Quantum Information and Quantum Computer

SS 2018 **7 . Exercise** **07.06.2018**

Task 1

a) Use the components of the discrete universal quantum gate (Hadamard, phase, "$\pi/8$" and CNOT gates) to design a circuit for the quantum Fourier transform of a 3-qubit register.

b) What is the explicit form of the transformation matrix for the circuit in a) ?

Task 2

The *order* of an integer number y modulo a (natural) number $N > y$ is defined as the smallest positive integer power r fulfilling

$$y^r \;=\; 1 (\mathrm{mod}\, N) \quad .$$

An important theorem says that for a number N which can be factorised it is *very likely* that the order r is even and $y^{r/2} \neq \pm 1 (\mathrm{mod}\, N)$ is valid, if the largest common factor of y and N is equal to 1 (GGT $(y, N) = 1$). In this case one finds due to

$$\begin{aligned} y^r \;&=\; (y^{r/2})^2 \;=\; 1 (\mathrm{mod}\, N) \\ (y^{r/2})^2 \;-\; 1 \;&=\; 0 (\mathrm{mod}\, N) \end{aligned}$$

the relation $(y^{r/2})^2 - 1 = j\,N$ with $j = 1, 2, 3, \ldots$. On the other hand, the relation $(y^{r/2})^2 - 1 = (y^{r/2}+1)\,(y^{r/2}-1)$ leads to GGT $(y^{r/2}+1, N) \cdot$ GGT $(y^{r/2}-1, N) = N$. In other words, GGT $(y^{r/2}+1, N)$ and GGT $(y^{r/2}-1, N)$ are the factors of N. Check this claim based on the concrete example $y = 10$ and $N = 21$, i. e. determine the order of y modulo N and with its help the factors in 21.

Task 3

Using the Shor algorithm for factorizing the number $N = 21$ with the (arbitrary) choice $y = 11$ and adopting 9 qubits yielded in one run on a quantum computer the result 427. Check whether the correct factors p and q can be obtained from this result.

(Please, turn the page . . .)

Task 4

In order to apply the phase-estimation algorithm it is necessary to prepare the corresponding eigenvectors. In the context of the Shor algorithm these are the eigenvectors of the operator $\hat{\mathrm{U}}_x$ that fulfils

$$\hat{\mathrm{U}}_x \,|\, y \,\rangle \;=\; |\, xy \,(\mathrm{mod}\, N) \,\rangle$$

with $y \in \{0,1\}^m$. Here, the additional convention $xy\,(\mathrm{mod}N) \equiv y$ for $N \leq y \leq r-1$ (where $r = 2^m$) was adopted.

a) Demonstrate that for integer numbers $0 \leq s \leq r-1$

$$|\, u_s \,\rangle \;=\; \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{-2\pi i\, sk/r} \,|\, x^k \bmod N \,\rangle$$

are the eigenvectors of the operator $\hat{\mathrm{U}}_x$, if the order (see previous task) of $x \bmod N$ is equal to r.

b) The efficient preparation of the eigenvectors given in a) appears on the first glance impossible. Instead of a preparation of the single eigenvectors $|\, u_s \,\rangle$ the relation

$$\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |\, u_s \,\rangle \;=\; |\, 1 \,\rangle$$

is used. Proof the validity of this relation.

c) Discuss the consequences of the trick for avoiding the preparation of single eigenvectors described that was described in b) has for the Shor algorithm.