VORLESUNG 12

13.7.2021

Sei $N \in \mathbb{N}$ und $G := \left(\mathbb{Z}/N\mathbb{Z}\right)^\times$. Sei $0 \le x < N$ mit $ggT(x, N) = 1$. Sei $\bar{x} \in G$ die Restklasse von x.

Ziel: Bestimme $\mathrm{ord}(\bar{x}) =: r$

Sei $0 \le s < r$. Dann definiert man

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

und

$$L = \lceil \log_2 N \rceil$$

$$U : \mathcal{H}^{\otimes L} \longrightarrow \mathcal{H}^{\otimes L}$$

$$|y\rangle \longmapsto \begin{cases} |xy \bmod N\rangle, & 0 \le y < N \\ |y\rangle, & \text{sonst} \end{cases}$$

Dann:

- $U|u_s\rangle = e^{2\pi i \frac{s}{r}} |u_s\rangle, \quad 0 \le s < r$
- $|1\rangle = \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |u_s\rangle$

Wir wenden den Phasenschätzer auf den Zustand $|1\rangle$ im zweiten Register an und erhalten als Ausgabe

$$\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} \underbrace{|\tilde{\varphi}_s\rangle}_{\text{im ersten Register } \mathcal{H}^{\otimes t}} |u_s\rangle, \quad \text{wobei}$$

$\left| \frac{s}{r} - \underbrace{\tilde{\varphi}_s}_{\in \mathbb{Q}} \right|$ "klein" ist

Wir müssen noch zeigen, wie man aus $\tilde{\varphi}_s$ die Ordnung r bestimmt.

<u>Satz:</u> Sei $\frac{s}{r} \in \mathbb{Q}$ mit $\left| \frac{s}{r} - \tilde{\varphi} \right| \leq \frac{1}{2r^2}$.

Dann ist $\frac{s}{r}$ ein Teilkettenbruch in der Kettenbruchentwicklung von $\tilde{\varphi}$. Diesen Teilkettenbruch kann man in $O(L^3)$ Operationen berechnen.

Den Satz können wir anwenden, <u>denn:</u>

$$\left| \frac{s}{r} - \tilde{\varphi}_s \right| \leq \frac{1}{2 \cdot 2^{2L}} \leq \frac{1}{2r^2}, \text{ da}$$

$$r \leq N \leq 2^L.$$

<u>Zusammenfassung:</u> Der Kettenbruchalgorithmus liefert effizient teilerfremde Brüche $\frac{s'}{r'} = \frac{s}{r}$.

Dann ist r' ein Kandidat für r. Falls $x^{r'} \equiv 1 \pmod N$, so sind wir fertig.

Der Kettenbruchalgorithmus

<u>Beispiel:</u> $\frac{31}{13} = 2 + \frac{5}{13} = 2 + \frac{1}{\frac{13}{5}}$

$$= 2 + \frac{1}{2+\frac{3}{5}} = 2 + \frac{1}{2+\frac{1}{\frac{5}{3}}}$$

$$= 2 + \frac{1}{2+\frac{1}{1+\frac{2}{3}}} = 2 + \frac{1}{2+\frac{1}{1+\frac{1}{\frac{3}{2}}}}$$

$$= 2 + \frac{1}{2+\frac{1}{1+\frac{1}{1+\frac{1}{2}}}}$$

"Abspalten und invertieren".

<u>Def.:</u> Sei $a_0 \in \mathbb{Z}$ und $a_1, \dots, a_n \in \mathbb{N}$.
Dann definiert man

$$[a_0; a_1, \dots, a_n] := a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots \cfrac{1}{a_{n-1} + \cfrac{1}{a_n}}}}.$$

Dies nennt man einen (endlichen) <u>Kettenbruch.</u>

<u>Kettenbruchalgorithmus:</u> Sei $x \in \mathbb{R}$, $x \neq 0$.
Definiere $f_0 := \frac{1}{x}$ und für $j > 0$

$$f_j := \frac{1}{f_{j-1}} - \left\lfloor \frac{1}{f_{j-1}} \right\rfloor \in [0,1).$$

Falls $f_j = 0$, so endet die Reihe mit f_{j-1}.
Setze: $a_j := \left\lfloor \frac{1}{f_j} \right\rfloor$

Man kann zeigen: Sei $x \in \mathbb{R}$, $x \neq 0$. Dann gilt:

$x \in \mathbb{Q} \iff$ der Kettenbruchalgorithmus bricht ab.

Beispiele:

$$\frac{12}{5} = 2 + \frac{2}{5} = 2 + \frac{1}{\frac{5}{2}}$$

$$= 2 + \frac{1}{2 + \frac{1}{2}} = [2; 2, 2]$$

Teilbrüche: $2, \frac{5}{2}, \frac{12}{5}$

$$\pi = [3; 7, 15, 1, 292, 1, 1, 1, 2, \dots]$$

Teilbrüche: $3, \quad 3 + \frac{1}{7} = \frac{22}{7}, \frac{333}{106}, \frac{355}{113}, \dots$

Satz: Sei $x \in \mathbb{Q}$ und $\frac{p}{q} \in \mathbb{Q}$ mit

$$\left| \frac{p}{q} - x \right| \leq \frac{1}{2q^2}.$$

Dann ist $\frac{p}{q}$ ein Teilbruch in der Kettenbruchentwicklung von x.

