Problem 1: Pauli-string rotations and quantum simulation

Time evolution under a Hamiltonian $\hat{H}$ expressed as a sum of Pauli strings, $\hat{H} = \sum_i \gamma_i P_i$, can be approximated using products of Pauli-string rotations $e^{-i\theta_i P_i}$ with $\theta_i = \gamma_i t$.

Part I: Pauli-string rotation gadget

A Pauli string P is the tensor product of n Pauli matrices $\sigma \in \{I, X, Y, Z\}$, i.e. $P = \sigma_1 \otimes \cdots \otimes \sigma_n$. Since $P^2 = I_{2^n}$, using the Taylor expansion of the exponential one can prove

$$e^{i\theta P} = \cos\theta\, I_{2^n} + i \sin\theta\, P,$$

where $I_{2^n} = I^{\otimes n}$ is the identity matrix of n qubits. A non-identity Pauli string has projectors Π_0 and Π_1 onto its eigenspaces, with $P\Pi_x = (-1)^x \Pi_x$, $P = \Pi_0 - \Pi_1$ and $\Pi_0 + \Pi_1 = I_{2^n}$.

a.

1. Using Euler's formula $e^{i\theta} = \cos\theta + i\sin\theta$ and the relations above, prove that
$$e^{-i\theta P} = e^{-i\theta}\,\Pi_0 + e^{+i\theta}\,\Pi_1.$$

2. Show that
$$H e^{-i\theta X} H = e^{-i\theta Z} = e^{-i\theta}\,|0\rangle\langle 0| + e^{+i\theta}\,|1\rangle\langle 1|\,.$$

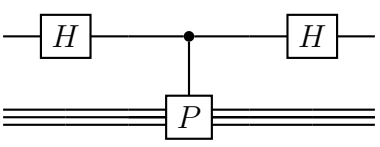
Solution:

1. Replacing $\theta \to -\theta$ in the Taylor-series result gives $e^{-i\theta P} = \cos\theta\, I_{2^n} - i\sin\theta\, P$. Substituting $I_{2^n} = \Pi_0 + \Pi_1$ and $P = \Pi_0 - \Pi_1$, and using Euler's formula,
$$e^{-i\theta P} = (\cos\theta - i\sin\theta)\,\Pi_0 + (\cos\theta + i\sin\theta)\,\Pi_1 = e^{-i\theta}\,\Pi_0 + e^{+i\theta}\,\Pi_1.$$
Analogously, $e^{+i\theta P} = e^{+i\theta}\Pi_0 + e^{-i\theta}\Pi_1$.

2. Using $e^{-i\theta X} = \cos\theta\, I - i\sin\theta\, X$, $H^2 = I$ and $HXH = Z$ (multiply $HZH = X$ by H on both sides),
$$H e^{-i\theta X} H = \cos\theta\, I - i\sin\theta\, HXH = \cos\theta\, I - i\sin\theta\, Z = e^{-i\theta Z}.$$
The projectors of Z are $\Pi_0 = |0\rangle\langle 0|$ and $\Pi_1 = |1\rangle\langle 1|$, so part 1 with $P = Z$ gives $e^{-i\theta Z} = e^{-i\theta}\,|0\rangle\langle 0| + e^{+i\theta}\,|1\rangle\langle 1|$.

---

b. Show that the circuit below implements the operator $I \otimes \Pi_0 + X \otimes \Pi_1$.



Solution: The ancilla is the first tensor factor and the register the second. Using $(A \otimes B)(C \otimes D) = AC \otimes BD$, $H|0\rangle = |+\rangle$, $H|1\rangle = |-\rangle$ and $H = H^\dagger$,

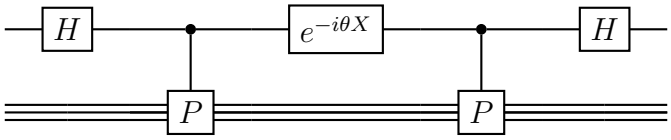
$$S \equiv (H \otimes I_{2^n})\left(|0\rangle\langle 0| \otimes I_{2^n} + |1\rangle\langle 1| \otimes P\right)(H \otimes I_{2^n}) = |+\rangle\langle +| \otimes I_{2^n} + |-\rangle\langle -| \otimes P.$$

