2.1) Hadamard test

We express $|q_1\rangle$ in the eigenbasis of U: $|q_1\rangle = \alpha|u_1\rangle + \beta|u_2$, where $U|u_1\rangle = |u_1\rangle$, and $U|u_2\rangle = -|u_2\rangle$. Since the circuit realizes the transformation

$$\begin{aligned}
|q_0\rangle|q_1\rangle &\equiv |0\rangle\,(\alpha|u_1\rangle + \beta|u_2) \\
&\mapsto (1/\sqrt{2})(|0\rangle + |1\rangle)\,(\alpha|u_1\rangle + \beta|u_2) \\
&\mapsto (1/\sqrt{2})|0\rangle\,(\alpha|u_1\rangle + \beta|u_2) + (1/\sqrt{2})|1\rangle\,(\alpha U|u_1\rangle + \beta U|u_2) \\
&= (1/\sqrt{2})|0\rangle\,(\alpha|u_1\rangle + \beta|u_2) + (1/\sqrt{2})|1\rangle\,(\alpha|u_1\rangle - \beta|u_2) \\
&\mapsto (1/2)(|0\rangle + |1\rangle)\,(\alpha|u_1\rangle + \beta|u_2) + (1/2)(|0\rangle - |1\rangle)\,(\alpha|u_1\rangle - \beta|u_2) \\
&= \alpha|0\rangle|u_1\rangle + \beta|1\rangle|u_2\rangle,
\end{aligned}$$

it implements a U-measurement on qubit $|q_1\rangle$: A $|q_0\rangle$ measurement with result 0 projects $|q_1\rangle$ to $|u_1\rangle$ and occurs with probability α^2, while the $|q_0\rangle$ measurement with result 1 corresponds to a projection of $|q_1\rangle$ to $|u_2\rangle$ and occurs with probability β^2. The scheme works also if $|q_1\rangle$ corresponds to a state of n qubits. It implements a projection to the corresponding eigenspaces.

2.2) Fidelity, Purity

(i) With $U \equiv U_{\text{SWAP}}$ and $|q_1\rangle \to |\Psi_1\rangle|\Psi_2\rangle \in \mathcal{H} \bigotimes \mathcal{H}$ our circuit implements

$$\begin{aligned}
|q_0\rangle|q_0\rangle &\equiv |0\rangle|\Psi_1\rangle|\Psi_2\rangle \\
&\mapsto (1/\sqrt{2})(|0\rangle + |1\rangle)|\Psi_1\rangle|\Psi_2\rangle \\
&\mapsto (1/\sqrt{2})(|0\rangle|\Psi_1\rangle|\Psi_2\rangle + |1\rangle|\Psi_2\rangle|\Psi_1\rangle \\
&\mapsto (1/2)(|0\rangle + |1\rangle)|\Psi_1\rangle|\Psi_2\rangle + (1/2)(|0\rangle - |1\rangle)|\Psi_2\rangle|\Psi_1\rangle \\
&= (1/2)|0\rangle(|\Psi_1\rangle|\Psi_2\rangle) + |\Psi_2\rangle|\Psi_1\rangle) + (1/2)|1\rangle(|\Psi_1\rangle|\Psi_2\rangle) - |\Psi_2\rangle|\Psi_1\rangle).
\end{aligned}$$

In order to calculate $\langle Z\rangle_{\text{out}} = P(0) - P(1)$, we need to calculate the probabilities of obtaining the measurement outcome 0 or 1. Since

$$\begin{aligned}
P(0) &= (1/4)\langle 0|((\langle\Psi_1|\langle\Psi_2| + \langle\Psi_2|\langle\Psi_1|)(|\Psi_1\rangle|\Psi_2\rangle) + |\Psi_2\rangle|\Psi_1\rangle))|0\rangle = 1/2 + (|\langle\Psi_1|\Psi_2\rangle|^2)/2, \\
P(1) &= (1/4)\langle 0|((\langle\Psi_1|\langle\Psi_2| - \langle\Psi_2|\langle\Psi_1|)(|\Psi_1\rangle|\Psi_2\rangle) - |\Psi_2\rangle|\Psi_1\rangle))|0\rangle = 1/2 - (|\langle\Psi_1|\Psi_2\rangle|^2)/2,
\end{aligned}$$

we obtain $\langle Z\rangle_{\text{out}} = P(0) - P(1) = |\langle\Psi_1|\Psi_2\rangle|^2$.

