Vorlesung 11

06.07.2021

Phasenschätzung

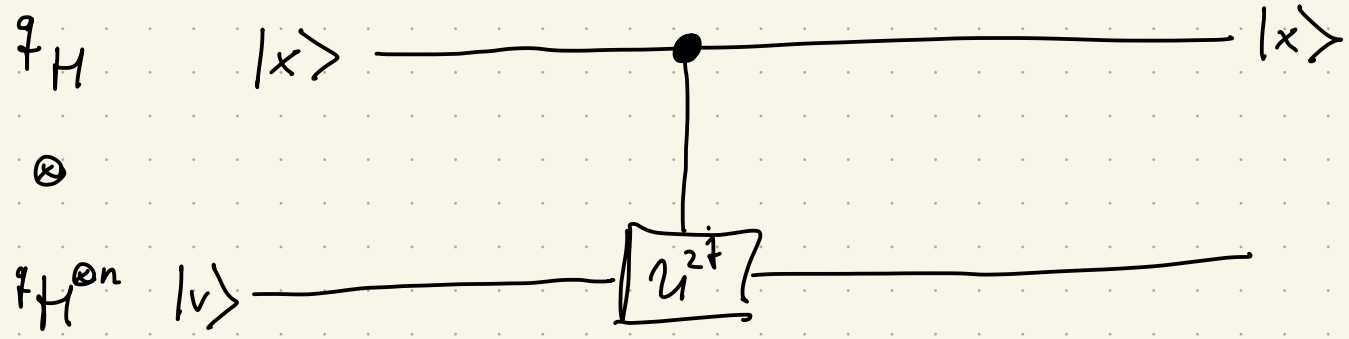
Sei $U : \mathbb{C}^{2^n} \to \mathbb{C}^{2^n}$ unitär und u sei ein EV. Sei

$$U|u\rangle = e^{2\pi i \varphi}|u\rangle, \quad 0 \le \varphi < 1.$$

ZIEL: Berechne eine gute Approximation an φ.

Voraussetzungen: Wir haben eine black box, die folgendes leistet: sie präpariert $|u\rangle$ und berechnet kontrolliertes U^{2^j} für $j \in \mathbb{N}_0$.

Zur Erinnerung:



tut das folgende $|0\,v\rangle \mapsto |0\,v\rangle$

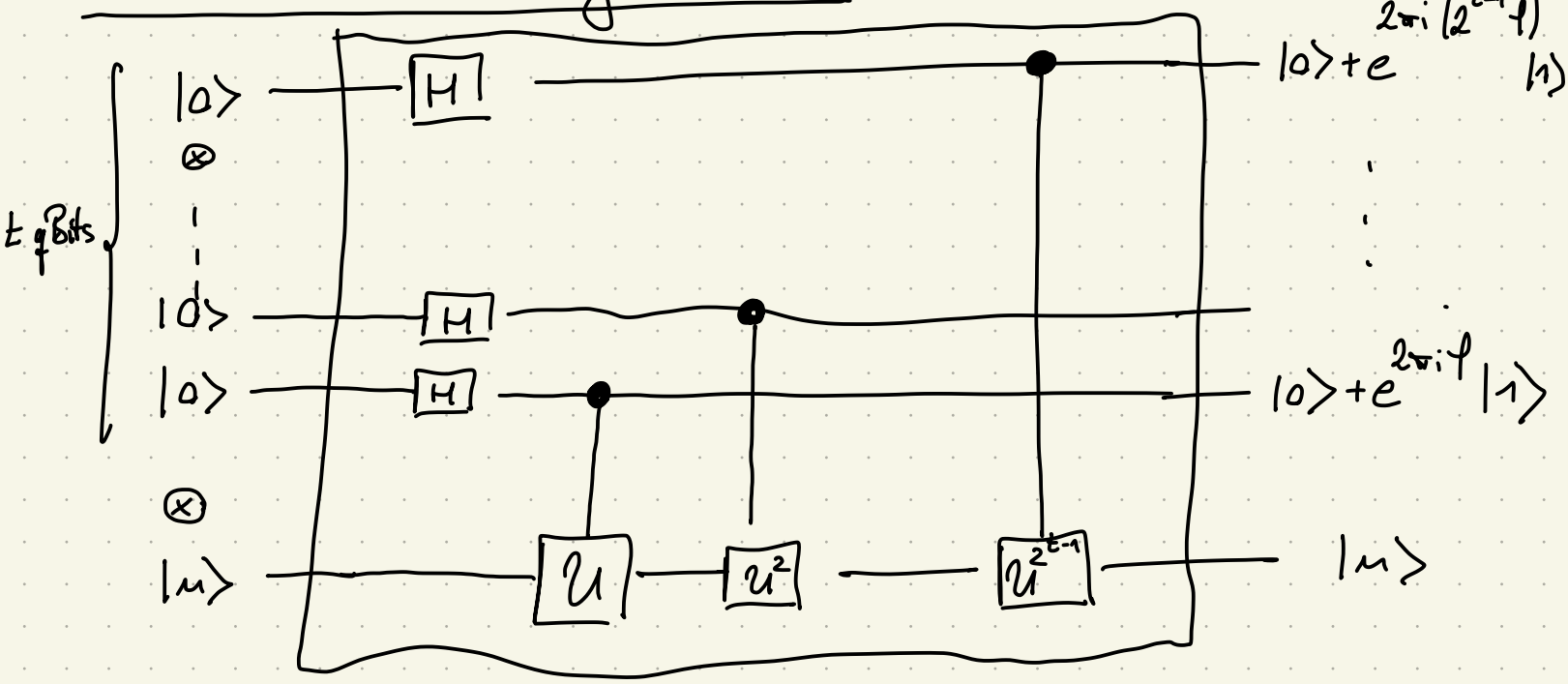
$|1\,v\rangle \mapsto |1\rangle \otimes U^{2^j}|v\rangle.$

