Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Enrico Thomae

Lösungsblatt zur Vorlesung

Quantenalgorithmen

WS 2011/2012

Blatt 1 / 17. Oktober 2011

Abgabe bis 31. Oktober 2011, 14 Uhr (vor der Übung)

AUFGABE 1 (5 Punkte)**:**
Gegeben seien zwei Zustände $|x_0\rangle = \frac{1}{2}\mathrm{e}^{i\frac{\pi}{4}}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle$ und $|x_1\rangle = \frac{2}{3}i|0\rangle + \frac{\sqrt{5}}{3}|1\rangle$.

(a) Berechnen Sie $\langle x_0|x_0\rangle$, $\langle x_1|x_1\rangle$ und $\langle x_0|x_1\rangle$.

(b) Geben Sie die Amplituden der Basiszustände $|01\rangle$ und $|10\rangle$ im Zwei-Bit-Register $|x_0x_1\rangle$ an.

Lösungsvorschlag:

(a) Es gilt $\langle x_0|x_0\rangle = \langle \begin{pmatrix} \frac{1}{2}e^{-i\frac{\pi}{4}} \\ \frac{\sqrt{3}}{2} \end{pmatrix} | \begin{pmatrix} \frac{1}{2}e^{i\frac{\pi}{4}} \\ \frac{\sqrt{3}}{2} \end{pmatrix} \rangle = (\frac{1}{2}e^{-i\frac{\pi}{4}}) \cdot (\frac{1}{2}e^{i\frac{\pi}{4}}) + \left(\frac{\sqrt{3}}{2}\right)^2 = \frac{1}{4} + \frac{3}{4} = 1.$

Es gilt $\langle x_1|x_1\rangle = \langle \begin{pmatrix} -\frac{2}{3}i \\ \frac{\sqrt{5}}{3} \end{pmatrix} | \begin{pmatrix} \frac{2}{3}i \\ \frac{\sqrt{5}}{3} \end{pmatrix} \rangle = (-\frac{2}{3}i) \cdot (\frac{2}{3}i) + \left(\frac{\sqrt{5}}{3}\right)^2 = \frac{4}{9} + \frac{5}{9} = 1.$

Es gilt $\langle x_0|x_1\rangle = \langle \begin{pmatrix} \frac{1}{2}e^{-i\frac{\pi}{4}} \\ \frac{\sqrt{3}}{2} \end{pmatrix} | \begin{pmatrix} \frac{2}{3}i \\ \frac{\sqrt{5}}{3} \end{pmatrix} \rangle = (\frac{1}{2}e^{-i\frac{\pi}{4}}) \cdot (\frac{2}{3}i) + (\frac{\sqrt{3}}{2}) \cdot (\frac{\sqrt{5}}{3}) = \frac{2}{6}ie^{-i\frac{\pi}{4}} + \frac{\sqrt{15}}{6} = \frac{1}{3}e^{i\frac{\pi}{4}} + \frac{\sqrt{15}}{6}.$

(b) Für das Zwei-Bit-Register $|x_0x_1\rangle$ gilt:

$|x_0x_1\rangle = |x_0\rangle \otimes |x_1\rangle = (\frac{1}{2}e^{i\frac{\pi}{4}}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle) \otimes (\frac{2}{3}i|0\rangle + \frac{\sqrt{5}}{3}|1\rangle) = \frac{1}{3}e^{i\frac{3\pi}{4}}|00\rangle + \frac{\sqrt{5}}{6}e^{i\frac{\pi}{4}}|01\rangle + \frac{\sqrt{3}}{3}i|10\rangle + \frac{\sqrt{15}}{6}|11\rangle.$
Somit ergeben sich für $|01\rangle$ bzw. $|10\rangle$ Amplituden von $\frac{\sqrt{5}}{6}e^{i\frac{\pi}{4}}$ bzw. $\frac{\sqrt{3}}{3}i$.

AUFGABE 2 (5 Punkte)**:**
Seien $|x\rangle = \frac{1}{5}(-3, 4)$, $|y\rangle = \frac{1}{5}(4, 3) \in \mathbb{C}^2$.

(a) Zeigen Sie, das $|x\rangle, |y\rangle$ eine orthonormale Basis des $\mathbb{C}^2$ bilden.

