Phase estimation

Vortrag im Rahmen des Seminars

"Quanten, Computer, Algorithmen"

der WE AℓZAGK im Sommersemester 2001

von

Marc Suling

12. & 19. Juni 2001

nach

Michael Nielsen, Ike Chuang :

"Quantum Computation and Quantum Information",

Cambridge Univ. Press, 2000

Ausgangspunkt

Die **phase estimation** (=Phasenabschätzung) ist ein Verfahren, welches in verschiedenen Quanten-Algorithmen zur Anwendung kommt, allen voran in dem von *Shor* vorgestellten Faktorisierungs-Algorithmus (vgl. Vortrag von *Dirk Stadil*), also lohnt es sich, diese Phasenabschätzung einmal näher zu betrachten.

Es geht im allgemeinen darum, mit einer vorher bestimmten Genauigkeit in einem Eigenzustand zu einem Eigenwert die Phase dieses Eigenwertes zu bestimmen. Es wird eine Methode vorgestellt, diese Genauigkeit mit einer frei wählbaren Wahrscheinlichkeit zu erreichen.

Wir haben gegeben :

- einen unitären Operator U
- einen Eigenzustand $|u\rangle$ zum Eigenwert $e^{2\pi i\varphi}$
- eine "black box", die folgende Operation ausführt :

$$\frac{1}{\sqrt{2^t}}\sum_{j=0}^{2^t-1}|j\rangle|u\rangle \longrightarrow \frac{1}{\sqrt{2^t}}\sum_{j=0}^{2^t-1}|j\rangle U^j|u\rangle = \frac{1}{\sqrt{2^t}}\sum_{j=0}^{2^t-1}e^{2\pi ij\varphi}|j\rangle|u\rangle$$

  Hier soll darauf hingewiesen werden, dass es im Moment nicht darauf ankommt, wie diese "black box" genau aussieht, dies ist ein Problem der konkreteren Anwendung der phase estimation.

Mit Hilfe der Phasenabschätzung wollen wir nun also die Phase φ des Eigenwertes $e^{2\pi i\varphi}$ zum Eigenzustand $|u\rangle$ mit einer vorher bestimmten Wahrscheinlichkeit abschätzen.

Vorgehensweise

Zunächst werden wir die grobe Vorgehensweise darlegen, welche dann im Anschluss näher analysiert wird. Der Algorithmus besteht aus 5 Schritten :

1.	$\|0\rangle\|u\rangle$	Anfangszustand
2.	$\frac{1}{\sqrt{2^t}}\sum_{j=0}^{2^t-1}\|j\rangle\|u\rangle$	Hadamard-Transformation auf das 1. Register anwenden
3.	$\frac{1}{\sqrt{2^t}}\sum_{j=0}^{2^t-1}\|j\rangle U^j\|u\rangle$ $= \frac{1}{\sqrt{2^t}}\sum_{j=0}^{2^t-1}e^{2\pi ij\varphi}\|j\rangle\|u\rangle$	"black box" anwenden
4.	$\rightarrow \|\varphi\rangle\|u\rangle$	inverse QuantenFourierTransformation anwenden
5.	$\rightarrow \varphi$	Messen des 1. Registers

Diese Schritte wollen wir nun etwas näher beleuchten.

Betrachtung eines einfachen Spezialfalles

Wir beginnen mit unserem Anfangszustand $|0\rangle|u\rangle$. Das erste Register besteht aus t Qubits, wobei wir später sehen werden, wie t gewählt werden sollte. Das zweite Register hat gerade soviele Qubits, wie nötig sind, um $|u\rangle$ darzustellen.

Auf das erste Register wenden wir nun die Hadamard-Transformation an (vgl. Vortrag von *Jörg Trommer*) :

$$|0\rangle|u\rangle \quad \longrightarrow \quad R^{(t)}|0\rangle|u\rangle = \frac{1}{\sqrt{2^t}} \sum_{j=0}^{2^t-1} |j\rangle|u\rangle$$

Damit befindet sich das 1. Register in Superposition, das 2. Register ist nach wie vor unverändert.