Der Algorithmus nutzt zwei Register:

1) t qBits, zu Anfang auf $|0\rangle$ gesetzt.

2) q_H qBits, zu Anfang im Zustand $|u\rangle$

1. Schritt des Algorithmus:



Zweiter Schritt: Führe eine inverse QFT F^{-1} durch.

Dritter Schritt: Simultane Messung von σ_j^z, $j = 0, \dots, t-1$ im ersten Register, wobei

$$\sigma_j^z := \mathrm{id} \otimes \cdots \otimes \mathrm{id} \otimes \sigma_z \otimes \mathrm{id} \otimes \cdots \otimes \mathrm{id}.$$

Lemma: Sei $x = \sum_{j=0}^{n-1} x_j \cdot 2^j$. Dann ist

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

Motivation / Intuition:

Angenommen $\varphi = 0.\varphi_1 \ldots \varphi_t = \frac{\varphi_1}{2} + \ldots + \frac{\varphi_t}{2^t}$

Dann erhalten wir nach dem ersten Schritt

$$\frac{1}{2^{t/2}} \left(|0\rangle + e^{2\pi i 0.\varphi_1 \ldots \varphi_t} |1\rangle \right) \otimes \ldots \otimes \left(|0\rangle + e^{2\pi i 0.\varphi_t} |1\rangle \right)$$

Aufgrund des Lemmas liefert F^{-1} (eventuell nach einer Permutation S) dann

$$|\varphi_1 \ldots \varphi_t\rangle.$$

Dies ist ein Eigenzustand von jedem

$$\sigma_j := id \otimes \ldots \otimes \sigma_z \otimes \ldots \otimes id$$

$\uparrow$ j-te Stelle

Die simultane Messung von σ_j, $j = 0, \ldots, t-1$ liefert dann die exakte Periode.

Bemerkung: Das Herzstück des Algorithmus ist die inverse QFT.

Wie gut ist die Approximation $\tilde{\varphi}$ an φ in Abhängigkeit von t? $\quad \epsilon(Q)$

Sei dazu $0 \le b \le 2^t - 1$, $\delta : \varphi - \frac{b}{2^t}$ minimal mit $\delta > 0$. Also: $0 \le \delta \le \frac{1}{2^t}$.

ZIEL: Die Messung m mit $0 \le m < 2^t$ soll mit großer Wahrscheinlichkeit nahe bei b liegen.

