Problem 1: Projectors and measurement

a. Consider the four Bell quantum states:

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \quad |\Phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle),$$
$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle), \quad |\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle).$$

Write the four matrices of their outer products $\Pi_{\Phi^\pm} = |\Phi^\pm\rangle\langle\Phi^\pm|$ and $\Pi_{\Psi^\pm} = |\Psi^\pm\rangle\langle\Psi^\pm|$ in the two-qubit computational basis $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$.

Solution:

$$\Pi_{\Phi^+} = |\Phi^+\rangle\langle\Phi^+| = \frac{1}{2}(|00\rangle\langle 00| + |00\rangle\langle 11| + |11\rangle\langle 00| + |11\rangle\langle 11|) = \frac{1}{2}\begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}$$

$$\Pi_{\Phi^-} = |\Phi^-\rangle\langle\Phi^-| = \frac{1}{2}(|00\rangle\langle 00| - |00\rangle\langle 11| - |11\rangle\langle 00| + |11\rangle\langle 11|) = \frac{1}{2}\begin{pmatrix} 1 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ -1 & 0 & 0 & 1 \end{pmatrix}$$

$$\Pi_{\Psi^+} = |\Psi^+\rangle\langle\Psi^+| = \frac{1}{2}(|01\rangle\langle 01| + |01\rangle\langle 10| + |10\rangle\langle 01| + |10\rangle\langle 10|) = \frac{1}{2}\begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

$$\Pi_{\Psi^-} = |\Psi^-\rangle\langle\Psi^-| = \frac{1}{2}(|01\rangle\langle 01| - |01\rangle\langle 10| - |10\rangle\langle 01| + |10\rangle\langle 10|) = \frac{1}{2}\begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & -1 & 0 \\ 0 & -1 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

---

b. First, show that $\Pi_{\Phi^\pm}$ and $\Pi_{\Psi^\pm}$ are projectors by verifying the condition $\Pi_i^2 = \Pi_i$. Then, show that Π_{Φ^+} and Π_{Φ^-} project onto orthogonal subspaces, as $\Pi_{\Phi^+}\Pi_{\Phi^-} = 0$. Finally, show also that $\Pi_{\Psi^+}\Pi_{\Psi^-} = 0$ and give a simple argument for $\Pi_{\Psi^\pm}\Pi_{\Phi^\pm} = 0$.

Solution: We first check the projector condition:

$$\Pi_{\Phi^+}^2 = \frac{1}{4}\begin{pmatrix}1&0&0&1\\0&0&0&0\\0&0&0&0\\1&0&0&1\end{pmatrix}\begin{pmatrix}1&0&0&1\\0&0&0&0\\0&0&0&0\\1&0&0&1\end{pmatrix} = \frac{1}{4}\begin{pmatrix}2&0&0&2\\0&0&0&0\\0&0&0&0\\2&0&0&2\end{pmatrix} = \Pi_{\Phi^+}$$

$$\Pi_{\Phi^-}^2 = \frac{1}{4}\begin{pmatrix}1&0&0&-1\\0&0&0&0\\0&0&0&0\\-1&0&0&1\end{pmatrix}\begin{pmatrix}1&0&0&-1\\0&0&0&0\\0&0&0&0\\-1&0&0&1\end{pmatrix} = \frac{1}{4}\begin{pmatrix}2&0&0&-2\\0&0&0&0\\0&0&0&0\\-2&0&0&2\end{pmatrix} = \Pi_{\Phi^-}$$

$$\Pi_{\Psi^+}^2 = \frac{1}{4}\begin{pmatrix}0&0&0&0\\0&1&1&0\\0&1&1&0\\0&0&0&0\end{pmatrix}\begin{pmatrix}0&0&0&0\\0&1&1&0\\0&1&1&0\\0&0&0&0\end{pmatrix} = \frac{1}{4}\begin{pmatrix}0&0&0&0\\0&2&2&0\\0&2&2&0\\0&0&0&0\end{pmatrix} = \Pi_{\Psi^+}$$

$$\Pi_{\Psi^-}^2 = \frac{1}{4}\begin{pmatrix}0&0&0&0\\0&1&-1&0\\0&-1&1&0\\0&0&0&0\end{pmatrix}\begin{pmatrix}0&0&0&0\\0&1&-1&0\\0&-1&1&0\\0&0&0&0\end{pmatrix} = \frac{1}{4}\begin{pmatrix}0&0&0&0\\0&2&-2&0\\0&-2&2&0\\0&0&0&0\end{pmatrix} = \Pi_{\Psi^-}$$