(ii) $|\Psi_1\rangle = |\Psi_2\rangle \Rightarrow |\langle\Psi_1|\Psi_2\rangle|^2 = 1$, since the states are normalized. (kliroklaro!) $|\langle\Psi_1|\Psi_2\rangle|^2 = 1 \Rightarrow |\Psi_1\rangle = |\Psi_2\rangle$ (up to a phase), since the Cauchy–Schwarz inequality tells us that $|\langle\Psi_1|\Psi_2\rangle| \leq \|\Psi_1\|\|\Psi_2\| = 1$.

(iii) $|q_1\rangle$ is replaced by two copies of a mixed state: $\rho = \sum_j p_j |j\rangle\langle j|$, where $|j\rangle$ is a ONB, $p_j > 0$, $p_j \in R \; \forall j$ and $\sum_j p_j = 1$. Recall that the expectation value for an observable A is given by

$$\langle A \rangle = Tr[\rho A] = \sum_j p_j \langle j|A|j\rangle.$$

$\langle Z \rangle_{out}$ is therefore given by

$$\langle Z \rangle_{out} = \sum_i \sum_j p_i p_j \langle i|\langle j||\langle i|j\rangle|^2|i\rangle|j\rangle = \sum_i p_i^2 = Tr[\rho^2].$$

Using the criterion

$$Tr[\rho^2] = 1 \Leftrightarrow \rho \text{ is pure}$$

we can show that $\langle Z \rangle_{out} = 1 \;\; \Leftrightarrow \;\; \rho$ is pure. Voila!

2.3) Quantum Phase Estimation

(i) Now $U = \exp(i2\pi\theta Z)$ with eigenvectors $|0\rangle$ and $|1\rangle$. We have $U|0\rangle = e^{i2\pi\theta}|0\rangle$ and $U|1\rangle = e^{-i2\pi\theta}|1\rangle$. θ lies in the set $\{0, 1/4, 1/2, 3/4\}$. In dual-representation $\theta \in \{0.00, 0.01, 0.10, 0.11\}$. Employing our circuit with $U \rightarrow U^2$ we can distinguish between the subsets $\{0, 1/2\}$ and $\{1/4, 3/2\}$, which means we can determine the last dual digit! Here we go:

$$\begin{aligned} |q_o\rangle|q_1\rangle &\equiv |0\rangle|0\rangle \\ &\mapsto (1/\sqrt{2})(|0\rangle + |1\rangle)|0\rangle \\ &\mapsto (1/\sqrt{2})(|0\rangle|0\rangle + |1\rangle)U^2|0\rangle = (1/\sqrt{2})(|0\rangle|0\rangle + e^{i4\pi\theta}|1\rangle)|0\rangle \\ &\mapsto (1/2)(|0\rangle + |1\rangle)|0\rangle + (1/2)e^{i4\pi\theta}(|0\rangle - |1\rangle)|0\rangle \\ &= |0\rangle|0\rangle(1 + e^{i4\pi\theta})/2 + |1\rangle|0\rangle(1 - e^{i4\pi\theta})/2 \end{aligned}$$

If $\theta \in \{0, 1/2\}$ (last digit is 0)$\Rightarrow$ $(1 + e^{i4\pi\theta})/2 = 1$, while $(1 - e^{i4\pi\theta})/2 = 0$. In this case measurement of $|q_0\rangle$ yields 0 with $P(0) = 1$, while $P(1) = 0$.
In case of $\theta \in \{0, 1/2\}$ (last digit is 1) $(1 + e^{i4\pi\theta})/2 = 1$, while $(1 - e^{i4\pi\theta})/2 = 0$ and the $|q_0\rangle$ measurement outcome is 1.