(b) Konstruieren Sie mittels Tensorprodukt-Konstruktion aus $|x\rangle, |y\rangle$ eine orthonormale Basis des $\mathbb{C}^4$.

Lösungsvorschlag:

(a) Es ist zu zeigen, dass $|x\rangle, |y\rangle$ Einheitsvektoren sind und senkrecht aufeinander stehen. Es muss also $||x\rangle| = ||y\rangle| = 1$ und $\langle x|y\rangle = 0$ gelten.
Es gilt $||x\rangle| = \sqrt{\langle x|x\rangle} = \sqrt{\frac{1}{25}((-3)^2 + 4^2)} = \sqrt{\frac{1}{25} \cdot 25} = 1$.
Für $||y\rangle|$ gilt:$||y\rangle| = \sqrt{\langle y|y\rangle} = \sqrt{\frac{1}{25}(4^2 + 3^2)} = 1$.
Weiter gilt: $\langle x|y\rangle = \frac{1}{25}((-3) \cdot 4 + 4 \cdot 3) = 0$.
Somit bilden $|x\rangle, |y\rangle$ eine orthonormale Basis.

(b) Da $\{|x\rangle, |y\rangle\}$ orthonormale Basis des $\mathbb{C}^2$ ist, ist eine orthonormale Basis des $\mathbb{C}^4$ durch $\{|xx\rangle, |xy\rangle, |yx\rangle, |yy\rangle\}$ gegeben. Für diese Vektoren gilt:
$|xx\rangle = |x\rangle \otimes |x\rangle = \frac{1}{5}(-3, 4) \otimes \frac{1}{5}(-3, 4) = \frac{1}{25}(9, -12, -12, 16)$.
$|xy\rangle = \frac{1}{25}(-12, -9, 16, 12)$.
$|yx\rangle = \frac{1}{25}(-12, 16, -9, 12)$.
$|yy\rangle = \frac{1}{25}(16, 12, 12, 9)$.

AUFGABE 3 (3 Punkte)**:**
Es seien die Abbildungen $M_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ und $\sqrt{M_1} = \begin{pmatrix} \frac{1+i}{2} & \frac{1-i}{2} \\ \frac{1-i}{2} & \frac{1+i}{2} \end{pmatrix}$ gegeben. Zeigen Sie, dass $\sqrt{M_1}$ unitär ist und $\left(\sqrt{M_1}\right)^2 = M_1$ gilt.

Lösungsvorschlag:

$\sqrt{M_1}$ ist genau dann unitär, wenn $(\sqrt{M_1}^*)^T = \sqrt{M_1}^{-1}$, d.h. $(\sqrt{M_1}^*)^T \cdot \sqrt{M_1} = I_2$ gilt. Hier gilt $(\sqrt{M_1}^*)^T = \left(\begin{pmatrix} \frac{1+i}{2} & \frac{1-i}{2} \\ \frac{1-i}{2} & \frac{1+i}{2} \end{pmatrix}^*\right)^T = \begin{pmatrix} \frac{1-i}{2} & \frac{1+i}{2} \\ \frac{1+i}{2} & \frac{1-i}{2} \end{pmatrix}$.
Es folgt $(\sqrt{M_1}^*)^T \cdot \sqrt{M_1} = \begin{pmatrix} \frac{1-i}{2} & \frac{1+i}{2} \\ \frac{1+i}{2} & \frac{1-i}{2} \end{pmatrix} \cdot \begin{pmatrix} \frac{1+i}{2} & \frac{1-i}{2} \\ \frac{1-i}{2} & \frac{1+i}{2} \end{pmatrix}$
$= \frac{1}{4} \begin{pmatrix} 2+2 & (1-i)^2 + (1+i)^2 \\ (1+i)^2 + (1-i)^2 & 2+2 \end{pmatrix} = \frac{1}{4} \begin{pmatrix} 4 & -2i + 2i \\ 2i - 2i & 4 \end{pmatrix} = I_2$.
Somit ist $\sqrt{M_1}$ unitär.