Since $|\pm\rangle\langle\pm| = \frac{1}{2}\begin{pmatrix} 1 & \pm 1 \\ \pm 1 & 1 \end{pmatrix} = \frac{1}{2}(I \pm X)$, and using $I_{2^n} = \Pi_0 + \Pi_1$, $P = \Pi_0 - \Pi_1$,

$$S = \tfrac{1}{2}(I + X) \otimes (\Pi_0 + \Pi_1) + \tfrac{1}{2}(I - X) \otimes (\Pi_0 - \Pi_1) = I \otimes \Pi_0 + X \otimes \Pi_1.$$

---

c. Consider now the following circuit, which uses the single-qubit X-rotation $R_x(2\theta) = e^{-i\theta X}$:



1. Using parts a and b, show that this circuit implements the *Pauli-string rotation* operator
$$|0\rangle\langle 0| \otimes e^{-i\theta P} + |1\rangle\langle 1| \otimes e^{+i\theta P}.$$

2. What is the output of the circuit if we input $|0\rangle \otimes |\psi\rangle$? What is the role of the upper ancillary qubit when its input is $|0\rangle$?

Solution:

1. Inserting $H^2 = I$ on the ancilla before and after the rotation, the circuit becomes two Hadamard test circuits around a Z-rotation of the ancilla, $S\left(He^{-i\theta X}H \otimes I_{2^n}\right)S = S\left(e^{-i\theta Z} \otimes I_{2^n}\right)S$. Using parts a.2 and b,

$$(I \otimes \Pi_0 + X \otimes \Pi_1)\left(e^{-i\theta}|0\rangle\langle 0| + e^{i\theta}|1\rangle\langle 1|\right) \otimes I_{2^n}(I \otimes \Pi_0 + X \otimes \Pi_1).$$

The cross terms vanish because $\Pi_0\Pi_1 = \Pi_1\Pi_0 = 0$, while $\Pi_x^2 = \Pi_x$, $X|0\rangle\langle 0|X = |1\rangle\langle 1|$ and $X|1\rangle\langle 1|X = |0\rangle\langle 0|$. Hence the circuit equals

$$\begin{aligned}
&\left(e^{-i\theta}|0\rangle\langle 0| + e^{i\theta}|1\rangle\langle 1|\right) \otimes \Pi_0 + \left(e^{-i\theta}|1\rangle\langle 1| + e^{i\theta}|0\rangle\langle 0|\right) \otimes \Pi_1 \\
&= |0\rangle\langle 0| \otimes \left(e^{-i\theta}\Pi_0 + e^{i\theta}\Pi_1\right) + |1\rangle\langle 1| \otimes \left(e^{i\theta}\Pi_0 + e^{-i\theta}\Pi_1\right) \\
&= |0\rangle\langle 0| \otimes e^{-i\theta P} + |1\rangle\langle 1| \otimes e^{i\theta P},
\end{aligned}$$

where in the last step we used part a.1.

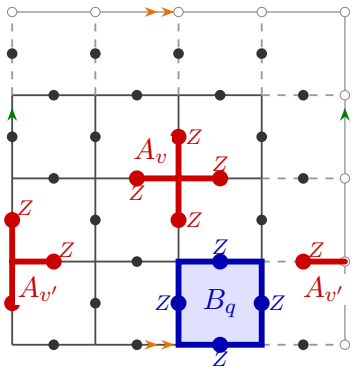
2. For the input $|0\rangle \otimes |\psi\rangle$ only the first term contributes, and the output is

$$|0\rangle \otimes e^{-i\theta P} |\psi\rangle .$$

The ancilla facilitates the implementation of $e^{-i\theta P}$ on the register, while remaining disentangled from it at the end: it returns to $|0\rangle$, so it can be reused for further Pauli-string rotations.