Next, the orthogonality conditions:

$$\Pi_{\Phi^+}\Pi_{\Phi^-} = \frac{1}{4}\begin{pmatrix}1&0&0&1\\0&0&0&0\\0&0&0&0\\1&0&0&1\end{pmatrix}\begin{pmatrix}1&0&0&-1\\0&0&0&0\\0&0&0&0\\-1&0&0&1\end{pmatrix} = \frac{1}{4}\begin{pmatrix}1-1&0&0&-1+1\\0&0&0&0\\0&0&0&0\\1-1&0&0&-1+1\end{pmatrix} = 0$$

$$\Pi_{\Psi^+}\Pi_{\Psi^-} = \frac{1}{4}\begin{pmatrix}0&0&0&0\\0&1&1&0\\0&1&1&0\\0&0&0&0\end{pmatrix}\begin{pmatrix}0&0&0&0\\0&1&-1&0\\0&-1&1&0\\0&0&0&0\end{pmatrix} = \frac{1}{4}\begin{pmatrix}0&0&0&0\\0&1-1&-1+1&0\\0&1-1&-1+1&0\\0&0&0&0\end{pmatrix} = 0$$

Finally, it is easy to see that $\Pi_{\Phi^+}\Pi_{\Psi^+} = 0$, as the two projectors act on orthogonal subspaces: $\text{span}\{|00\rangle, |11\rangle\}$ for Π_{Φ^+} and $\text{span}\{|01\rangle, |10\rangle\}$ for Π_{Ψ^+}. The same holds for any pair of projectors obtained by choosing one from $\Pi_{\Phi^\pm}$ and a second one from $\Pi_{\Psi^\pm}$.

---

c. Check the completeness relation for the measurement in the Bell basis $\{|\Phi^\pm\rangle, |\Psi^\pm\rangle\}$.

Solution: The completeness relation states that $\sum_i \Pi_i = I$. To check it, consider the sums of the $\Phi^\pm$ and $\Psi^\pm$ projectors:

$$\Pi_{\Phi^+} + \Pi_{\Phi^-} = \frac{1}{2}\begin{pmatrix}1&0&0&1\\0&0&0&0\\0&0&0&0\\1&0&0&1\end{pmatrix} + \frac{1}{2}\begin{pmatrix}1&0&0&-1\\0&0&0&0\\0&0&0&0\\-1&0&0&1\end{pmatrix} = \begin{pmatrix}1&0&0&0\\0&0&0&0\\0&0&0&0\\0&0&0&1\end{pmatrix}$$

$$\Pi_{\Psi^+} + \Pi_{\Psi^-} = \frac{1}{2}\begin{pmatrix}0&0&0&0\\0&1&1&0\\0&1&1&0\\0&0&0&0\end{pmatrix} + \frac{1}{2}\begin{pmatrix}0&0&0&0\\0&1&-1&0\\0&-1&1&0\\0&0&0&0\end{pmatrix} = \begin{pmatrix}0&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&0\end{pmatrix}$$

Therefore $\Pi_{\Phi^+} + \Pi_{\Phi^-} + \Pi_{\Psi^+} + \Pi_{\Psi^-} = I$.

---

d. Compute the probability $\Pr(\Phi^+) = \|\Pi_{\Phi^+} |\psi\rangle\|^2$ for an arbitrary two-qubit state $|\psi\rangle = \psi_{00}|00\rangle + \psi_{01}|01\rangle + \psi_{10}|10\rangle + \psi_{11}|11\rangle$. Then, compute the post-measurement state $|\psi_{\Phi^+}\rangle$ for the same outcome, obtained by dividing the projected vector by its norm:

$$|\psi_{\Phi^+}\rangle = \frac{\Pi_{\Phi^+}|\psi\rangle}{\|\Pi_{\Phi^+}|\psi\rangle\|}.$$

Solution: Writing $|\psi\rangle$ as a column vector in the computational basis and using the matrix of Π_{Φ^+} from part a, we have

$$\Pi_{\Phi^+}|\psi\rangle = \frac{1}{2}\begin{pmatrix}1&0&0&1\\0&0&0&0\\0&0&0&0\\1&0&0&1\end{pmatrix}\begin{pmatrix}\psi_{00}\\\psi_{01}\\\psi_{10}\\\psi_{11}\end{pmatrix} = \frac{1}{2}\begin{pmatrix}\psi_{00}+\psi_{11}\\0\\0\\\psi_{00}+\psi_{11}\end{pmatrix} = \frac{1}{2}(\psi_{00}+\psi_{11})(|00\rangle + |11\rangle).$$

