Advanced Quantum Information (Exercise I)

discussion: 25.10.12

1. Bernstein-Vazirani algorithm (2 P)

Consider a function $f(\vec{x})$ which is promised to be of the form $f(\vec{x}) = \vec{a} \cdot \vec{x} \oplus b$, where $\vec{a}, \vec{x}, \vec{y}, \vec{z} \in \{0, 1\}^n$ and $b \in \{0, 1\}$. Find the unknown $n$-bit string $\vec{a}$ by using the Deutsch-Jozsa algorithm.

*Hint:* First show that $\frac{1}{2^n} \sum_{\vec{z}} (-1)^{\vec{z} \cdot (\vec{x} \oplus \vec{y})} = \delta_{\vec{x} \vec{y}}$. Here the scalar product is defined by $\vec{a} \cdot \vec{b} = (\sum_{i=1}^{n} a_i b_i) \mod 2$, and $a \oplus b = (a + b) \mod 2$.

2. Grover algorithm (8 P)

(a) Oracle of the Grover algorithm for two qubits (2 P)

The oracle "marks" the solution element $(x_s)$ by minus one, i.e. the oracle $O$ transforms the initial state to $|\Psi\rangle = \sum_x (-1)^{f(x)} |x\rangle$ with $f(x_s) = 1$ and $f(x) = 0 \ \forall \ x \neq x_s$. In the case of two qubits the corresponding unitary matrix is

$$U_O = \begin{pmatrix}
(-1)^{f(0)} & 0 & 0 & 0 \\
0 & (-1)^{f(1)} & 0 & 0 \\
0 & 0 & (-1)^{f(2)} & 0 \\
0 & 0 & 0 & (-1)^{f(3)}
\end{pmatrix}.$$  \hspace{1cm} (1)

Devise the four quantum circuits implementing the unitary transformation of the oracle for each search solution.

(b) A two qubit example of the Grover algorithm (3 P)

Calculate the unitary transformation represented by the circuit in the figure below, choosing $x_s = 2$ for the oracle transformation. Calculate the state vector after applying this transformation to the initial state $|\phi\rangle = |00\rangle$. To which step of the algorithm (lecture) does the part in the green box belong?
(c) **The Grover iteration (1 P)**

Show that $H^\otimes n(2|0\rangle \langle 0| - 1)H^\otimes n = (2|\psi_0\rangle \langle \psi_0| - 1) = U$, with $|\psi_0\rangle = \frac{1}{\sqrt{2^n}} \sum_x |x\rangle$, holds and that $U$ is a unitary transformation.

(d) **Failure probability of the Grover algorithm (2 P)**

In the lecture it was shown that the quantum state after $k$ Grover iterations has the form $G^k|\psi_0\rangle = \cos \theta_k |X_0\rangle + \sin \theta_k |X_1\rangle$, with $\theta_k = (k + 1/2)\theta$ and $\sin(\theta/2) = \sqrt{M/N}$. Here $|X_0\rangle$ denotes the vector of superpositions of all non-solution states and $|X_1\rangle$ the vector containing all solutions to the search problem. Calculate the probability ($p_w$) of getting a wrong answer after $k$ iterations. Estimate or bound the failure probability using the optimal $k$. Discuss why it may not be possible to exactly reach $p_w = 0$ for $N > 4$.

3. **The inverse modulo $n$ of $a$ (3 P)**

Derive a procedure to calculate the integer $a^{-1}$ which is the inverse modulo $n$ of $a$, i.e. $aa^{-1} \equiv 1 \pmod{n}$. Here, $a$ and $n$ are integers and $\gcd(a, n) = 1$.

4. **The Chinese remainder theorem (4 P)**

A basket with eggs of a nice lady was crushed by a soldier. He wants to refund the lady, but she does not know how many eggs were in the basket, but she knows: if she would have taken out 2 eggs at a time, at the end 1 egg would have been left. The same would have happened in the case of 3 or 5 eggs per turn. In the case of 7 eggs on the other hand, no egg would have remained. How many eggs did she have in the basket?

*Hint: Find a suitable system of congruences to different moduli and use Theorem 2 (Gauß) to solve this problem.*