Nun kommt die "black box" zur Anwendung. Wie diese im speziellen aussieht, ist nicht wichtig, jedoch besteht sie im wesentlichen in der Anwendung sukzessiver Zweierpotenzen von U. Damit erhalten wir den Zustand

$$\frac{1}{\sqrt{2^t}}(|0\rangle+e^{2\pi i 2^{t-1}\varphi}|1\rangle)(|0\rangle+e^{2\pi i 2^{t-2}\varphi}|1\rangle)\cdots(|0\rangle+e^{2\pi i 2^{0}\varphi}|1\rangle)|u\rangle = \frac{1}{\sqrt{2^t}} \sum_{k=0}^{2^t-1} e^{2\pi i\varphi k}|k\rangle|u\rangle \quad (1)$$

Die Summendarstellung ist uns bekannt aus dem einem Vortrag von *Jens Gamst* und wird später im allgemeinen Teil eine Rolle spielen.

Nehmen wir nun einmal an, das gesuchte φ liesse sich mit genau t Qubits darstellen, dann gäbe es eine Darstellung

$$\varphi = 0.\varphi_1\varphi_2\ldots\varphi_t = \sum_{j=1}^{t} \varphi_j 2^{-j}$$

Wenn wir eine solche Darstellung haben, können wir unseren Zustand (1) auch umschreiben in die Form :

$$\frac{1}{\sqrt{2^t}}(|0\rangle + e^{2\pi i 0.\varphi_t}|1\rangle)(|0\rangle + e^{2\pi i 0.\varphi_{t-1}\varphi_t}|1\rangle)\cdots(|0\rangle + e^{2\pi i 0.\varphi_1\varphi_2\ldots\varphi_t}|1\rangle)|u\rangle \quad (2)$$

und das ist im 1. Register gerade die Produktdarstellung einer QuantenFourierTransformation (vgl. Vortrag von *Jens Gamst* über die QFT). Die QFT ist invertierbar, und wir wollen nun die inverse QFT auf das 1.Register unseres Zustandes (2) anwenden :

$$\frac{1}{\sqrt{2^t}}(|0\rangle+e^{2\pi i 0.\varphi_t}|1\rangle)(|0\rangle+e^{2\pi i 0.\varphi_{t-1}\varphi_t}|1\rangle)\cdots(|0\rangle+e^{2\pi i 0.\varphi_1\varphi_2\ldots\varphi_t}|1\rangle)|u\rangle \overset{\mathrm{QFT}^{-1}}{\longrightarrow} |\varphi_1\varphi_2\ldots\varphi_t\rangle|u\rangle$$

Wenn wir jetzt das 1. Register messen, haben wir gerade das gesuchte φ gefunden.

In diesem speziellen Fall also liefert uns die Phasenabschätzung genau das gesuchte Ergebnis, aber was ist, wenn die Voraussetzungen nicht so günstig sind, sich also φ nicht durch genau t Qubits darstellen lässt ?

Betrachtung des allgemeinen Falles

Sein nun $b \in \mathbb{N}, b \leq 2^t - 1$ derart, dass $\frac{b}{2^t} = 0.b_1 b_2 \dots b_t$ die beste t-Bit-Approximation von φ mit $\frac{b}{2^t} < \varphi$ ist. Für die Differenz δ gelte :

$$\delta := \varphi - \frac{b}{2^t}, \quad 0 < \delta < 2^{-t}$$

Das Ziel ist nun, zu zeigen, dass die Phasenabschätzung ein Ergebnis m liefert, welches mit hoher Wahrscheinlichkeit nahe an b liegt und damit auch nahe an φ.

