Ruhr-Universität Bochum
Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Gottfried Herold

Präsenzübungen zur Vorlesung

Quantenalgorithmen

SS 2016

Blatt 1 / 18. April 2016

AUFGABE 1:

Betrachte ein Qubit mit Basiszuständen $|0\rangle, |1\rangle$ sowie Zustände

$|x\rangle = \frac{4i}{5}|0\rangle + \frac{3}{5}|1\rangle$
$|y\rangle = \frac{3}{5}|0\rangle + \frac{4i}{5}|1\rangle$
$|z\rangle = \frac{1+i}{2}|0\rangle + \frac{1-i}{2}|1\rangle$

(a) Zeigen Sie, dass $|x\rangle, |y\rangle, |z\rangle$ Einheitsvektoren sind.

(b) Schreiben Sie $\langle y|$ als Linearkombination von $\langle 0|$ und $\langle 1|$.

(c) Berechnen Sie $\langle y|x\rangle$, $\langle x|y\rangle$, $\langle y|z\rangle$, $\langle z|y\rangle$, $\langle x|z\rangle$ sowie $\langle z|x\rangle$.

(d) Schreiben Sie $|z\rangle$ als Linearkombination von $|x\rangle$ und $|y\rangle$.

Bei einer Messung an einem Qubit gibt es immer zwei mögliche Ergebnisse. Normalerweise sind diese $|0\rangle, |1\rangle$, soweit nicht anders spezifiziert. Abhängig von der physikalischen Realisierung ist es manchmal auch möglich, in einer anderen Basis $|v\rangle, |w\rangle$ zu messen, wobei $|v\rangle, |w\rangle$ ein Orthonormalsystem sein müssen.

(e) Nehmen Sie an, das Qubit ist im Zustand $|z\rangle$ und Sie messen in der Basis $|x\rangle, |y\rangle$. Was sind die möglichen Zustände des Qubits nach der Messung und mit welchen Wahrscheinlichkeiten treten diese möglichen Züstände jeweils ein?

AUFGABE 2:

Zeigen Sie, dass die unitären $n \times n$ Matrizen eine Gruppe bilden.

Bitte wenden!

AUFGABE 3:

Wir betrachten nun *äußere Produkte* von der Form $|\alpha\rangle\langle\beta|$.

(a) Betrachten Sie

$$M_\neg = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Schreiben Sie $M_\neg$ als Linearkombination von $|0\rangle\langle 0|$, $|0\rangle\langle 1|$, $|1\rangle\langle 0|$, $|1\rangle\langle 1|$.

Sei $|v\rangle$ ein beliebiger Einheitsvektor. Wir betrachten den *Projektionsoperator* $P_{|v\rangle} = |v\rangle\langle v|$.

(b) Zeigen Sie: $P_{|v\rangle}^\dagger := (P_{|v\rangle}^*)^T = P_{|v\rangle}$ sowie $P_{|v\rangle}^2 = P_{|v\rangle}$.

(c) Sei $|v_1\rangle, \ldots, |v_m\rangle$ eine Orthonormalbasis. Dann gilt $\sum_i P_{|v_i\rangle} = \mathrm{id}$.