The probability is the squared norm of this vector, i.e. the sum of the squared moduli of its components:

$$\Pr(\Phi^+) = \|\Pi_{\Phi^+}|\psi\rangle\|^2 = \frac{1}{4}|\psi_{00}+\psi_{11}|^2 + \frac{1}{4}|\psi_{00}+\psi_{11}|^2 = \frac{1}{2}|\psi_{00}+\psi_{11}|^2.$$

Alternative solution (Dirac notation). Using $\Pi_{\Phi^+} = |\Phi^+\rangle\langle\Phi^+|$ and $\langle\Phi^+|\psi\rangle = \frac{1}{\sqrt{2}}(\psi_{00}+\psi_{11})$,

$$\Pi_{\Phi^+}|\psi\rangle = |\Phi^+\rangle\langle\Phi^+|\psi\rangle = \frac{\psi_{00}+\psi_{11}}{\sqrt{2}}|\Phi^+\rangle = \frac{1}{2}(\psi_{00}+\psi_{11})(|00\rangle+|11\rangle).$$

Since $|\Phi^+\rangle$ is normalised,

$$\Pr(\Phi^+) = \|\Pi_{\Phi^+}|\psi\rangle\|^2 = \left|\frac{\psi_{00}+\psi_{11}}{\sqrt{2}}\right|^2 \langle\Phi^+|\Phi^+\rangle = \frac{1}{2}|\psi_{00}+\psi_{11}|^2.$$

Equivalently, $\|\Pi_{\Phi^+}|\psi\rangle\|^2 = \langle\psi|\Pi_{\Phi^+}^2|\psi\rangle = \langle\psi|\Pi_{\Phi^+}|\psi\rangle = |\langle\Phi^+|\psi\rangle|^2$.
For the post-measurement state, assuming $\psi_{00}+\psi_{11} \neq 0$ (otherwise the outcome Φ^+ never occurs), we have $\|\Pi_{\Phi^+}|\psi\rangle\| = \frac{|\psi_{00}+\psi_{11}|}{\sqrt{2}}$ and therefore

$$|\psi_{\Phi^+}\rangle = \frac{\Pi_{\Phi^+}|\psi\rangle}{\|\Pi_{\Phi^+}|\psi\rangle\|} = \frac{\psi_{00}+\psi_{11}}{|\psi_{00}+\psi_{11}|}|\Phi^+\rangle = e^{i\varphi}|\Phi^+\rangle,$$

where $e^{i\varphi} = (\psi_{00}+\psi_{11})/|\psi_{00}+\psi_{11}|$ is a phase of modulus one. Since a global phase has no physical consequence, after obtaining the outcome Φ^+ the two qubits are left in the Bell state $|\Phi^+\rangle$, independently of the initial state $|\psi\rangle$.

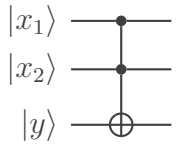
Problem 2: Grover's Algorithm

Consider a search space of dimension $N = 4$, with its elements encoded in binary as 00, 01, 10 and 11. Suppose you are searching for the element $z = 11$.

a. Construct the circuit implementing the quantum oracle $O_f : |x\rangle |y\rangle \to |x\rangle |y \oplus f(x)\rangle$ for the function:

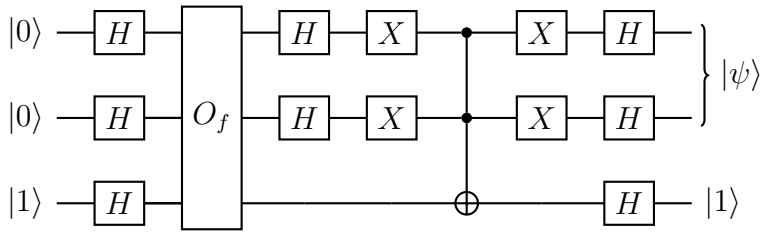
$$f(x) = \begin{cases} 1 & \text{for } x = z, \\ 0 & \text{otherwise.} \end{cases}$$

Solution: In order to construct the circuit that implements the quantum oracle, we need to see how it acts on the computational basis. The register consists of two qubits, and the classical function returns 1 only if $x_1 x_2 = 11$. Looking carefully at the action of the oracle, we see that the target qubit is flipped only if both register qubits are in the state $|1\rangle$. This is exactly the action of the controlled-controlled-NOT (Toffoli) gate. Thus, the quantum circuit implementing the oracle is:



---

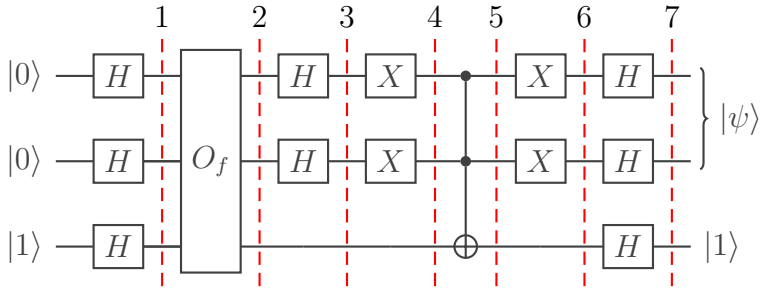
b. We can now construct the quantum circuit which performs the initial Hadamard transformations and a single Grover iteration G:



1. Compute the output state.
2. What happens after we measure the output in the computational basis?
3. How many times do we have to repeat G to obtain z in this example?
4. In the lectures we saw that the scaling of Grover's algorithm is $T \approx \frac{\pi}{4} 2^{n/2}$, which could have led us to think that we would need 2 Grover steps to find the solution. What would be wrong with our reasoning?

Solution:

1. First of all, we divide the quantum circuit into steps and calculate the state of the composite system at each stage:



The three-qubit state at step 1 is:

$$|\psi\rangle_1 = H^{\otimes 3}|001\rangle = |+\rangle|+\rangle|-\rangle = \frac{1}{2}(|00\rangle|-\rangle + |01\rangle|-\rangle + |10\rangle|-\rangle + |11\rangle|-\rangle)$$

We choose to write it in this form in order to use the fact that the action of the oracle on the state $|x\rangle|-\rangle$, where $|x\rangle$ is a computational basis state, is:

$$O_f|x\rangle|-\rangle = (-1)^{f(x)}|x\rangle|-\rangle$$

Using this property, the state after the oracle (step 2) is:

$$\begin{aligned}|\psi\rangle_2 &= \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle - |11\rangle)|-\rangle \\ &= \frac{1}{\sqrt{2}}(|0\rangle|+\rangle + |1\rangle|-\rangle)|-\rangle\end{aligned}$$

At step 3, we act with the Hadamard operator on the register qubits, using $H|0\rangle = |+\rangle$, $H|+\rangle = |0\rangle$, $H|1\rangle = |-\rangle$ and $H|-\rangle = |1\rangle$:

$$|\psi\rangle_3 = (H \otimes H \otimes I)|\psi\rangle_2 = \frac{1}{\sqrt{2}}(|+\rangle|0\rangle + |-\rangle|1\rangle)|-\rangle$$

At step 4, we apply NOT gates on the register qubits, which, using $X|+\rangle = |+\rangle$ and $X|-\rangle = -|-\rangle$, leads to:

$$|\psi\rangle_4 = \frac{1}{\sqrt{2}}(|+\rangle|1\rangle - |-\rangle|0\rangle)|-\rangle = \frac{1}{2}(|01\rangle + |11\rangle - |00\rangle + |10\rangle)|-\rangle$$

Then we act with the controlled-controlled-NOT gate on $|\psi\rangle_4$. Since the target is in the state $|-\rangle$, it adds a phase -1 to the $|11\rangle$ term:

$$|\psi\rangle_5 = \frac{1}{2}(|01\rangle - |11\rangle - |00\rangle + |10\rangle)|-\rangle$$

At step 6, we flip again the first two qubits:

$$|\psi\rangle_6 = \frac{1}{2}(|10\rangle - |00\rangle - |11\rangle + |01\rangle)|-\rangle = -\frac{1}{2}(|0\rangle-|1\rangle)(|0\rangle-|1\rangle)|-\rangle = -|-\rangle|-\rangle|-\rangle$$

Finally, the last layer of Hadamard gates maps each $|-\rangle$ to $|1\rangle$, so

$$|\psi\rangle_7 = -|1\rangle|1\rangle|1\rangle .$$

Since the global phase has no physical consequence, we can neglect it, and the output state is

$$|\psi\rangle \otimes |1\rangle = |11\rangle|1\rangle .$$

2. If we measure the output in the computational basis, we always obtain the outcome 11, i.e. the outcome 11 has probability one.