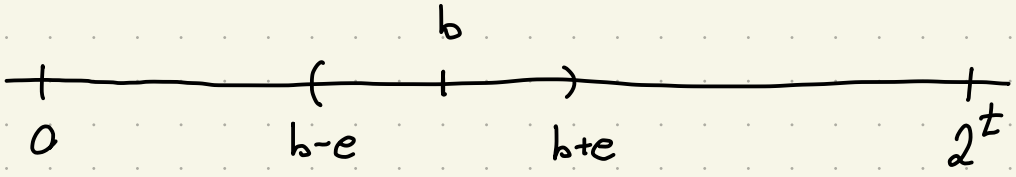
Wende QFT^{-1} an auf

$$\frac{1}{2^{t/2}} \sum_{k=0}^{2^t-1} e^{2\pi i \varphi k} |k\rangle$$

Dies liefert

$$\frac{1}{2^t} \sum_{k=0}^{2^t-1} e^{2\pi i \varphi k} \sum_{l=0}^{2^t-1} e^{-2\pi i k l / 2^t} |l\rangle$$

$$= \sum_{l=0}^{2^t-1} \underbrace{\left(\frac{1}{2^t} \sum_{k=0}^{2^t-1} e^{2\pi i k (\varphi - l)/2^t} \right)}_{\alpha_l} |l\rangle$$



Sei $e > 1$ eine vorgegebene Fehlertoleranz.

Dann gilt:

$$p(|m-b| > e) = \sum_{\substack{\ell=0 \\ |\ell-b|>e}}^{2^b-1} |\alpha_\ell|^2$$

$$\leq \frac{1}{2(e-1)}$$

(elementare Rechnungen, Nielsen/Chuang S. 224)

Falls man $\tilde{\varphi} := \frac{m}{2^t}$ bestimmen will, so daß

$$|\varphi - \tilde{\varphi}| \leq \frac{1}{2^n}, \quad n \in \mathbb{N} \text{ gegeben},$$

gilt, so hat man

$$e = 2^{t-n} - 1$$

zu setzen, denn:

$$|\varphi - \frac{m}{2^t}| \leq |\varphi - \frac{b}{2^t}| + |\frac{b}{2^t} - \frac{m}{2^t}|$$

$$\leq \frac{1}{2^t} + \frac{1}{2^t}\,|b-m|$$

$$\leq \frac{1}{2^t} + \frac{e}{2^t} \leq \frac{1}{2^n}$$

Setze: $t = n+p$, $e = 2^p - 1$. Dann ist die Wahrscheinlichkeit eine Approximation

$$\tilde{\varphi} = \frac{m}{2^t} \quad \text{mit} \quad |\varphi - \tilde{\varphi}| \leq \frac{1}{2^n}$$

zu erhalten größer

$$1 - \frac{1}{2(2^p-2)}.$$

Sei $\varepsilon > 0$. Will man φ erfolgreich mit Fehler $\leq \frac{1}{2^n}$ und Wahrscheinlichkeit $1-\varepsilon$ bestimmen, so muss gelten

$$1 - \frac{1}{2(2^p-2)} \geq 1 - \varepsilon$$

$$\Leftrightarrow \quad p \geq \log_2\left(2 + \frac{1}{2\varepsilon}\right).$$

Nimm: $t = n + \left\lceil \log_2\left(2 + \frac{1}{2\varepsilon}\right) \right\rceil$.

Motivation: Sei $N \in \mathbb{N}$ zu faktorisieren.

Versuche eine Kongruenz

$$x^2 \equiv 1 \pmod{N} \qquad (*)$$

zu finden. Dann folgt

$$N \mid x^2 - 1 = (x+1)(x-1)$$

Falls q ein Primteiler von N ist, so folgt

$$q \mid (x+1) \quad \text{oder} \quad q \mid (x-1)$$

d.h. $\operatorname{ggT}(N, x+1) > 1$ oder $\operatorname{ggT}(N, x-1) > 1$.

Zu x mit $(*)$ berechne mit euklidischem Algorithmus

$$\operatorname{ggT}(N, x \pm 1)$$

Falls $x \not\equiv \pm 1 \pmod{N}$, so finden wir einen nicht-trivialen Teiler.

Wie also erzeugt man Kongruenzen der Form $(*)$:

- Wähle zufällig $a \in \left(\mathbb{Z}/N\mathbb{Z}\right)^\times$ und berechne $r := \operatorname{ord}(a)$, d.h.

$$r := \min \{ m \in \mathbb{N} : a^m \equiv 1 \pmod N \}$$

Also ist r die Periode von $m \mapsto a^m$

- Mit "großer Wahrscheinlichkeit" ist r gerade und für $x := a^{r/2}$ gilt:

$$x \not\equiv \pm 1 \pmod N.$$

Die Quantenanteil in Shors Algorithmus ist die Berechnung von r.