Wenden wir in diesen allgemeinen Fall die inverse QFT auf unseren Zustand (1) an, so erhalten wir :

$$\frac{1}{\sqrt{2^t}} \sum_{k=0}^{2^t-1} e^{2\pi i \varphi k} |k\rangle |u\rangle \overset{\text{QFT}^{-1}}{\longrightarrow} \frac{1}{2^t} \sum_{k,l=0}^{2^t-1} e^{-\frac{2\pi i k l}{2^t}} e^{2\pi i \varphi k} |l\rangle |u\rangle \tag{3}$$

Im folgenden wollen wir eine Abschätzung für die Wahrscheinlichkeit finden, dass das Messergebnis m der Phasenabschätzung von b weiter als ϵ entfernt liegt, wobei hier ϵ eine von uns zugelassene Fehlertoleranz ist, auf die wir später noch näher eingehen werden. Wir wollen also folgende Wahrscheinlichkeit abschätzen :

$$p\big(|m - b| > \epsilon\big)$$

Diese Wahrscheinlichkeit kann identifiziert werden mit :

$$p\big(|m - b| > \epsilon\big) = \sum_{l=-2^{t-1}+1}^{-(\epsilon+1)} |\alpha_l|^2 + \sum_{l=\epsilon+1}^{2^{t-1}} |\alpha_l|^2 \tag{4}$$

wobei die α_l jeweils die Amplituden zu den l sind. Diese Amplituden sind aber gegeben durch die Koeffizienten der $|l\rangle$ in der Darstellung (3). Diese Koeffizienten haben die Form

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

und da wir in den Exponenten modulo 2^t rechnen, ersetzen wir nun l durch $b + l$ und summieren noch immer über die selben Terme und erhalten als Amplituden α_l :

$$\begin{aligned}
\alpha_l &= \frac{1}{2^t} \sum_{k=0}^{2^t-1} e^{-\frac{2\pi i k (b+l)}{2^t}} e^{2\pi i k \varphi} \\
&= \frac{1}{2^t} \sum_{k=0}^{2^t-1} e^{2\pi i k (\varphi - (b+l) \cdot \frac{1}{2^t})} \\
&= \frac{1}{2^t} \sum_{k=0}^{2^t-1} \Big(e^{2\pi i (\varphi - (b+l) \cdot \frac{1}{2^t})} \Big)^k
\end{aligned}$$

Dieses ist aber eine Partialsumme einer geometrischen Reihe, und wir erhalten damit

weiter :

$$\begin{aligned}\alpha_l &= \frac{1}{2^t}\cdot\frac{1-\left(e^{2\pi i(\varphi-(b+l)\cdot\frac{1}{2^t})}\right)^{2t}}{1-e^{2\pi i(\varphi-(b+l)\cdot\frac{1}{2^t})}}\\ &= \frac{1}{2^t}\cdot\frac{1-e^{2\pi i(2^t\varphi-(b+l))}}{1-e^{2\pi i(\varphi-(b+l)\cdot\frac{1}{2^t})}}\end{aligned}$$

Jetzt erinnern wir uns daran, dass gilt :

$$\delta=\varphi-\frac{b}{2^t}\quad\Longleftrightarrow\quad 2^t\delta=2^t\varphi-b$$

und erhalten damit vorerst :

$$\alpha_l=\frac{1}{2^t}\cdot\frac{1-e^{2\pi i(2^t\delta-l)}}{1-e^{2\pi i(\delta-\frac{l}{2^t})}}$$

Wegen $|1-e^{i\theta}|\leq 2$ folgt :

$$\begin{aligned}|\alpha_l| &= \frac{1}{2^t}\cdot\left|\frac{1-e^{2\pi i(2^t\delta-l)}}{1-e^{2\pi i(\delta-\frac{l}{2^t})}}\right|\\ &\leq \frac{2}{2^t\cdot\left|1-e^{2\pi i(\delta-\frac{l}{2^t})}\right|}\end{aligned}$$