Part II: Quantum simulation of an Ising-type lattice model

Consider an $L \times L$ square lattice with periodic boundary conditions (a torus), where L is even, and with $2L^2$ qubits located on its edges. The Figure below shows the example $L = 4$. We define the Hamiltonian $\hat{H} = \sum_v A_v + \sum_q B_q$, composed of *star operators* $A_v = \prod_{i \in v} Z_i$, acting on the four qubits on the edges meeting at vertex v, and *plaquette operators* $B_q = \prod_{i \in q} Z_i$, acting on the four qubits on the edges of the square plaquette q. The periodic boundary conditions mean that the top side of the lattice is identified with the bottom side (orange double arrows in the Figure) and the right side with the left side (green single arrows). Hence the dashed edges wrap around the torus, and the white circles on the top and right lines are copies of the vertices on the bottom and left lines.



Example: $L = 4$
• qubit ($2L^2 = 32$)
$A_v = \prod_{i \in v} Z_i$, $B_q = \prod_{i \in q} Z_i$
$\hat{H} = \sum_v A_v + \sum_q B_q$
▶: right side ≡ left side
▶▶: top side ≡ bottom side
∘ copy of a vertex on the opposite side

Since all the terms A_v and B_q are products of Z operators, they commute with each other, and therefore

$$e^{-i\theta\hat{H}} = \prod_v e^{-i\theta A_v} \prod_q e^{-i\theta B_q},$$

which allows the implementation of each term independently of each other.

a. We want to implement $e^{-i\theta\hat{H}}$ using the Pauli-string rotation gadget of Part I, where P is replaced by the terms A_v and B_q. How many Pauli-string rotation gadgets do we need to fully implement $e^{-i\theta\hat{H}}$ if we implement one term at a time? What is the minimum number of ancillary qubits required?

Solution: An $L \times L$ lattice with periodic boundary conditions has L^2 vertices and L^2 plaquettes, hence L^2 star operators A_v and L^2 plaquette operators B_q. Implementing one term at a time requires $L^2 + L^2 = 2L^2$ Pauli-string rotation gadgets (32 for $L = 4$). Since

each gadget returns the ancilla to $|0\rangle$, unentangled (Part I, c.2), the same ancilla can be reused for every gadget: the minimum number of ancillary qubits is 1.

---

b. All terms $e^{-i\theta B_q}$ that do not have overlapping qubits can be implemented in parallel, and the same holds for the set of terms $e^{-i\theta A_v}$. If we decide to first implement all terms $e^{-i\theta B_q}$, followed by all terms $e^{-i\theta A_v}$, what is the minimum depth, counted in Pauli-string rotation gadgets? How many ancillary qubits are now required?

Solution: Two plaquette operators overlap if and only if they share an edge, i.e. they are neighbouring plaquettes; plaquettes touching only at a corner share no qubit. Similarly, two star operators overlap if and only if their vertices are nearest neighbours (they share the connecting edge). Label the plaquettes, and separately the vertices, by (i, j) and colour them as a checkerboard according to the parity of $i + j$. Since L is even, this colouring is consistent across the periodic boundaries, so two colours suffice for each type and terms of the same colour never overlap:

- layers 1 and 2: the $L^2/2$ "even" plaquettes, then the $L^2/2$ "odd" plaquettes;
- layers 3 and 4: the $L^2/2$ "even" stars, then the $L^2/2$ "odd" stars.

The minimum depth is therefore 4 Pauli-string rotation gadgets (one layer cannot hold two neighbouring terms, so each type needs at least two layers). Each layer runs $L^2/2$ gadgets simultaneously, each needing its own ancilla, so $L^2/2$ ancillary qubits are required, reused from layer to layer (8 for $L = 4$). For odd L the checkerboard colouring would fail across the boundary and a third layer per type would be needed.

Problem 2: Quantum Fourier Transform

As you have seen in the lectures, we can represent any integer z in its binary form as:

$$z = z_1 z_2 \dots z_n$$

where $z_1, z_2, \dots, z_n$ are such so that:

$$z = z_1 2^{n-1} + \dots + z_{n-1} 2^1 + z_n$$

a. How many qubits at least would we need to encode the integer states $|14\rangle$ and $|9\rangle$? What is their binary representation when using qubits to encode the integers?

