Lehr- und Forschungsgebiet
Mathematische Grundlagen der Informatik
RWTH Aachen
Prof. Dr. E. Grädel, D. Fischer, T. Ganzow,
B. Puchala

Complexity Theory and Quantum Computing — Assignment 11

Due: Monday, January 25, 12:00

Exercise 1

Consider the amplitude amplification by inversion about the mean as presented in the lecture, i.e., the transformation $|\varphi\rangle \mapsto \sum_{x\in\{0,1\}^n}(2\overline{a} - a_x)|x\rangle$. Prove that this transformation is linear and described by the matrix $H^{\otimes n} \cdot R_n \cdot H^{\otimes n}$ where $H^{\otimes n}$ is the n-fold tensor product of the Hadamard matrix with itself and R_n is the $2^n \times 2^n$ matrix given by

$$R_n|x\rangle = \begin{cases} |x\rangle & \text{for } x = 0\dots0 \\ -|x\rangle & \text{for } x \in \{0,1\}^n \setminus \{0\dots0\}. \end{cases}$$

Exercise 2

Let $f : \{0,1\}^n \to \{0,1\}$ be a function and let $T := \{x \mid f(x) = 1\}$. We define $|\varphi^+\rangle = \frac{1}{\sqrt{|T|}}\sum_{x\in T}|x\rangle$ and $|\varphi^-\rangle = \frac{1}{\sqrt{2^n-|T|}}\sum_{x\notin T}|x\rangle$. Moreover, let $\sin\vartheta_0 = \sqrt{\frac{|T|}{2^n}}$ and let $|\psi\rangle$ be the equal superposition of all basis state of H_{2^n}, i.e., $|\psi\rangle = H^{\otimes n}|0\dots0\rangle$.

(a) Prove that $|\psi\rangle = \sin\vartheta_0|\varphi^+\rangle + \cos\vartheta_0|\varphi^-\rangle$.

(b) Consider the mapping, induced by the Grover matrix on the two dimensional vector space with basis $(|\varphi^-\rangle, |\varphi^+\rangle)$. Prove that this mapping is described by the matrix

$$\begin{pmatrix} \cos(2\vartheta_0) & -\sin(2\vartheta_0) \\ \sin(2\vartheta_0) & \cos(2\vartheta_0) \end{pmatrix}.$$

(c) Prove that after r iterations of the Grover operator on $|\psi\rangle$, the quantum system is in the state $|\psi_r\rangle = \sin((2r+1)\vartheta_0)|\varphi^+\rangle + \cos((2r+1)\vartheta_0)|\varphi^-\rangle$.

(d) Let $|T| < \frac{3}{4}\cdot 2^n$ and let $t := \lfloor\sqrt{2^n}\rfloor + 1$. Prove that the value $y \in \{0,1\}^n$ which is chosen by the algorithm of Grover satisfies $f(y) = 1$ with a probability of $\frac{1}{2} - \frac{\sin(4t\vartheta_0)}{4t\sin(2\vartheta_0)}$.

(e) Prove the Theorem of Grover:
There is a quantum algorithm which finds, with at most $O(\sqrt{2^n})$ queries to a given function $0 \neq f : \{0,1\}^n \to \{0,1\}$, a $y \in \{0,1\}^n$ such that $f(y) = 1$ with a probability of at least $\frac{1}{4}$.

Hint: Use (without proof) that for any $\alpha \in \mathbb{R}$ and any $m \in \mathbb{N}$, the following equations hold.

- $\sin(2\alpha) = 2\sin\alpha\cos\alpha$.
- $\sum_{r=0}^{m-1}\cos((2r+1)\alpha) = \frac{\sin(2m\alpha)}{2\sin\alpha}$.
- $\cos(2\alpha) = 1 - 2\sin^2\alpha$.