(ii) The scheme can be generalized to measure more than one digit. We consider now the measurement of two digits, i.e. we distinguish between the values 0, 1/4, 1/2 and 3/4. The first two Hadarmard gates, the controlled U^2 operation and the Hadarmard gate on $|q_0\rangle$ amount to

$$|q_o\rangle|q_1\rangle|q_2\rangle \equiv |0\rangle|0\rangle|0\rangle$$

$$\begin{aligned}
&\mapsto (1/2)(|0\rangle|0\rangle + |0\rangle|1\rangle + |1\rangle|0\rangle + |1\rangle|1\rangle)|0\rangle \\
&\mapsto (1/2)(|0\rangle|0\rangle + |0\rangle|1\rangle + e^{i4\pi\theta}|1\rangle|0\rangle + e^{i4\pi\theta}|1\rangle|1\rangle)|0\rangle \\
&\mapsto (1/\sqrt{8})(|0\rangle + |1\rangle)(|0\rangle + |1\rangle)|0\rangle + e^{i4\pi\theta}(|0\rangle - |1\rangle)(|0\rangle + |1\rangle)|0\rangle \\
&= (1/\sqrt{8})|0\rangle \left[(1 + e^{i4\pi\theta})|0\rangle|0\rangle + (1 + e^{i4\pi\theta})|1\rangle|0\rangle\right] \\
&\quad +(1/\sqrt{8})|1\rangle \left[(1 - e^{i4\pi\theta})|0\rangle|0\rangle + (1 - e^{i4\pi\theta})|1\rangle|0\rangle\right]
\end{aligned}$$

By measuring $|q_0\rangle$, we determine the last digit as in (i). We measure $q_0 = 0$ if the last digit is 0 and $q_0 = 1$ if the last digit is 1. In the first case we are left with the state $(1/\sqrt{2})(|0\rangle|0\rangle + |0\rangle|1\rangle)$ and proceed simply as before (no extra-operation has to be applied, the question mark operation in the sketch is only needed in the case $q_0 = 1$, as we will see below.) The remaining controlled U operation and the last Hadamard gate result in

$$\begin{aligned}
(1/\sqrt{2})(|0\rangle|0\rangle + |0\rangle|1\rangle) &\mapsto (1/\sqrt{2})(|0\rangle|0\rangle + e^{i2\pi\theta}|0\rangle|1\rangle) \\
&\mapsto (1/2)(|0\rangle + |1\rangle)|0\rangle + (1/2)e^{i2\pi\theta}(|0\rangle - |1\rangle)|0\rangle \\
&= |0\rangle|0\rangle(1 + e^{i2\pi\theta})/2 + |1\rangle|0\rangle(1 - e^{i2\pi\theta}/2.
\end{aligned}$$

If $\theta = 0$, i.e. the first digit is 0, we obtain $q_1 = 0$, since $(1 + e^{i2\pi\theta})/2 = 1$, while $(1 - e^{i2\pi\theta})/2 = 0$.
If $\theta = 1/2$, i.e. the first digit is 1, we obtain $q_1 = 1$, since $(1 + e^{i2\pi\theta})/2 = 0$, while $(1 - e^{i2\pi\theta})/2 = 1$.
In the other case (the first measurements yields $q_0 = 1$) we cannot proceed in the same way, since we cannot distinguish between $\theta = 1/4$ and $\theta = 3/4$ via the factor $(1 \pm e^{i2\pi\theta})/2$. Therefore we have to apply (conditioned on the measurement outcome q_0) an operation $? = \exp(i2\pi Z0.0p_0)$. With this additional rotation

$$\begin{aligned}
(1/\sqrt{2})(|0\rangle|0\rangle + |0\rangle|1\rangle) &\mapsto (1/\sqrt{2})(|0\rangle|0\rangle + e^{-i\pi/2)}|0\rangle|1\rangle) \\
&\mapsto (1/\sqrt{2})(|0\rangle|0\rangle + e^{i2\pi(\theta-1/4)}|0\rangle|1\rangle) \\
&\mapsto (1/2)(|0\rangle + |1\rangle)|0\rangle + (1/2)e^{i2\pi(\theta-1/4)}(|0\rangle - |1\rangle)|0\rangle \\
&= |0\rangle|0\rangle(1 + e^{i2\pi(\theta-1/4)})/2 + |1\rangle|0\rangle(1 - e^{i2\pi(\theta-1/4)})/2.
\end{aligned}$$

We obtain $q_1 = 0$ if the first digit is 0 ($\theta = 1/4$), and $q_1 = 1$ if the first digit is 1 ($\theta = 3/4$).