Für eine weitere Abschätzung zeigen wir folgende

Behauptung 1 : Für alle $\theta\in[-\pi,\pi]$ gilt :

$$|1-e^{i\theta}|\geq 2|\theta|\frac{1}{\pi}$$

Beweis : Bekannt ist :

$$\begin{aligned}|1-e^{i\theta}|^2 &= (1-e^{i\theta})(1-e^{-i\theta})\\ &= e^{i\frac{\theta}{2}}(e^{-i\frac{\theta}{2}}-e^{i\frac{\theta}{2}})\cdot e^{-i\frac{\theta}{2}}(e^{i\frac{\theta}{2}}-e^{-i\frac{\theta}{2}})\\ &= 4\sin^2\frac{\theta}{2}\end{aligned}$$

Daher können wir die Behauptung zunächst auf die Ungleichung

$$4\sin^2\frac{\theta}{2}\geq\frac{4}{\pi^2}\theta^2$$

und damit auf

$$\sin\frac{\theta}{2}\geq\frac{1}{\pi}\theta\qquad\theta\in[0,\pi]$$

reduzieren.
Nun ist aber $(\sin\frac{\theta}{2})''=-\frac{1}{4}\sin\frac{\theta}{2}<0$, und damit ist $(\sin\frac{\theta}{2})$ im Intervall $[0,\pi]$ konkav, liegt also über der Geraden $\frac{1}{\pi}\theta$.
Damit ist die Behauptung gezeigt.

Behauptung 2 : Für $-2^{t-1}+1 \leq l \leq 2^{t-1}$ gilt :

$$-1 < 2(\delta - \frac{l}{2^t}) < 1$$

Beweis : Zum Beweis der Behauptung betrachten wir die 2 Extremfälle :

(1) Sei $l = -2^{t-1}+1$. Dann gilt :

$$\begin{array}{rccccl} & -1 & < & 2\delta - 2^{-t+1} + 1 & < & 1 \qquad \text{nach Def. von } \delta \\ \Rightarrow & -1 & < & 2\delta + \frac{2^{t-1}-1}{2^{t-1}} & < & 1 \\ \Rightarrow & -1 & < & 2\delta - \frac{-2^{t-1}+1}{2^{t-1}} & < & 1 \\ \Rightarrow & -1 & < & 2\delta - \frac{l}{2^{t-1}} & < & 1 \end{array}$$

(2) Sei $l = 2^{t-1}$. Dann gilt :

$$\begin{array}{rccccl} & -1 & < & 2\delta - 1 & < & 1 \qquad \text{nach Def. von } \delta \\ \Rightarrow & -1 & < & 2\delta - \frac{2^{t-1}}{2^{t-1}} & < & 1 \\ \Rightarrow & -1 & < & 2\delta - \frac{l}{2^{t-1}} & < & 1 \end{array}$$

Damit ist die Behauptung bewiesen.

Behauptung 2 liefert :

$$-\pi \leq 2\pi\Big(\delta - \frac{l}{2^t}\Big) \leq \pi$$

Nun können wir weiter abschätzen :

$$\begin{aligned} |\alpha_l| &\leq \frac{2}{2^t \cdot \left|1 - e^{2\pi i(\delta - \frac{l}{2^t})}\right|} \\ &\leq \frac{2}{2^t \cdot 2\left|2\pi(\delta - \frac{l}{2^t})\right| \cdot \frac{1}{\pi}} \\ &= \frac{1}{2^{t+1}\left|\delta - \frac{l}{2^t}\right|} \end{aligned}$$

Wenn wir diese Abschätzung der Amplituden in (4) einsetzen, erhalten wir als Abschätzung für die gesuchte Wahrscheinlichkeit :

$$p\big(|m-b| > \epsilon\big) \leq \sum_{l=-2^{t-1}+1}^{-(\epsilon+1)} \left|\frac{1}{2^{t+1}\left|\delta - \frac{l}{2^t}\right|}\right|^2 + \sum_{l=\epsilon+1}^{2^{t-1}} \left|\frac{1}{2^{t+1}\left|\delta - \frac{l}{2^t}\right|}\right|^2$$

