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

Präsenzübungen zur Vorlesung

Quantenalgorithmen

SS 2016

Blatt 3 / 23. Mai 2016

AUFGABE 1:

Geben Sie einen Schaltkreis über $\{\neg, \wedge, \vee\}$ an, der die Summe aus einer 2-Bit Zahl x_1x_0 und einer 1-Bit Zahl y_0 berechnet. Was ist die Komplexität Ihres Schaltkreises?

AUFGABE 2:

Geben Sie einen Schaltkreis über $\{\text{nand}, c\}$ an, der die Summe zweier 1-Bit Zahlen x, y berechnet. Was ist die Komplexität Ihres Schaltkreises?

AUFGABE 3:

Zeigen Sie, dass die Menge $\{\oplus, \wedge, c\}$ *nicht* universell ist. Wie lässt sich dies beheben?

AUFGABE 4:

Wir bezeichnen eine unitäre Abbildung $D : \mathbb{C}^4 \to \mathbb{C}^4$ als *Quantenlöscher*, falls gilt:

$$D|0x\rangle = |yz\rangle \text{ und } D|1x\rangle = |yz\rangle$$

für beliebige Qubits $|x\rangle, |y\rangle, |z\rangle \in \mathbb{C}^2$. D.h. D überschreibt das 1. Qubit.

Zeigen Sie, dass es keinen Quantenlöscher gibt.

Bitte wenden!

AUFGABE 5:

Seien $|x\rangle, |y\rangle, |z\rangle \in \mathbb{C}^2$ drei Zustände mit $\langle x|x\rangle = \langle y|y\rangle = \langle z|z\rangle = 1$.

(a) Zeigen Sie, dass

$$1 - |\langle y|z\rangle| \leq |\langle x|y\rangle|^2 + |\langle x|z\rangle|^2 \leq 1 + |\langle y|z\rangle| \ .$$

gilt.

(b) Interpretieren Sie die Grenzfälle $\langle y|z\rangle = 0$ und $\langle y|z\rangle = 1$.

(c) Zeigen Sie, dass $|\langle x|y\rangle|^2 + |\langle x|z\rangle|^2 \leq 1 + |\langle y|z\rangle|$ auch für $|x\rangle, |y\rangle, |z\rangle \in \mathbb{C}^m$ mit $m > 2$ gilt.

Hinweis: Überlegen Sie sich, warum Sie o.B.d.A. annehmen können, dass $\langle y|z\rangle$ reell und ≥ 0 ist. Zeigen Sie dann, dass in diesem Fall $|\langle x|y\rangle|^2 + |\langle x|z\rangle|^2$ sein Maximum bzw. Minimum für $|x\rangle = \frac{|y\rangle \pm |z\rangle}{\| |y\rangle \pm |z\rangle \|}$ annimmt.