QFT entfernt den Shift

Lemma Entfernen des Shifts durch QFT

$$\mathrm{QFT}_{mr}|z_{r,b}\rangle = \frac{1}{\sqrt{r}} \sum_{\ell=0}^{r-1} e^{2\pi i \frac{b}{r}\ell} |m\ell\rangle$$

Beweis:

- Es gilt $\mathrm{QFT}_{mr}|z_{r,b}\rangle = \frac{1}{\sqrt{m}} \sum_{k=0}^{m-1} \mathrm{QFT}_{mr}|kr+b\rangle$. Umformung liefert
$$\frac{1}{\sqrt{m^2 r}} \sum_{y=0}^{mr-1} \sum_{k=0}^{m-1} e^{2\pi i \frac{kr+b}{mr} y} |y\rangle$$
- Wir ziehen den vom Shift b abhängigen Term aus der 1. Summe
$$\frac{1}{\sqrt{m^2 r}} \sum_{y=0}^{mr-1} e^{2\pi i \frac{by}{mr}} \sum_{k=0}^{m-1} e^{2\pi i \frac{ky}{m}} |y\rangle.$$
- Für $y = m\ell$, $\ell \in \mathbb{Z}_r$ erhalten wir $e^{2\pi i \frac{by}{mr}} = e^{2\pi i \frac{b}{r}\ell}$ und $e^{2\pi i \frac{ky}{m}} = 1$.
- Dies liefert sofort die geforderte obige Formel.
- Übungsaufgabe: Rechnen Sie nach, dass für $m \not| y$ gilt
$$\sum_{k=0}^{m-1} \left(e^{2\pi i \frac{y}{m}}\right)^k = 0$$
- D.h. die restlichen Amplituden heben sich gegenseitig auf.

Finden der Ordnung von 2 in $\mathbb{Z}_{15}^*$

Beispiel: Finden der Periode von 2 in $\mathbb{Z}_{15}^*$

Gegeben: $|\mathbb{Z}_{15}^*| = 8$
Gesucht: $\mathrm{ord}_{\mathbb{Z}_{15}^*}(2)$

- Sei $f(x) = 2^x \bmod 15$ mit reversibler Einbettung U_f.
- Auf $|0^3\rangle|0^3\rangle$ wird $H_3 \otimes I_3$ und U_f angewendet. Dies liefert
$$\frac{1}{\sqrt{8}} \sum_{x=0}^{7} |x\rangle|2^x \bmod 15\rangle = \frac{1}{\sqrt{8}} \Big(|0\rangle|1\rangle + |1\rangle|2\rangle + |2\rangle|4\rangle + |3\rangle|8\rangle + |4\rangle|1\rangle + |5\rangle|2\rangle + |6\rangle|4\rangle + |7\rangle|8\rangle \Big).$$
- Angenommen wir messen $|2\rangle$ im rechten Teil.
- Dann steht in den ersten 3 Qubits der periodische Zustand
$$|z_{4,1}\rangle = \frac{1}{\sqrt{2}}(|1\rangle + |5\rangle).$$
- $\mathrm{QFT}_8(|z_{4,1}\rangle) = \frac{1}{2} \sum_{\ell=0}^{3} e^{2\pi i \frac{1}{4}\ell} |2\ell\rangle = \frac{1}{2}(|0\rangle + i|2\rangle - |4\rangle - i|6\rangle)$.
- Bei Messung von 6 erhalten wir $\frac{6}{|\mathbb{Z}_{15}^*|} = \frac{3}{4}$.
- Der Nenner impliziert $4 \mid \mathrm{ord}(2)$. Wir prüfen $2^4 = 1 \bmod 15$.

Finden der Periode ohne Vielfachheit

Problem Finden der Periode

Gegeben: n, periodischer Zustand $|z_{r,b}\rangle = \frac{1}{\sqrt{m}} \sum_{k|0 \le kr+b<2^n} |kr+b\rangle$ mit $r \le m \le \frac{2^n}{r}$, so dass $|z_{r,b}\rangle$ ein Einheitsvektor ist.

