Introduction to quantum information

WS 2012/13 **12.12.2012**
Assignment 5 **Due date 11.1.2013**

Prof. Dr. Wilhelm-Mauch http://qsolid.uni-saarland.de/?Lehre

Problem 1 *Simon's algorithm*

Consider the two-bit version of Simon's algorithm with $s = 2$, specifically $f(0) = f(2) = 0$ and $f(1) = f(3) = 1$.

a) Write out a quantum circuit for the function evaluation, i.e., a circuit that takes $|x\rangle|0\rangle$ into $|x\rangle|f(x)\rangle$. *(2 points)*

b) What is the state of the quantum computer right after the evaluation? Is it entangled? *(1 point)*

Problem 2 *Quantum Fourier transform*

a) In the quantum Fourier transform, we have bounded the error of estimating a phase factor $\nu \in [0, 1]$ that is not a finite-length binary fraction as $p(x) = \frac{1}{4^n}\frac{\sin^2(\pi(2^n\nu - x))}{\sin^2(\pi(\nu - x/2^n))}$ where n is the number of digits of the binary and $\frac{x}{2^n}$ is the estimate of the frequency, hence $|\phi| = |\nu - \frac{x}{2^n}| < 1$. Plot this function for $\nu = \frac{1}{3}$ and $n = 2, 10, 100, 1000$ using a computer. *(2 points)*

b) Much of the simplicity of the phase estimation circuit comes from the fact that a frequency eigenstate encoded by a single binary number is non-entangled. Consider the case of a 2-bit quantum Fourier transform running on a frequency input state of the form $(|01\rangle + |10\rangle)/\sqrt{2}$. Applying the 2-bit quantum Fourier transform, is the output an entangled state? *(3 points)*

Problem 3 *RSA and number theory*

a) Prove that $xy\ \mathrm{mod}N = (x\mathrm{mod}N)(y\mathrm{mod}N)\mathrm{mod}N$. *(1 point)*

b) Using a computer, analyse the periodic function $f(x) = b^x\mathrm{mod}N$ for $N = 1023$ and $b = 99$. Find the period of the function. *(1 point)*

c) Verify $a^{(q-1)(p-1)} = 1\mathrm{mod}(pq)$ for $p = 7$ and $q = 11$ and $a = 15$. *(1 point)*

d) [*] You want to encode text given in 7-bit ASCII code. Find a suitable choice of coding numbers. Explicitly encode the string 'UdS' using this code. *(1 point)*

e) [*] Choose two random 7-digit numbers and apply the Euclidian algorithm to find their greatest common divisor. *(1 point)*

[*] This item is extra credit.