Solution: In order to represent an integer state $|N\rangle$, one would require at least $n = \lceil \log(N+1) \rceil$ qubits. This implies that for both cases we require 4 qubits. The binary representation of these four-qubit integer states is:

$$|14\rangle = |1110\rangle$$
$$|9\rangle = |1001\rangle$$

---

b. Recall that:

$$0.z_l z_{l+1} \dots z_m \equiv \frac{z_l}{2} + \frac{z_{l+1}}{2^2} + \dots + \frac{z_m}{2^{m-l+1}}$$

Calculate:

1. $2^3 \cdot 0.z_1 z_2 z_3$, $2^2 \cdot 0.z_1 z_2 z_3$ and $2 \cdot 0.z_1 z_2 z_3$, where $z_i \in \{0, 1\}$.
2. $e^{2\pi i \cdot 2^2 \cdot 0.j_1 j_2 j_3}$ where $j_i \in \{0, 1\}$.

Solution: We start by writing down the expression for $0.z_1 z_2 z_3$:

$$0.z_1 z_2 z_3 = \frac{z_1}{2} + \frac{z_2}{4} + \frac{z_3}{8}$$

Then it is easy to calculate the expressions above. For the first case, we have:

$$2^3 \cdot 0.z_1 z_2 z_3 = 4z_1 + 2z_2 + z_3$$
$$2^2 \cdot 0.z_1 z_2 z_3 = 2z_1 + z_2 + \frac{z_3}{2}$$
$$2 \cdot 0.z_1 z_2 z_3 = z_1 + \frac{z_2}{2} + \frac{z_3}{4}$$

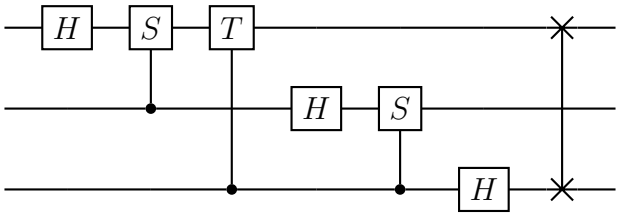
For the second case:

$$e^{2\pi i \cdot 2^2 \cdot 0.j_1 j_2 j_3} = e^{2\pi i (2j_1 + j_2 + j_3/2)} = e^{2\pi i (2j_1 + j_2)} e^{2\pi i j_3/2} = e^{2\pi i 0.j_3},$$

where in the second equality we used the fact that $2j_1 + j_2$ is an integer and therefore $e^{2\pi i (2j_1 + j_2)} = 1$.

---

c. Now consider the quantum Fourier circuit for three qubits:

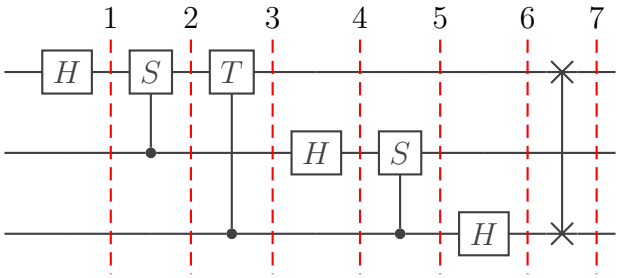


with S and T being the gates:

$$S = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/2} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}, T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$$

Suppose that we input the state $|j\rangle = |j_1 j_2 j_3\rangle$. What will be the output state?

Solution: We start as usual by dividing the quantum circuit into subsequent steps:



Initially, the system is in the state:

$$|\psi\rangle_0 = |j_1 j_2 j_3\rangle$$

Then we act with the Hadamard operator on the first qubit and use the fact that $e^{2\pi i 0.j_1}$ is $+1$ if $j_1 = 0$ and -1 if $j_1 = 1$. Thus the state at step 1 is transformed to:

$$|\psi\rangle_1 = \frac{1}{2^{1/2}}(|0\rangle + e^{2\pi i 0.j_1}|1\rangle)|j_2 j_3\rangle$$

Recall that the unitary operator R_k is defined as:

$$R_k = \begin{pmatrix} 1 & 0 \\ 0 & e^{2\pi i/2^k} \end{pmatrix}$$

It's easy to see that both S and T are special cases of the operator R_k for two different choices of k. S corresponds to R_2 while T corresponds to R_3.