Anwendung der Phasenschätzung:
Ordnungsbestimmung und Faktorisierung

Problem: Sei $N \in \mathbb{N}$ und $G = \left(\mathbb{Z}/N\mathbb{Z}\right)^\times$.
Sei $0 \le x < N$, $\operatorname{ggT}(x, N) = 1$. Dann ist $\bar{x} \in G$ und wir wollen $\operatorname{ord}(\bar{x})$ bestimmen.

Betrachte dazu den unitären Operator

$$U : {}^q\mathcal{H}^{\otimes L} \longrightarrow {}^q\mathcal{H}^{\otimes L}, \quad L = \lceil \log_2 N \rceil$$

$$|y\rangle \longmapsto \begin{cases} |xy \bmod N\rangle, & 0 \le y < N \\ |y\rangle, & N \le y < 2^L - 1 \end{cases}$$

Sei $r := \mathrm{ord}(\bar{x})$.

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

$0 \le s \le r-1$, sind Eigenzustände von U.

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

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

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

∎

Wir werden sehen: Aus der Kenntnis von einer guten Näherung an $\frac{s}{r}$ kann mit großer Wahrscheinlichkeit r berechnet.

Problem: Die Präparation von $|u_s\rangle$ erfordert die Kenntnis von r.

Es gilt: $\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |u_s\rangle = |1\rangle$

Dann:

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

$$= \frac{1}{r} \sum_{k=0}^{r-1} \left(\sum_{s=0}^{r-1} \underbrace{\exp\left(\frac{-2\pi i k}{r}\right)^s}_{r\text{-te EHW}} \right) |x^k \bmod N\rangle$$

$$\underbrace{\neq 1 \text{, für } k \neq 0}_{\begin{cases} = 0, \text{ für } k \neq 0 \\ = r, \text{ für } k = 0 \end{cases}}$$

$$= |1\rangle.$$

∎

Präpariert man den Zustand $|1\rangle$ und wendet den Phasensatz an, so erhält man intuitiv die Ausgabe

$$\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |\tilde{\varphi}_s\rangle |u_s\rangle \text{, wobei } \left|\frac{s}{r} - \tilde{\varphi}_s\right| \text{ klein ist.}$$

Liest man das erste Register dann erhält man $|\tilde{\varphi}_s\rangle$ mit Wahrscheinlichkeit $\frac{1}{r}$.

Setzt man $t = 2L+1 + \left\lceil \log\left(2 + \frac{1}{2\varepsilon}\right) \right\rceil$, fixiert s, dann erhält man $\tilde{\varphi}_s \approx \frac{s}{r} = \varphi_s$ mit einer Genauigkeit von $2L+1$ Bits mit der Wahrscheinlichkeit $\geq \frac{1-\varepsilon}{r}$

Bemerke: r ist in der Anwendung sehr groß. Das macht nichts, denn mit großer Wahrscheinlichkeit misst man $\frac{\tilde{s}}{r}$ mit $ggT(s,r) = 1$. Dann kann man mit der Kettenbruchentwicklung aus $\frac{\tilde{s}}{r}$ die exakten Werte s und r berechnen.

Ein weiteres Problem: Es ist kontrolliertes U^{2^t} für $U|y\rangle = \begin{cases} |xy \bmod N\rangle, & 0 \le y < N \\ |y\rangle, & \text{sonst} \end{cases}$

effizient berechnen.

Dazu ist zu berechnen

$$|z\rangle|y\rangle \longmapsto |z\rangle U^{z_0} U^{z_1 2} \cdots U^{z_{t-1} 2^{t-1}} |y\rangle$$

$$= |z\rangle U^z |y\rangle$$

$$= \begin{cases} |z\rangle |x^z y \bmod N\rangle, & 0 \le y < N \\ |x\rangle, & \text{sonst} \end{cases}$$

x^z kann man schnell berechnen. Beispiel:

$3^{13} \pmod{10}$

$13 = 1 + 0 \cdot 2 + 1 \cdot 2^2 + 1 \cdot 2^3$

$3 \mapsto 3 \cdot 3^2 = 7 \mapsto 7^2 = 9 \mapsto 3 \cdot 9^2 = 3$

$x \cdot x^2 \qquad (x \cdot x^2)^2 = x((x \cdot x^2)^2)^2$

Dies kann man nutzen, um einen Quantenschaltkreis zu konstruieren, der $|z\rangle|y\rangle \mapsto |x^z y \bmod N\rangle$ unter Benutzung von $O(L^3)$ elementaren Gattern berechnet (siehe [Scherer, Kapitel 5.3.6])