QCLG Exercise sheet 9

Exercise 1. *We consider any unitary operation U on 1 qubit. We say that $\lambda \in \mathbb{C}$ is an eigenvalue of U with corresponding eigenvector $|\psi\rangle$ iff. $U|\psi\rangle = \lambda|\psi\rangle$.*

(a) Show that an eigenvalue λ of a unitary U necessarily satisfies $|\lambda| = 1$.

(b) Let $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Show that $|+\rangle$ and $|-\rangle$ are two eigenvectors of X. What are their associated eigenvalues?

(c) Let $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. This matrix has two distinct eigenvalues. What are the eigenvalues of Z and give some corresponding eigenvectors.

(d) Let $Y = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. This matrix has two distinct eigenvalues. What are the eigenvalues of Y and give some corresponding eigenvectors.

Exercise 2. *Our goal is to construct a quantum circuit that constructs the unitary operation $U|x\rangle|y\rangle = (-1)^{x \cdot y}|x\rangle|y\rangle$ for any $x, y \in \{0, 1\}$, eventually using auxiliary qubits.*

(a) Using only CNOT *and* $\mathrm{SWAP}_{i,j}$ *gates, describe the circuit that computes the unitary $U|x\rangle|y\rangle|0\rangle \rightarrow |x\rangle|y\rangle|x \oplus y\rangle$.*

(b) Write U in matrix form.

(c) From the state $|x\rangle|y\rangle|x \oplus y\rangle$, apply a single qubit operation on each qubit to obtain the state $(-1)^{xy}|x\rangle|y\rangle|x \oplus y\rangle$, and this should hold for each $x, y \in \{0, 1\}$. Each single qubit operation will be of the form $\begin{pmatrix} 1 & 0 \\ 0 & \alpha \end{pmatrix}$ for possibly different α.

(d) Conclude the exercise on how to construct the unitary U.

Exercise 3. *Consider the function $f(a) = 7^a \mod 10$.*

1. *What is the period r of f?*

2. *Show how Shor's algorithm finds the period of f, using a Fourier transform over $q = 128$ elements. Write down all intermediate superpositions of the algorithm for this case (don't just copy the general expressions from the notes,*

but instantiate them with actual numbers as much as possible, incl. with the value of the period found in (a)). You may assume you're lucky, meaning the first run of the algorithm already gives a measurement outcome $b = cq/r$ *with* c *coprime to* r.