On the next step, applying the S operator on the first qubit controlled by the second qubits produces the state:

$$|\psi\rangle_2 = \frac{1}{2^{1/2}}(|0\rangle + e^{2\pi i 0.j_1} e^{2\pi i 0.0 j_2}|1\rangle)|j_2 j_3\rangle = \frac{1}{2^{1/2}}(|0\rangle + e^{2\pi i 0.j_1 j_2}|1\rangle)|j_2 j_3\rangle$$

Next, we perform the controlled-T operation and so we get:

$$|\psi\rangle_3 = \frac{1}{2^{1/2}}(|0\rangle + e^{2\pi i 0.j_1 j_2} e^{2\pi i 0.00 j_3}|1\rangle)|j_2 j_3\rangle = \frac{1}{2^{1/2}}(|0\rangle + e^{2\pi i 0.j_1 j_2 j_3}|1\rangle)|j_2 j_3\rangle$$

If we work with the exact same way for the rest of the steps we will get:

Step 4:

$$|\psi\rangle_4 = \frac{1}{2}(|0\rangle + e^{2\pi i 0.j_1 j_2 j_3}|1\rangle)(|0\rangle + e^{2\pi i 0.j_2})|j_3\rangle$$

Step 5:

$$|\psi\rangle_4 = \frac{1}{2}(|0\rangle + e^{2\pi i 0.j_1 j_2 j_3}|1\rangle)(|0\rangle + e^{2\pi i 0.j_2 j_3})|j_3\rangle$$

Step 6:

$$|\psi\rangle_4 = \frac{1}{2^{3/2}}(|0\rangle + e^{2\pi i 0.j_1 j_2 j_3}|1\rangle)(|0\rangle + e^{2\pi i 0.j_2 j_3})(|0\rangle + e^{2\pi i 0.j_3}|1\rangle)$$

At the final step, we swap the state of the first and third qubit and recover the *quantum Fourier transformation*:

$$|\psi\rangle_4 = \frac{1}{2^{3/2}}(|0\rangle + e^{2\pi i 0.j_3}|1\rangle)(|0\rangle + e^{2\pi i 0.j_2 j_3})(|0\rangle + e^{2\pi i 0.j_1 j_2 j_3}|1\rangle)$$

Problem 3: Order-Finding

For two positive integers x and N with $x < N$ the *order* of x modulo N is defined to be the *least positive integer* r such that $x^r = 1 \bmod N$.

a. Show that for $x = 2$ and $N = 5$ we have $r = 4$.

Solution: It's easy to see that for $r = 4$:

$$2^4 = 3 \times 5 + 1,$$

which implies $2^4 = 1 \mod 5$. Similarly, one can show that $2^3 = 3 \mod 5$ and $2^2 = 4 \mod 5$. Therefore, $r = 4$ is the least integer such that $2^4 = 1 \mod 5$.

Note: Remark that modular exponentiation is a periodic function of period r. You can check that for $x = 3$ we also obtain $r = 4$, but for $x = 4$ we have $r = 2$, the latest can be easily derived from the case of $x = 2$.

---

b. Now consider the transformation U_x which acts on the computational basis states as $U_x |y\rangle \equiv |xy \bmod N\rangle$. Prove that:

1. $U_x U_{x'} = U_{xx'}$
2. $U_{x^{-1}} = U_x^{-1} = U_x^\dagger$, using the fat that x has an inverse $x^{-1} \pmod N$ if and only if x and N are co-prime.
3. $U_x U_x^\dagger = U_x^\dagger U_x = I$, which proves it is an unitary transformation.
4. $U_x^r = I$ where r is the period of x modulo N.

