Advanced Cryptography: Quantum Cryptography

MICHAEL NÜSKEN, DANIEL LOEBENBERGER

10. Exercise sheet
Hand in solutions until Monday, 17 January 2011, 23:59h.

Exercise 10.1 (Grover on a tiny database). (11 points)

Assume you are running Grover on a database of size $N = 4$.

(i) For each $x_i \in \{0, 1, 2, 3\}$ give a quantum circuit that implements the oracle for the function $f(x)$, where $f(x) = 1$ if and only of $x = x_i$. [2]

(ii) Give an explicit quantum circuit for a single Grover iteration. [3]

(iii) Compute θ in this special case. [1]

(iv) Compute the number of necessary Grover iterations to find x_i. [1]

(v) Give now the circuit of Grover's algorithm for this tiny database. [2]

(vi) Explain why this algorithm finds *always* the correct solution. [2]

Exercise 10.2 (Runtime of Grover's algorithm). (5+3 points)

We are going to explore in more detail the runtime of Grover's algorithm. Always keep the geometric picture of the Grover iteration in mind.

(i) Compute again (as we did in the lecture) the number R of necessary iterations by requiring that $\frac{2R+1}{2}\theta$ should be roughly equal to $\pi/2$. [1]

(ii) Now do a similar computation by requiring that $R\theta$ equals roughly the angle between $|\psi\rangle$ and $|\beta\rangle$. [2]

(iii) Perform a series expansion on the second result and compare it to the first one. What do you ovserve? [2]

(iv) Draw conclusions. [+3]

Exercise 10.3 (Success probability of Grover's algorithm). (8 points)

In the lecture we discussed how one computes the number M of solutions to $f(x) = 1$. There we computed M up to some error. We do not consider the counting algorithm now, but we assume that we use Grover's algorithm with incorrect $M' = M + \Delta(M)$.

(i) Draw again the geometric picture of the Grover iteration and try to figure out the success probability geometrically. [3]

(ii) Compute a lower bound on the error probability of Grover's algorithm when we know M exactly. [2]

(iii) Now assume that the used M' is correct up to an error $\Delta(M) \neq 0$, e.g. assume that you know the upper half of the bits of M, that is $\Delta(M) = \mathcal{O}(\sqrt{M})$. Do the same computation as before with this error. [3]

Exercise 10.4 (Filling some gaps). (3 points)

[3] Use the Cauchy-Schwarz inequality to show that for any normalized state vector $|\psi\rangle$ an set of N orthonormal basis vectors $|x\rangle$ we have

$$\sum_{|x\rangle} \| \, |\psi\rangle - |x\rangle \, \|^2 \geq 2N - 2\sqrt{N}.$$