3. In this example we have to apply G only once.

4. The relation $T \approx \frac{\pi}{4}2^{n/2}$, which gives $T \approx 1.57 \approx 2$ for $n = 2$, relies on two approximations: $T \gg 1$ and $\theta_0 \ll 1$, so that $\sin\theta_0 \approx \theta_0$. Neither is true in our example with such a small number of qubits. Instead, if we revisit the exact relation $(2T+1)\theta_0 = \pi/2$ and use the fact that for $n = 2$ we have $\sin\theta_0 = 1/\sqrt{N} = 1/2$, and therefore $\theta_0 = \pi/6$, we obtain $T = 1$, as observed above.

   Remark that for large n we will rarely achieve exactly the angle $\pi/2$ (which corresponds to reaching the target state) after T Grover iterations, but rather $\pi/2 - \delta$. The probability of failing to find the solution is then $\sin^2\delta \approx \delta^2$, which is small (as $\delta \ll 1$ is expected when $N \gg 1$), and can be made smaller still by repeating the algorithm a few times.

Problem 3: Simon's Algorithm

Suppose we run Simon's algorithm on the following function $f : \{0,1\}^3 \to \{0,1\}^3$:

$$\begin{aligned} f(000) &= f(111) = 000, \\ f(001) &= f(110) = 001, \\ f(010) &= f(101) = 010, \\ f(011) &= f(100) = 011, \end{aligned}$$

where f is two-to-one and satisfies $f(x) = f(x \oplus a)$ for all $x \in \{0,1\}^3$, for some unknown period $a \neq 000$.

a. By inspecting the function given above, find the period a.

Solution: Looking at the table, the inputs are grouped in pairs with the same output: $\{000, 111\}$, $\{001, 110\}$, $\{010, 101\}$ and $\{011, 100\}$. In each pair the two inputs differ in all three bits, i.e. $000 \oplus 111 = 001 \oplus 110 = 010 \oplus 101 = 011 \oplus 100 = 111$. Hence $f(x) = f(x \oplus 111)$ for all x, and the period is $a = 111$.

Of course, finding a this way requires knowing the whole table, i.e. querying f on many inputs. The rest of this problem shows how Simon's algorithm recovers a with only a few quantum queries.

---

b. What is the initial state of the two registers in Simon's algorithm?

Solution: The input of Simon's algorithm is:

1. A function $f : \{0,1\}^3 \to \{0,1\}^3$ *promised* to obey the property: there exists a string $a \in \{0,1\}^3$ such that $[f(x) = f(y)] \iff [x \oplus y \in \{000, a\}]$ for all $x, y \in \{0,1\}^3$.
2. Access to this function only through queries to a quantum oracle O_f.
3. The initial state of the two n-qubit registers, $|0^n\rangle \otimes |0^n\rangle = |0\rangle^{\otimes n} \otimes |0\rangle^{\otimes n}$. In this case, for $n = 3$: $|\psi_{\text{initial}}\rangle = |000\rangle \otimes |000\rangle = |000000\rangle$.

---

c. What will the state be after:

1. the first layer of Hadamard gates applied to the upper three qubits;
2. the oracle query $O_f |x\rangle |y\rangle = |x\rangle |y \oplus f(x)\rangle$?

Solution:

1. After the first Hadamard transform on the first three qubits we have:

$$|\psi'\rangle = \left(H^{\otimes 3} |000\rangle\right) \otimes |000\rangle = \frac{1}{\sqrt{2^3}} \sum_{x \in \{0,1\}^3} |x\rangle \otimes |000\rangle$$

2. After the oracle query we have:

$$\begin{aligned}
|\psi''\rangle &= \frac{1}{\sqrt{2^3}} \sum_{x \in \{0,1\}^3} |x\rangle |f(x)\rangle \\
&= \frac{1}{\sqrt{2^3}} \big(|000\rangle |f(000)\rangle + |001\rangle |f(001)\rangle + |010\rangle |f(010)\rangle + |011\rangle |f(011)\rangle \\
&\qquad + |100\rangle |f(100)\rangle + |101\rangle |f(101)\rangle + |110\rangle |f(110)\rangle + |111\rangle |f(111)\rangle \big) \\
&= \frac{1}{\sqrt{2^3}} \big((|000\rangle + |111\rangle) |000\rangle + (|001\rangle + |110\rangle) |001\rangle \\
&\qquad + (|010\rangle + |101\rangle) |010\rangle + (|011\rangle + |100\rangle) |011\rangle \big) \\
&= \frac{1}{2} \Big(\tfrac{1}{\sqrt{2}} (|000\rangle + |111\rangle) |000\rangle + \tfrac{1}{\sqrt{2}} (|001\rangle + |110\rangle) |001\rangle \\
&\qquad + \tfrac{1}{\sqrt{2}} (|010\rangle + |101\rangle) |010\rangle + \tfrac{1}{\sqrt{2}} (|011\rangle + |100\rangle) |011\rangle \Big).
\end{aligned}$$

d. What would the state be after measuring the second register, supposing that the measurement gave the outcome 001?