Solution: We start with the first property, which result from the associativity of the multiplication of integer $\mod N$. We have:

$$U_x U_{x'} |y\rangle = U_x |x'y \mod N\rangle = |xx'y \mod N\rangle$$
$$U_{xx'} |y\rangle = |xx'y \mod N\rangle$$

and thus:

$$U_x U_{x'} = U_{xx'} = U_{x'} U_x$$

We continue with the second property:

$$U_{x^{-1}} U_x |y\rangle = U_{x^{-1}} |xy \mod N\rangle = |y\rangle$$

and thus:

$$U_{x^{-1}} = U_x^{-1}$$

Now for the second part of the second property:

$$\langle y| U_x^\dagger U_x |y\rangle = \langle yx \mod N | yx \mod N\rangle = 1$$

and thus $U_x^\dagger U_x = I$ and so the inverse of U_x is $U_x^\dagger$, i.e.:

$$U_{x^{-1}} = U_x^{-1} = U_x^\dagger$$

The third property follows immediately from the previous property as $U_x U_x^\dagger = U_x U_x^{-1} = I = U_x^\dagger U_x$ and thus U_x is a unitary operator.

Then for the final property we have:

$$\underbrace{U_x U_x \dots U_x}_{r} |y\rangle = |x^r y \mod N\rangle = |y\rangle$$

and so we proved that:

$$U_x^r = I$$

---

c. Show that the states $|u_s\rangle \equiv \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{-2\pi i s k/r} |x^k \bmod N\rangle$, for integer $0 \leq s \leq r-1$, are eigenstates of U_x. What is their corresponding eigenvalues?

Solution: If we act with U_x on the states $|u_s\rangle$ we get:

$$U_x |u_s\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{-\frac{2\pi i s k}{r}} U_x |x^k \mod N\rangle$$

$$= \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{-\frac{2\pi i s k}{r}} |x^{k+1} \mod N\rangle = \frac{1}{\sqrt{r}} \sum_{k'=1}^{r} e^{-\frac{2\pi i s (k'-1)}{r}} |x^{k'} \mod N\rangle$$

where in the last step we switched the variable k with the variable $k' = k+1$. If we continue with the calculation we have:

$$U_x |u_s\rangle = e^{2\pi i s/r} \frac{1}{\sqrt{r}} \sum_{k'=1}^{r} e^{-\frac{2\pi i s k'}{r}} |x^{k'} \mod N\rangle$$

But recall that r is the order of x modulo N and so $x^r = 1 \mod N$. It's easy to see then that the sum in the expression can be replaced to:

$$\sum_{k'=1}^{r} \to \sum_{k=0}^{r-1},$$

as it correspond only to a reordering of the same sum (a shift to the left of a closed cycle). Thus, we can conclude that $|u_s\rangle$ is an eigenstate of the operator U_x with eigenvalue $e^{2\pi i s/r}$:

$$U_x |u_s\rangle = e^{2\pi i s/r} |u_s\rangle$$

---

d. As you can see preparing the state $|u_s\rangle$ requires that we know r in advance. Fortunately there is clever observation which circumvents the problems of preparing $|u_s\rangle$. Show that:

1. $\sum_{s=0}^{r-1} e^{-2\pi isk/r} = r\delta_{k,0}$,
2. $\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} e^{2\pi isk/r} |u_s\rangle = |x^k \bmod N\rangle$,

which has as special case when $k = 0$: $\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |u_s\rangle = |1\rangle$, which is a trivial state to generate. This opens the door to applying quantum phase-estimation to sample from $\varphi = s/r$, which later leads to a guess of r as explained in the lecture on Shor's algorithm.