Betrachte $\sqrt{M_1}^2$ so gilt:
$\sqrt{M_1}^2 = \begin{pmatrix} \frac{1+i}{2} & \frac{1-i}{2} \\ \frac{1-i}{2} & \frac{1+i}{2} \end{pmatrix} \cdot \begin{pmatrix} \frac{1+i}{2} & \frac{1-i}{2} \\ \frac{1-i}{2} & \frac{1+i}{2} \end{pmatrix} = \frac{1}{4} \begin{pmatrix} (1+i)^2 + (1-i)^2 & 2+2 \\ 2+2 & (1-i)^2 + (1+i)^2 \end{pmatrix} =$
$\frac{1}{4} \begin{pmatrix} 2i - 2i & 4 \\ 4 & -2i + 2i \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = M_1$.

AUFGABE 4 (5 Punkte)**:**
Gegeben seien $|x_0\rangle = |0\rangle$ und $|x_1\rangle = \frac{\sqrt{3}}{2}|0\rangle + \frac{i}{2}|1\rangle$. Finden Sie eine unitäre Abbildung U mit $|x_0\rangle = U|x_1\rangle$.

Bonusfrage (+1 Punkt): Wie viele solcher unitärer Abbildungen gibt es?

Lösungsvorschlag:

Sei $U_0 := \frac{1}{2}\begin{pmatrix}\sqrt{3} & i \\ i & \sqrt{3}\end{pmatrix}$. Dann hat U_0 die gewünschten Eingenschaften:

Zeige: U_0 ist unitär
$(U_0{}^*)^T = \frac{1}{2}\begin{pmatrix}\sqrt{3} & -i \\ -i & \sqrt{3}\end{pmatrix}$.
Also gilt: $(U_0{}^*)^T \cdot U_0 = \frac{1}{4}\begin{pmatrix}\sqrt{3} & -i \\ -i & \sqrt{3}\end{pmatrix} \cdot \begin{pmatrix}\sqrt{3} & i \\ i & \sqrt{3}\end{pmatrix} = \frac{1}{4}\begin{pmatrix}3+1 & \sqrt{3}i - \sqrt{3}i \\ -\sqrt{3}i + \sqrt{3}i & 1+3\end{pmatrix} = I_2$.
U_0 ist also unitär.

Bleibt $|x_0\rangle = U_0|x_1\rangle$ zu zeigen:
$U|x_1\rangle = \frac{1}{2}\begin{pmatrix}\sqrt{3} & -i \\ -i & \sqrt{3}\end{pmatrix}(\frac{\sqrt{3}}{2}|0\rangle + \frac{i}{2}|1\rangle) = \frac{1}{2}(\frac{\sqrt{3}}{2}(\sqrt{3}|0\rangle - i|1\rangle) + \frac{i}{2}(-i|0\rangle + \sqrt{3}|1\rangle))$
$= \frac{3}{4}|0\rangle - \frac{\sqrt{3}i}{4}|1\rangle + \frac{1}{4}|0\rangle + \frac{\sqrt{3}i}{4}|1\rangle = |0\rangle = |x_0\rangle$.

U_0 ist eine Drehmatrix (U_0 unitär und $\det U_0 = 1$), die $|x_1\rangle$ auf $|x_0\rangle$ dreht. Scharfes Hinsehen liefert, dass es sich um eine Drehung um $-\frac{\pi}{6}$ handelt.
U_0 lässt sich auch als

$$U_0 = \begin{pmatrix}\cos(-\frac{\pi}{6}) & -i\sin(-\frac{\pi}{6}) \\ -i\sin(-\frac{\pi}{6}) & \cos(-\frac{\pi}{6})\end{pmatrix}$$

schreiben. Somit erhalten wir unendlich abzählbar viele Matrizen durch

$$U_k := \begin{pmatrix}\cos(-\frac{\pi}{6} + 2k\pi) & -i\sin(-\frac{\pi}{6} + 2k\pi) \\ -i\sin(-\frac{\pi}{6} + 2k\pi) & \cos(-\frac{\pi}{6} + 2k\pi)\end{pmatrix}$$

mit $k \in \mathbb{Z}$.
Offensichtlich liefert U_k für alle $k \in \mathbb{Z}$ die gleiche Rotationsmatrix wie U_0, da sin und cos 2π-periodisch sind. U_k entspricht dabei einer Drehung um $-\frac{\pi}{6} + 2k\pi$.