Dies wollen wir nun mittels einfacher Umformungen noch weiter vereinfachen :

$$\begin{aligned}
p\big(|m-b|>\epsilon\big) &\leq \sum_{l=-2^{t-1}+1}^{-(\epsilon+1)} \left| \frac{1}{2^{t+1}\big|\delta-\frac{l}{2^t}\big|} \right|^2 + \sum_{l=\epsilon+1}^{2^{t-1}} \left| \frac{1}{2^{t+1}\big|\delta-\frac{l}{2^t}\big|} \right|^2 \\
&= \frac{1}{4}\left(\sum_{l=-2^{t-1}+1}^{-(\epsilon+1)} \frac{1}{(l-2^t\delta)^2} + \sum_{l=\epsilon+1}^{2^{t-1}} \frac{1}{(l-2^t\delta)^2} \right) \\
&\leq \frac{1}{4}\left(\sum_{l=-2^{t-1}+1}^{-(\epsilon+1)} \frac{1}{l^2} + \sum_{l=\epsilon+1}^{2^{t-1}} \frac{1}{(l-1)^2} \right) \\
&= \frac{1}{4}\left(\sum_{l=-2^{t-1}+1}^{-(\epsilon+1)} \frac{1}{l^2} + \sum_{l=\epsilon}^{2^{t-1}-1} \frac{1}{l^2} \right) \\
&\leq \frac{1}{2} \sum_{l=\epsilon}^{2^{t-1}-1} \frac{1}{l^2} \\
&\leq \frac{1}{2} \int_{l=\epsilon-1}^{2^{t-1}-1} \frac{1}{l^2}\ dl \\
&= \frac{1}{2}\Big[-\frac{1}{l}\Big]_{\epsilon-1}^{2^{t-1}-1} \\
&= \frac{1}{2(\epsilon-1)}
\end{aligned}$$

Nun haben wir also eine schöne Abschätzung für die gesuchte Wahrscheinlichkeit gefunden. Diese hängt wesentlich von ϵ ab, worauf im folgenden näher eingegangen werden soll. Die Frage, die sich nun stellt, ist : Wie muss t gewählt sein, um die gewünschte Genauigkeit mit der gewünschten Wahrscheinlichkeit zu erreichen ?

Dies wollen wir nun erörtern.

Genaue Bestimmung von t

Wollen wir das φ mit einer Genauigkeit von 2^{-n} bestimmen, müssen wir zunächst das ϵ bestimmen, von dem die eben gefundene Abschätzung abhängt. Dazu betrachten wir

$$\begin{array}{rrcll} & |\varphi - \frac{m}{2^t}| & = & 2^{-n} & \\ \Rightarrow & |\varphi - \frac{m}{2^t}| & > & 2^{-n} - 2^{-t} & \\ \Rightarrow & |\frac{b}{2^t} - \frac{m}{2^t}| & > & 2^{-n} - 2^{-t} & \text{da } |\varphi - \frac{b}{2^t}| < 2^{-t} \\ \Rightarrow & |b - m| & > & 2^{t-n} - 1 & \end{array}$$

Nun setzen wir $\epsilon = 2^{t-n} - 1$.

Sei nun $t = n + p$, dann folgt sofort :

$$\epsilon = 2^p - 1$$

Mit der obigen Abschätzung haben wir nun eine untere Schranke für die Wahrscheinlichkeit, eine gute Näherung für φ zu erhalten, gefunden :

$$p\big(|m - b| \leq \epsilon\big) \geq 1 - \frac{1}{2(2^p - 2)}$$

Wollen wir nun also φ auf mindestens n Bits mit einer Wahrscheinlichkeit von mindestens $1 - \varepsilon$ approximieren, dann wählen wir $p = \log_2(\frac{1}{2\varepsilon} + 2)$, denn es ist

$$\Big[p = \log_2\big(\frac{1}{2\varepsilon} + 2\big)\Big] \quad \Leftrightarrow \quad \Big[\varepsilon = \frac{1}{2(2^p - 2)}\Big]$$

und erhalten somit :

$$t = n + \log_2\big(\frac{1}{2\varepsilon} + 2\big).$$