Solution: Consider the first expression and let $k = 0$. It's easy to see that we have a sum of r terms, all equal to the identity and thus:

$$\sum_{s=0}^{r-1} e^{-2\pi isk/r} = r \text{ if } k = 0$$

Now consider $k \neq 0$. The sum then corresponds to a geometric series which is equal to:

$$\sum_{s=0}^{r-1} e^{-2\pi isk/r} = \frac{1 - e^{-2\pi ik}}{1 - e^{-2\pi ik/r}} = 0$$

for every $k \in \mathbb{Z}$ with $k \neq 0$. Thus we can conclude that:

$$\sum_{s=0}^{r-1} e^{-2\pi isk/r} = r\delta_{k,0}$$

For the second expression we have:

$$\begin{aligned}\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} e^{2\pi isk/r} |u_s\rangle &= \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} \left[e^{2\pi isk/r} \frac{1}{\sqrt{r}} \sum_{k'=0}^{r-1} e^{-\frac{2\pi isk'}{r}} |x^{k'} \mod N\rangle \right] \\ = \frac{1}{r} \sum_{s=0}^{r-1} \sum_{k'=0}^{r-1} e^{2\pi is(k-k')/r} |x^k \mod N\rangle &= \frac{1}{r} \sum_{k'=0}^{r-1} r\delta_{0,k-k'} |x^{k'} \mod N\rangle\end{aligned}$$

where in the last equality we used the result from expression 1. It's trivial to see that $\delta_{0,k-k'} = \delta_{k,k'}$ and the sum over k' contributes only when $k' = k$. Thus:

$$\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} e^{2\pi isk/r} |u_s\rangle = |x^k \mod N\rangle .$$

The case $k = 1$ is only a corollary of this last result, leading to the input state $|1\rangle$ used in the order finding algorithm.

---

e. If we wanted to apply a phase estimation procedure we must have efficient procedures to implement a controlled-U^{2^j} operation for any integer j. Given an integer number x, propose a technique to compute x^{2^k} that scales linearly in k.

Solution: if we want to compute x^{2^k} an inefficient approach is to multiply 2^k times x. A more efficient approach is to square iteratively, i.e., we apply the function $y^2 \mod N$ k times to the input x. It is easy to see then that we get the series x^2, x^4, x^{2^3},..., x^{2^k}. Because the multiplication is $\mod N$, the memory register does not need to increase, as it will never be larger than N.

---

f. Assuming that we are given an unitary S such that implements $S|x\rangle = |x^2 \bmod N\rangle$ that needs $O(L^2)$ gates, where $L = \lceil \log N \rceil$, i.e., the size of the register. How many gates we will be needed to implement $|x\rangle \to |x^{2^k} \bmod N\rangle$?

Solution: We are given that the unitary S is such that implements $S|x\rangle = |x^2 \mod N\rangle$ using $O(L^2)$ gates. Clearly if we want to implement $|x\rangle \to |x^{2^k} \mod N\rangle$ we need to apply S k times, which lead to an asymptotic scaling $O(kL^2)$ of number of gates. Because in phase estimation we need to implement up to U^{2^k} where $k \in \{0, 2L+1\}$, it is easy to see that need $O(L^3)$ gates.

Extra problem: SWAP Test

Given the two-qubit SWAP gate:

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

and the two single-qubit states $|\phi_1\rangle = a|0\rangle + b|1\rangle$ and $|\phi_2\rangle = c|0\rangle + d|1\rangle$.

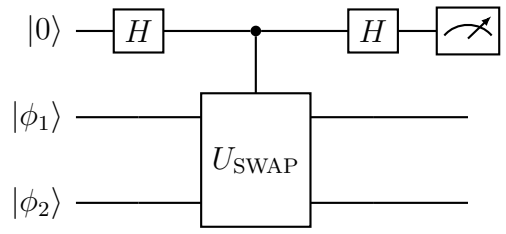
a. Show that $U_{\text{SWAP}}|\phi_1\rangle \otimes |\phi_2\rangle = |\phi_2\rangle \otimes |\phi_1\rangle$

Solution: We have $|\phi_1\rangle \otimes |\phi_2\rangle = ac|00\rangle + ad|01\rangle + bc|10\rangle + bd|11\rangle$. The action of the SWAP gate is to exchange $|10\rangle$ and $|01\rangle$, leading to

$$\begin{aligned} U_{\text{SWAP}}|\phi_1\rangle \otimes |\phi_1\rangle &= ac|00\rangle + bc|01\rangle + ad|10\rangle + bd|11\rangle && (1)\\ &= c|0\rangle \otimes (a|0\rangle + b|1\rangle) + d|1\rangle \otimes (a|0\rangle + b|1\rangle) && (2)\\ &= (c|0\rangle + d|0\rangle) \otimes (a|0\rangle + b|1\rangle) && (3)\\ &= |\phi_2\rangle \otimes |\phi_1\rangle && (4) \end{aligned}$$

---

b. Consider the following SWAP test circuit acting on the two states $|\phi_1\rangle$ and $|\phi_2\rangle$.