Solution: To answer this question, we apply the projector $I \otimes \Pi_{001}$, with $\Pi_{001} = |001\rangle\langle 001|$, to $|\psi''\rangle$. Because $\langle y|f(x)\rangle \neq 0$ if and only if $f(x) = y$, we obtain

$$(I \otimes \Pi_{001})\,|\psi''\rangle = (I \otimes |001\rangle\langle 001|)\,|\psi''\rangle = \frac{1}{2} \cdot \frac{1}{\sqrt{2}}(|001\rangle + |110\rangle)\,|001\rangle\,.$$

The outcome 001 therefore occurs with probability $\|(I \otimes \Pi_{001})\,|\psi''\rangle\,\|^2 = 1/4$. After renormalisation (the factor $\frac{1}{2}$ disappears), the upper register is left in the state

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|001\rangle + |110\rangle) = \frac{1}{\sqrt{2}}(|001\rangle + |001 \oplus a\rangle),$$

with $a = 111$.

e. Imagine we now apply the final step, three Hadamard transforms. Using the formula

$$H^{\otimes n}\,|x\rangle = \frac{1}{\sqrt{2^n}} \sum_{y\in\{0,1\}^n} (-1)^{x\cdot y}\,|y\rangle\,,$$

write the state after applying this step.

Solution: Applying $H^{\otimes 3}$ to the state $\frac{1}{\sqrt{2}}(|001\rangle + |110\rangle)$ gives

$$|\tilde{\psi}\rangle = \frac{1}{\sqrt{2^3}}\frac{1}{\sqrt{2}}\left(\sum_{z\in\{0,1\}^3} (-1)^{z_3}\,|z_1z_2z_3\rangle + \sum_{z\in\{0,1\}^3} (-1)^{z_1+z_2}\,|z_1z_2z_3\rangle\right),$$

which, after factoring out $(-1)^{z_3}$ and using $(-1)^{-z_3} = (-1)^{z_3}$, reads:

$$|\tilde{\psi}\rangle = \frac{1}{4}\sum_{z\in\{0,1\}^3} (-1)^{z_3}\left(1 + (-1)^{z_1+z_2+z_3}\right)|z_1z_2z_3\rangle\,.$$

We see an interference effect: the factor $1 + (-1)^{z_1+z_2+z_3}$ equals 2 for the outcomes satisfying $z_1 \oplus z_2 \oplus z_3 = a \cdot z = 0$, and 0 for those satisfying $a \cdot z = 1$, which therefore cancel. Hence

$$|\tilde{\psi}\rangle = \frac{1}{2}\sum_{z\in\{0,1\}^3:\ a\cdot z=0} (-1)^{z_3}\,|z_1z_2z_3\rangle\,,$$

where the sum runs over the 4 strings $z \in \{000, 011, 101, 110\}$ satisfying $a \cdot z = 0$. The state is correctly normalised, as these 4 outcomes are equiprobable, each with probability $1/4$, while the outcomes with $a \cdot z = 1$ never occur.

f. Suppose the first run of the algorithm gives $y = 011$ and the second run gives $y = 101$. Show that, assuming $a \neq 000$, these two runs of the algorithm already determine that $a = 111$.

Solution: As discussed in the lectures, every outcome y must satisfy $a \cdot y = 0$, so the period must satisfy $a \cdot 011 = 0$ and $a \cdot 101 = 0$. The first equation is fulfilled for $a \in \{000, 100, 011, 111\}$ and the second for $a \in \{000, 010, 101, 111\}$. This means that both equations are fulfilled only for $a \in \{000, 111\}$, and since it is assumed that $a \neq 000$, it follows that $a = 111$.

Alternatively, $a \cdot 011 = 0$ implies $a_2 \oplus a_3 = 0$ and $a \cdot 101 = 0$ implies $a_1 \oplus a_3 = 0$. This is equivalent to $a_2 = a_3$ and $a_1 = a_3$, which implies $a_1 = a_2 = a_3$, leading to $a = 111$ as the only non-zero solution.