Gesucht: r

Idee der Lösung:

- Es gilt $\mathrm{QFT}_{2^n}(|z_{r,b}\rangle) = \frac{1}{\sqrt{m2^n}} \sum_{y=0}^{2^n-1} e^{2\pi i \frac{by}{2^n}} \sum_{k=0}^{m-1} e^{2\pi i \frac{kr}{2^n} y} |y\rangle$.
- Amplitude $\sum_{k=0}^{m-1} e^{2\pi i \frac{kr}{2^n} y}$ wird groß, falls y nahe einem Vielfachem von $\frac{2^n}{r}$ ist. Wir zeigen $\left| y - \frac{2^n}{r} \cdot \ell \right| \le \frac{1}{2}$ für ein $\ell \in \mathbb{Z}_r$ mit hoher Ws.
- Wegen $2^n \ge r^2$ folgt damit $\left| \frac{y}{2^n} - \frac{\ell}{r} \right| \le \frac{1}{22^n} \le \frac{1}{2r^2}$.
- Damit kommt $\frac{\ell}{r}$ in der Kettenbruchentwicklung von $\frac{y}{2^n}$ vor.
- Zeigen alternativ, dass man $\frac{r}{\gcd(\ell_1, r)}$ mittels Gittern finden kann.
- 2 Durchgänge des Algorithmus liefern $r_1 = \frac{r}{\gcd(\ell_1, r)}$, $r_2 = \frac{r}{\gcd(\ell_2, r)}$.
- Mit Ws $\ge \frac{6}{\pi^2}$ gilt $r = \mathrm{kgV}(r_1, r_2)$.

Messung von y

Lemma Gemessenes y approxiert Vielfaches von $\frac{2^n}{r}$

Mit Ws mindestens $\frac{4}{\pi^2} \geq 0.4$ erhalten wir ein y mit $\left| y - \frac{2^n}{r} \cdot \ell \right| \leq \frac{1}{2}$.

Beweisskizze:

- Sei $y_\ell = \frac{2^n}{r}\ell + \delta_\ell$ für $|\delta_\ell| \leq \frac{1}{2}$ und $p(y_\ell) = \frac{1}{m2^n} \left| \sum_{k=0}^{m-1} e^{2\pi i \frac{kr}{2^n} y_\ell} \right|^2$.
- Für die Berechnung von $p(y_\ell)$ trägt nur der Term δ_ℓ bei.
- Übung: $m2^n \cdot p(y_\ell) = \left| \frac{e^{2\pi i \frac{r}{2^n} m\delta_\ell} - 1}{e^{2\pi i \frac{r}{2^n} \delta_\ell} - 1} \right|^2 = \frac{\sin^2(\pi \frac{r}{2^n} m\delta_\ell)}{\sin^2(\pi \frac{r}{2^n} \delta_\ell)}$.
- Wegen $m \approx \frac{2^n}{r}$ und $sin(x) \approx x$ für kleine x erhalten wir

$$p(y_\ell) \approx \frac{1}{m2^n} \left(\frac{\sin(\pi\delta_\ell)}{\pi \frac{r}{2^n} \delta_\ell} \right)^2 \approx \frac{1}{r} \left(\frac{\sin(\pi\delta_\ell)}{\pi\delta_\ell} \right)^2 .$$

- Es gilt $\sin(x) \geq \frac{2}{\pi}x$ für $x \in [0, \frac{\pi}{2}]$, d.h. $p(y_\ell) \geq \frac{1}{r} \left(\frac{\frac{2}{\pi}\pi\delta_\ell}{\pi\delta_\ell} \right)^2 = \frac{1}{r}\frac{4}{\pi^2}$.
- Ws gilt für alle $p(y_\ell)$ mit $\ell \in \mathbb{Z}_r$, d.h. wir messen ein y mit Ws $\geq \frac{4}{\pi^2}$.

Berechnen von $r/\gcd(\ell, r)$

Lemma Berechnen von ℓ und r

Sei $y \in \mathbb{Z}$ mit $\left| y - \frac{2^n}{r} \cdot \ell \right| \leq \frac{1}{2}$ und $\ell \in \mathbb{Z}_r$, $r^2 \leq 2^n$. Dann kann $\frac{r}{\gcd(\ell,r)}$ in Zeit $\mathcal{O}(n^2)$ berechnet werden.

Beweisskizze:

- Es gilt $yr - 2^n\ell = x$ für ein $x \in \mathbb{Z}$ mit $|x| \leq \frac{r}{2}$.
- Seien r', ℓ', x' die durch $\gcd(\ell, r)$ gekürzten Unbekannten r, ℓ, x.
- Definieren $f(r', x') = yr' - x'$ mit $f(r', x') = 0 \bmod 2^n$.
- f ist modulares lineares Polynom mit Nullstelle (r', x'), so dass
$$|r' \cdot x'| \leq r' \cdot \frac{r}{2} \leq 2^{n-1}.$$
- Vorlesung Kryptanalyse: r', x' werden in Zeit $\mathcal{O}(n^2)$ gefunden, sofern $|r' \cdot x'|$ kleiner als der Modul 2^n ist.
- Sei $B = \begin{pmatrix} 1 & y \\ 0 & 2^n \end{pmatrix}$. Dann gilt $(r', -\ell') \cdot B = (r', x')^t$ und (r', x') ist eine kürzeste ganzzahlige Linearkombination von Vektoren aus B.
- D.h. ein kürzester Vektor liefert $r' = \frac{r}{\gcd(\ell,r)}$.

