat{G}} (I_{d_\sigma} \otimes \sigma^*).$$

Die nächste Folgerung verallgemeinert die bekannten Charakterrelationen aus der Theorie der abelschen Gruppen.

Folgerung 3.2.8

$$\text{a)} \qquad \sum_{\sigma\in\hat{G}} d_\sigma^2 = |G|.$$

$$\text{b)} \qquad \sum_{\sigma\in\hat{G}} d_\sigma \chi_\sigma(x) = \begin{cases} |G|, & \text{falls } x = 1, \\ 0, & \text{falls } x \neq 1. \end{cases}.$$

3.3 Die nicht-abelsche Fouriertransformierte

Wie im AHSP identifizieren wir die Gruppenelemente $g \in G$ mit Elementen der Rechenbasis $|g\rangle \in H^A := {}^q\mathbb{H}^{\otimes n}$, wobei $n := \lceil \log_2(|G|) \rceil$. Wegen $\sum_{\sigma \in \hat{G}} d_\sigma^2 = |G|$ können wir die Menge $\{(\sigma, i, j) \mid \sigma \in \hat{G}, 1 \leq i, j \leq d_\sigma\}$ mit derselben Menge der Rechenbasis identifizieren und $|\sigma, i, j\rangle$ schreiben. Wie früher setzen wir $H^A := \langle |g\rangle \colon g \in G\rangle_{\mathbb{C}} = \langle |\sigma, i, j\rangle \colon \sigma \in \hat{G}, 1 \leq i, j \leq d_\sigma\rangle_{\mathbb{C}}$
Wir definieren nun die Quanten-Fouriertransformierte $F_G \colon H^A \longrightarrow H^A$ im nicht-abelschen Fall. Dazu setzen wir

$$|\hat{g}\rangle := F_G|g\rangle := \frac{1}{\sqrt{|G|}} \sum_{\sigma \in \hat{G}} d_\sigma |\sigma, \sigma(g)\rangle$$

mit

$$|\sigma(g)\rangle = \sum_{j=1}^{d_\sigma} \sum_{k=1}^{d_\sigma} \frac{\sigma(g)_{jk}}{\sqrt{d_\sigma}} |j, k\rangle.$$

Äquivalent können wir schreiben

$$F_G = \sum_{g \in G} F_G|g\rangle\langle g| = \sum_{g \in G} |\hat{g}\rangle\langle g| = \sum_{g \in G} \sum_{\sigma \in \hat{G}} \sqrt{\frac{d_\sigma}{|G|}} \sum_{j,k=1}^{d_\sigma} \sigma(g)_{jk} |\sigma, j, k\rangle\langle g|$$

Man beachte, dass die Definition von F_G abhängig von der Wahl einer Basis des Darstellungsraumes V_σ ist.

Lemma 3.3.1 *F_G ist unitär.*

3.4 Weak Fouriersampling im NAHSP

Schritt 1: Erzeuge den Zustand

$$|G\rangle := \frac{1}{|G|} \sum_{x \in G} |x\rangle \in H^A.$$

Schritt 2: Wende das Gatter U_f an und erhalte

$$\frac{1}{|G|} \sum_{x \in G} |x\rangle \otimes |\widetilde{f(x)}\rangle \in H^A \otimes H^B.$$

Hier ist wie im AHSP $m = |S|$ und $H^B := {}^qH^{\otimes m}$.
Schritt 3: Vergiss das zweite Register H^B. Der Zustand in H^A wird dann beschrieben durch den Dichteoperator

$$\rho^A = \rho_H := \frac{1}{|G|} \sum_{x \in G} |xH\rangle\langle xH|,$$

wobei wir für $x \in G$

$$|xH\rangle := \frac{1}{\sqrt{|H|}} \sum_{h \in H} |xh\rangle$$

definieren. Man nennt ρ_H den "hidden subgroup state". Eine Rechnung zeigt nun, dass $F_G \rho_H F_G^*$ bezüglich der gewählten Basis die Matrixdarstellung

$$F_G \rho_H F_G^* = \frac{1}{|G|} \bigoplus_{\sigma \in \hat{G}} (I_{d_\sigma} \otimes \sigma(H)^*) \text{ mit } \sigma(H) := \sum_{h \in H} \sigma(h) \in M_{d_\sigma}(\mathbb{C})$$

hat. Die Matrix zu $F_G \rho_H F_G^*$ ist also eine Blockdiagonalmatrix der Form

$$\begin{pmatrix} \ddots & & \\ & \frac{1}{|G|}\sigma(H)^* & \\ & & \ddots \end{pmatrix}_{\sigma \in \hat{G}}$$

Da diese Matrix Blockdiagonalgestallt hat, kann man $\sigma \in \hat{G}$ messen, und zwar mit der Wahrscheinlichkeit

$$P(\sigma) = \frac{d_\sigma}{|G|} \sum_{h \in H} \chi_\sigma(h) = \frac{d_\sigma |H|}{|G|} \left(1_H, \mathrm{Res}_H^G(\sigma)\right.\,.$$

Es stellt sich nun die Frage, ob diese Informationen ausreichen, um das NAHSP in polynomialer Zeit (in n) zu lösen. Im Allgemeinen geht das nicht auf diese Art und Weise, es reicht aber, um normale Untergruppen H zu finden. Falls nämlich H ein Normalteiler ist, so folgt

$$P(\sigma) = \begin{cases} \frac{d_\sigma^2 |H|}{|G|}, & \text{falls } H \subseteq \ker(\sigma), \\ 0, & \text{sonst.} \end{cases}$$

Wir können daher wie im AHSP vorgehen.

4 Literatur

Die Vorlesung orientiert sich über weite Strecken an dem Buch [Sch] von Wolfgang Scherer. Ein sehr einfacher Einstieg ist durch [Hom] gegeben. Aus diesem Buch ist die Präsentation von Simons Algorithmus entnommen. Ein wichtiges Buch in dieser Theorie ist [NC00]. Ihm ist unter anderem die Darstellung des Phasenschätzers entnommen.

Für das HSP (und auch anderes) sind [CvD10] und [HRTS03] interessant.

Literatur

[CvD10] Andrew M. Childs and Wim van Dam, *Quantum algorithms for algebraic problems*, Rev. Modern Phys. **82** (2010), no. 1, 1–52. MR 2629607

[Hom] Matthias Homeister, *Quantum computing verstehen.*

[HRTS03] Sean Hallgren, Alexander Russell, and Amnon Ta-Shma, *The hidden subgroup problem and quantum computation using group representations*, SIAM J. Comput. **32** (2003), no. 4, 916–934. MR 2001890

[NC00] Michael A. Nielsen and Isaac L. Chuang, *Quantum computation and quantum information*, Cambridge University Press, Cambridge, 2000. MR 1796805

[Sch] Wolfgang Scherer, *Mathematics of quantum computing.*