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

Hausübungen zur Vorlesung

Quantenalgorithmen

SS 2016

Blatt 6 / 1. Juli 2016

Abgabe: 11. Juli 2016, 10.00 Uhr (vor der Vorlesung), Kasten NA/02

AUFGABE 1 (7 Punkte)**:**

Wir betrachten die verallgemeinerte Datenbanksuche. Sei $f\colon \mathbb{F}_2^n \to \mathbb{F}_2$. Wir suchen *irgend ein* $x \in \mathbb{F}_2^n$ mit $f(x) = 1$. Sei $N = 2^n$ und $1 \leq M < N$ die Anzahl der Lösungen. Wir definieren

$$|\alpha\rangle = \frac{1}{\sqrt{N-M}} \sum_{f(x')=0} |x'\rangle,$$

$$|\beta\rangle = \frac{1}{\sqrt{M}} \sum_{f(x)=1} |x\rangle,$$

d.h. $|\alpha\rangle$ entspricht der Summe über alle nicht-Lösungen und $|\beta\rangle$ der Summe über alle Lösungen. Sei $|\psi\rangle := \frac{1}{\sqrt{N}} \sum_y |y\rangle$.

(a) Zeigen Sie, dass $|\alpha\rangle, |\beta\rangle$ orthogonal zueinander sind.

(b) Schreiben Sie den Zustand $|\psi\rangle$ als Linearkombination von $|\alpha\rangle$, $|\beta\rangle$.

(c) Zeigen Sie, dass die Grover-Iteration den von $|\alpha\rangle, |\beta\rangle$ aufgespannten Raum erhält. (d.h. die Grover-Iteration bildet Zustände aus diesem Unterraum wieder in diesen Unterraum ab). Zeigen Sie zudem, dass die Grover-Iteration auf diesem Unterraum die darstellende Matrix

$$G = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$

bzgl. der Basis $|\alpha\rangle, |\beta\rangle$ hat, wobei $\frac{\theta}{2}$ der Winkel zwischen $|\psi\rangle$ und $|\alpha\rangle$ ist.

Bemerkungen: Der Winkel ϕ zwischen zwei (reellwertigen) Vektoren $|\psi\rangle, |\alpha\rangle$ der Länge 1 erfüllt $\cos\phi = \langle\alpha|\psi\rangle$ (Das ist im Wesentlichen die Defition des Winkels zwischen Vektoren). Es gilt $\cos 2\phi = 2\cos^2\phi - 1$ und $\sin 2\phi = 2\sin\phi\cos\phi$.

Bitte wenden!

AUFGABE 2 (8 Punkte)**:**

Sei $f\colon \{0,1\}^4 \to \{0,1\}$, wobei es genau 3 Werte x mit $f(x) = 1$ gibt.

(a) Geben Sie den Quantenschaltkreis für Grovers Algorithmus an sowie Instruktionen, wo gemessen wird. Die Anzahl der Iterationen soll dabei der Einfachheit halber 1 betragen. Ihr Schaltkreis darf dabei ausschliesslich U_f (die reversible Einbettung von f), sowie Hadamard- und Toffoli-Gates verwenden.

(b) Was ist der Zustand nach Anwendung Ihres Schaltkreises?

(c) Geben Sie die Wahrscheinlichkeit an, dass sie ein x mit $f(x) = 1$ messen, wenn Sie 1 bzw. 2 Iterationen von Grovers-Algorithmus durchführen.

Bemerkung: Es ist ratsam, Aufgabe 1 für Aufgabe 2 zu benutzen (incl. der Notation von Aufgabe 1).

AUFGABE 3 (5 Punkte)**:**

Wir betrachten ein Public-Key Verschlüsselungsverfahren mit öffentlichem Schlüssel pk, geheimen Schlüssel sk. Der geheime Schlüssel habe n_k Bit. Das Verschlüsselungsverfahren $\mathrm{Enc}_{\mathrm{sk}}(m)$ laufe in (probabilistischer) Polynomialzeit und verschlüssele n_m-Bit Nachrichten m, wobei die Verschlüsselung randomisiert ist und n_r Zufallsbits pro Aufruf von $\mathrm{Enc}_{\mathrm{sk}}$ benötigt werden.
Der Algorithmus Enc is bekannt, ebenso pk. Der geheime Schlüssel sk ist unbekannt. Wir nehmen an, dass es einen Polynomzeitalgorithmus gibt, der bei gegebenem pk überprüft, ob ein Kandidat sk' korrekter geheimer Schlüssel ist.

Nehmen Sie an, Sie haben einen Ciphertext c, der Verschlüsselung einer uniform gewählten Nachricht m ist.

(a) Geben Sie einen Quantenalgorithmus an, um den geheimen Schlüssel sk schneller als Durchprobieren aller Schlüssel zu ermitteln. Was ist seine Komplexität?

(b) Geben Sie einen Quantenalgorithmus an, um m in erwarteter Laufzeit $\mathrm{poly}(n)\cdot\mathcal{O}(2^{\frac{n_r+n_m}{2}})$ zu ermitteln.