Gaußalgorithmus

Definition Gitter

Sei $B \in \mathbb{Z}^{2\times 2}$. Wir bezeichnen mit $L(B) = \{\mathbf{x} \in \mathbb{Z}^2 \mid \mathbf{a}B = \mathbf{x}, \mathbf{a} \in \mathbb{Z}^2\}$ das von den Vektoren von B aufgespannte *Gitter*. Wir verwenden für die Länge von Gittervektoren $\mathbf{x} = (x_1, x_2)$ die ℓ_2-Norm $\|\mathbf{x}\| = \sqrt{x_1 + x_2}$.

Algorithmus Gaußalgorithmus

EINGABE: Basis $B = \begin{pmatrix} \mathbf{b_1} \\ \mathbf{b_2} \end{pmatrix} \in \mathbb{Z}^{2\times 2}$

1. Subtrahiere vom längeren Basisvektor ein ganzzahliges Vielfaches des kürzeren Basisvektors, das die Norm minimiert.
2. Vertausche die beiden Vektoren.
3. Iteriere Schritte 1+2 solange sich die Norm in Schritt 1 verkürzt.

AUSGABE: Reduzierte Basis

Gaußalgorithmus liefert kürzeste Vektoren

Fakt Gaußalgorithmus

Der Gaußalgorithmus liefert bei Eingabe einer Basis B mit maximalem Basiseintrag b_m in Zeit $\mathcal{O}(\log^2 b_m)$ eine reduzierte Basis mit kürzestem Gittervektor in $L(B)$.

Shor's Algorithmus (1994)

Algorithmus Shor's Algorithmus zum Finden der Ordnung

EINGABE: a, N

1. Benötigen $2^n \geq N^2 \geq \phi^2(N)$, d.h. wähle $n = \lceil 2 \log N \rceil$.
2. Sei U_f die reversible Einbettung von $f(x) = a^x \bmod N$.
3. Wende auf $|0^n\rangle|0^n\rangle$ zunächst $H_n \otimes I_n$ dann U_f an. Liefert
$$\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle|a^x \bmod N\rangle = \sum_{b=0}^{r-1} \left(\frac{1}{\sqrt{2^n}} \sum_{k=0}^{m-1} |kr+b\rangle \right) |a^b \bmod N\rangle.$$
4. Messen der hinteren n Register liefert in den ersten n Registern
$$|z_{r,b}\rangle = \frac{1}{\sqrt{m}} \sum_{k=0}^{m-1} |kr+b\rangle.$$
5. Berechne $\mathrm{QFT}_{2^n}(|z_{r,b}\rangle)$ und messe ein y_1.
6. Wiederhole Schritte 1-5 für ein y_2.
7. Berechne $r_1 = \frac{r}{\gcd(\ell_1, r)}$, $r_2 = \frac{r}{\gcd(\ell_2, r)}$ aus y_1, y_2 mit Gauß-Alg.
8. Berechne $r = \mathrm{kgV}(r_1, r_2)$. Falls $a^r \neq 1 \bmod N$, Ausgabe "Fehler".

AUSGABE: $r = \mathrm{ord}_{\mathbb{Z}_N *}(a)$

Finden der Ordnung von 2 in $\mathbb{Z}_{21}^*$

Beispiel: Finden der Periode von 2 in $\mathbb{Z}_{21}^*$

- Wähle der Einfachheit halber nur $n = 6$. Wir erhalten
$$\frac{1}{8}\sum_{x=0}^{63}|x\rangle|2^x \bmod 21\rangle = \frac{1}{\sqrt{8}}\Big(|0\rangle|1\rangle + |1\rangle|2\rangle + \quad \ldots \quad + |5\rangle|11\rangle$$
$$\vdots$$
$$+|60\rangle|1\rangle + |61\rangle|2\rangle + |62\rangle|4\rangle + |63\rangle|8\rangle\Big).$$
- Messung von $|4\rangle$ im rechten Teil liefert im linken Teil
$$|z_{6,2}\rangle = \frac{1}{\sqrt{11}}\sum_{i=0}^{10}|10k+2\rangle.$$
- $\mathrm{QFT}_{2^6}(|z_{6,2}\rangle)$ und Messung liefert ein $y = 11\ell$ mit Ws $\geq \frac{4}{\pi^2}$.
- Bei Messung von $y = 11 \cdot 1$ erhalten wir die Gitterbasis
$$B = \begin{pmatrix} 1 & 11 \\ 0 & 64 \end{pmatrix}.$$
- Gaußalgorithmus liefert kürzesten Vektor $(6, 2) = (r, x)$ in $L(B)$.
- Wir prüfen $2^r = 2^6 = 1 \bmod 21$.