TECHNISCHE UNIVERSITÄT DARMSTADT
FACHGEBIET KRYPTOGRAPHISCHE PROTOKOLLE
Alexander May, Ulrich Vollmer
Maike Ritzenhofen

Präsenzübungen zur Vorlesung

Quantenalgorithmen

WS 2006/07

Blatt 7 / 31. Januar 2007

AUFGABE 1:
Seien $v = (v_1, \ldots, v_n)$ und $w = (w_1, \ldots, w_n)$ zwei linear unabhängige Vektoren in $\mathbb{R}^n$ der Länge 1. Geben Sie die Koordinaten eines Vektors $u \in \mathbb{R}^n$ an, für den gilt, daß

1. $|u| = 1$.
2. Es existieren $a, b \in \mathbb{R}$ derart, daß $av + bw = u$.
3. $\langle w, u \rangle = 0$.

AUFGABE 2:
Seien $v, w \in \mathbb{R}^2$ zwei linear unabhängige Vektoren.
Seien weiter U_v und U_w die linearen Abbildungen, welche einen Vektor x an $v^\perp = \{\, u \in \mathbb{R}^2 \mid \langle u, v \rangle = 0 \,\}$ bzw. $w^\perp$ spiegeln, d.h.

$$U_v(x) = \begin{cases} x & \text{falls } x \in v^\perp, \\ -x & \text{falls } x = av \text{ mit } a \in \mathbb{R}, \end{cases}$$

und analog für U_w. Zeigen Sie, daß $U_v \circ U_w$ eine Drehung um das Doppelte des Winkels $\theta = \arg(v, w)$ zwischen v und w ergibt.

AUFGABE 3:
Konstruieren Sie einen Schaltkreis aus Hadamard-, Not- und Toffoli-Gittern, der $|x_0 \ldots x_{m-1}\rangle$ auf $(-1)^{x_0 \cdot \cdots \cdot x_{m-1}} |x_0 \ldots x_{m-1}\rangle$ abbildet. Sei

$$s = \frac{1}{\sqrt{M}}$$

Können Sie auch einen Schaltkreis angeben, der $|x\rangle$ auf $|x\rangle$ abbildet, falls $\langle x, s \rangle = 0$, und s auf $-s$?