Give the quantum state of the three qubit system at each step of the circuit.

Solution: The input to the circuit reads $|\psi_0\rangle = |0\rangle \otimes |\phi_1\rangle \otimes |\phi_2\rangle$. After the first Hadamard gate, the state reads

$$\begin{aligned} |\psi_1\rangle &= H \otimes I \otimes I|0\rangle \otimes |\phi_1\rangle \otimes |\phi_2\rangle && (5)\\ &= \frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes |\phi_1\rangle \otimes |\phi_2\rangle && (6) \end{aligned}$$

After the controlled SWAP, the state reads

$$|\psi_2\rangle = \frac{1}{\sqrt{2}}\left[|0\rangle \otimes |\phi_1\rangle \otimes |\phi_2\rangle + |1\rangle \otimes |\phi_2\rangle \otimes |\phi_1\rangle\right] \quad (7)$$

After the last Hadamard gate, the state reads

$$\begin{aligned}|\psi_3\rangle &= \frac{1}{2}\left[(|0\rangle+|1\rangle)\otimes|\phi_1\rangle\otimes|\phi_2\rangle+(|0\rangle-|1\rangle)\otimes|\phi_2\rangle\otimes|\phi_1\rangle\right]\\ &= |0\rangle\otimes\frac{1}{2}\left[|\phi_1\rangle\otimes|\phi_2\rangle+|\phi_2\rangle\otimes|\phi_1\rangle\right]+|1\rangle\otimes\frac{1}{2}\left[|\phi_1\rangle\otimes|\phi_2\rangle-|\phi_2\rangle\otimes|\phi_1\rangle\right]\end{aligned}$$

---

c. Compute the probability $P(0)$ of obtaining the outcome 0 at the top qubit, the probability $P(1)$ of obtaining the outcome 1, and their bias $P(0)-P(1)$.

Solution: The probability of outcome result correspond to $||\tilde{\Pi}_0|\psi_3\rangle||^2 = \langle\psi_3|\tilde{\Pi}_0|\psi_3\rangle$. It is easy to see that

$$\tilde{\Pi}_0|\psi_3\rangle = |0\rangle\otimes\frac{1}{2}\left[|\phi_1\rangle\otimes|\phi_2\rangle+|\phi_2\rangle\otimes|\phi_1\rangle\right]. \tag{8}$$

Then the probability of its outcome reads

$$\begin{aligned}\langle\psi_3|\tilde{\Pi}_0|\psi_3\rangle &= \frac{1}{4}\left[\langle\phi_1|\otimes\langle\phi_2|+\langle\phi_2|\otimes\langle\phi_1|\right]\left[|\phi_1\rangle\otimes|\phi_2\rangle+|\phi_2\rangle\otimes|\phi_1\rangle\right]\\ &= \frac{1}{4}+\frac{1}{4}\langle\phi_2|\phi_1\rangle\langle\phi_1|\phi_2\rangle+\frac{1}{4}\langle\phi_1|\phi_2\rangle\langle\phi_2|\phi_1\rangle+\frac{1}{4} &(9)\\ &= \frac{1}{2}+\frac{1}{2}\langle\phi_1|\phi_2\rangle\langle\phi_1|\phi_2\rangle^* &(10)\\ &= \frac{1}{2}+\frac{1}{2}|\langle\phi_2|\phi_1\rangle|^2 &(11)\end{aligned}$$

A similar calculation as above leads to:

$$P(1) = \frac{1}{2}-\frac{1}{2}|\langle\phi_2|\phi_1\rangle|^2. \tag{12}$$

Therefore, the bias of probabilities reads $P(0)-P(1) = |\langle\phi_2|\phi_1\rangle|^2$.