Folg: Falls $ggT(p, q) = 1$ und p, q L-Bit ganze Zahlen sind, so kann man die Kettenbruchentwicklung in $O(L^3)$-Operationen

berechnen.

ohne Beweise (Literatur: [Scherer, Anhang E])

Anwendung: Im Algorithmus von Shor ist $x = \tilde{\varphi} = \frac{b}{2^t}$, $0 \le b < 2^t$. Also kann man die Kettenbruchentwicklung in $O(t^3)$ Operationen berechnen. Einrichtung: $t = 2L+1+\lceil \log_2(2+\frac{1}{2\varepsilon}) \rceil$,

$$L = \lceil \log_2 N \rceil .$$

Was kann schief gehen?

- $\frac{s}{r}$ ist nicht gekürzt. Dann liefert der Kettenbruchalgorithmus nur einen Teiler r' von r. Starte dann einen neuen Versuch.
- Mit Wahrscheinlichkeit $\varepsilon > 0$ liefert der Phasenschätzer einen falschen Schätzwert. Starte einen neuen Versuch.

Der Algorithmus zur Berechnung von $r = \mathrm{ord}(\bar{x})$.

Input: (1) Eine Black box $U_{x,N}$ die

$$|j\rangle|k\rangle \longmapsto |j\rangle|x^j k \bmod N\rangle$$

für $0 \le x < 2^L$, $\mathrm{ggT}(x,N) = 1$, $L = \lceil \log_2 N \rceil$, berechnet.

(2) $t = 2L + 1 + \left\lceil \log_2 \left(2 + \frac{1}{2\varepsilon}\right) \right\rceil$ qBits, präpariert im Zustand $|0\rangle$

(3) L qBits im Zustand $|1\rangle$

Output: $r = \mathrm{ord}(\bar{x})$ mit "großer Wahrscheinlichkeit"

Laufzeit: $O(L^3)$ Operationen.

1. Initialisiere $|0\rangle \otimes |1\rangle$ in ${}^qH^{\otimes t} \otimes {}^qH^{\otimes L}$

2. $\longrightarrow \frac{1}{\sqrt{2^t}} \sum_{j=0}^{2^t-1} |j\rangle \otimes |1\rangle$ (erster Schritt im Phasenraster)

3. $\longrightarrow \frac{1}{\sqrt{2^t}} \sum_{j=0}^{2^t-1} |j\rangle \otimes |x^j \bmod N\rangle$ (wende $U_{x,N}$ an)

$$= \frac{1}{\sqrt{r\,2^t}} \sum_{s=0}^{r-1} \left(\sum_{j=0}^{2^t-1} e^{2\pi i s j / r} |j\rangle \right) \otimes |u_s\rangle$$

$$= \frac{1}{\sqrt{2^t}} \sum_{s=0}^{r-1} \left(\sum_{\substack{j=0 \\ j \equiv s \,(\mathrm{mod}\, r)}}^{2^t-1} |j\rangle \right) \otimes |x^s \bmod N\rangle$$

4. Wende die inverse QFT an

$$\longrightarrow \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} \left| \frac{\tilde{s}}{r} \right\rangle \otimes |u_s\rangle$$

5. Messung im ersten Register $\longrightarrow \frac{\tilde{s}}{r} \in \mathbb{Q}$

6. Wende den Kettenbruchalgorithmus auf $\frac{\tilde{s}}{r}$.
Dieser liefert

$$\frac{p_1}{q_1}, \frac{p_2}{q_2}, \text{----}, \quad \text{mit } ggT(p_i, q_i) = 1.$$

Falls $x^{q_i} \equiv 1 \pmod N$, so gilt $r = q_i$.
Andernfalls gehe zu 1.

Erläuterung: (1) $\sum_{j=0}^{2^t-1} e^{2\pi i s j / r} |j\rangle$

$$= \sum_{j=0}^{2^t-1} e^{2\pi i \left(\frac{s}{r} 2^t\right) j / 2^t} |j\rangle$$

$$= F \left| \frac{s}{r} \cdot 2^t \right\rangle \quad , \text{ falls } \frac{s}{r} \cdot 2^t \in \mathbb{N}$$

Wir würden also exakt $\frac{s}{r} = \frac{\frac{s}{r} \cdot 2^t}{2^t}$ bestimmen. Im Allgemeinen erhalten wir nur gute 2^t Approximationen

(2) $$F^{-1}\left(\frac{1}{\sqrt{2^t}} \sum_{s=0}^{r-1} \left(\sum_{\substack{j=0 \\ j \equiv s \,(\mathrm{mod}\, r)}}^{2^t-1} |j\rangle \right) \otimes |x^s \bmod N\rangle \right)$$

$$= \frac{1}{\sqrt{2^t}} \sum_{s=0}^{r-1} F^{-1}\left(\sum_{\substack{j=0 \\ j \equiv s \,(\mathrm{mod}\, r)}}^{2^t-1} |j\rangle \right) \otimes |x^s \bmod N\rangle$$

Faktorisierungsalgorithmus

Input: Eine zusammengesetzte Zahl N mit mindestens 2 Primfaktoren.

Output: Ein nicht-trivialer Faktor von N.

Laufzeit: $O\left(\lceil \log_2 N \rceil^3\right)$

Schritt 1: Wähle $b \in \mathbb{N}$ mit $1 \leq b < N$ und bestimme $ggT(b, N)$. Falls $ggT(b, N) > 1$, so gibt $ggT(b, N)$ aus. Sonst gehe zu Schritt 2.

Schritt 2: Bestimme $r := ord(\overline{b})$ mit Quantenalgorithmus oben. Falls r ungerade ist, so gehe zu Schritt 1. Falls r gerade ist, gehe zu Schritt 3.

Schritt 3: Berechne $ggT(N, b^{r/2} \pm 1) =: d$. Falls $1 < d < N$, so gib d aus. Sonst gehe zu Schritt 1.