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.

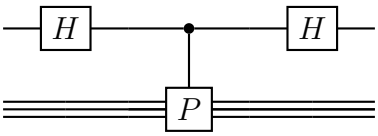
1. Using Euler's formula $e^{i\theta} = \cos\theta + i\sin\theta$ and the relations above, prove that

$$e^{-i\theta P} = e^{-i\theta}\,\Pi_0 + e^{+i\theta}\,\Pi_1.$$

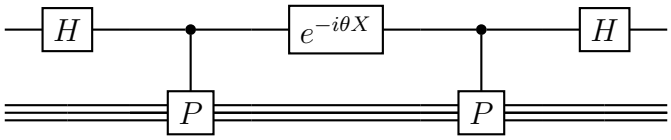
2. Show that

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

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



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



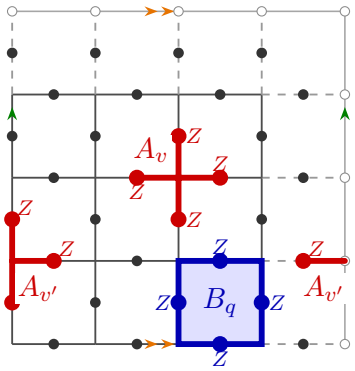
1. Using parts a and b, show that this circuit implements the *Pauli-string rotation* operator

$$|0\rangle\langle 0| \otimes e^{-i\theta P} + |1\rangle\langle 1| \otimes e^{+i\theta P}.$$

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 $|0\rangle$?

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 ($2L^2 = 32$)

$A_v = \prod_{i \in v} Z_i$, $\quad B_q = \prod_{i \in q} Z_i$

$\hat{H} = \sum_v A_v + \sum_q B_q$

▶: 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?

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?

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?

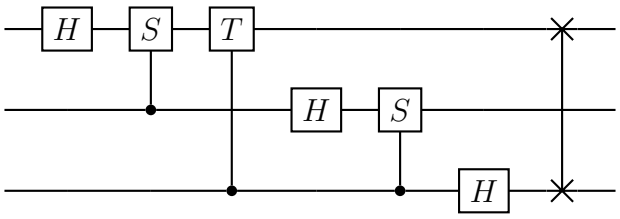
b. Recall that:

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

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 $j_i \in \{0, 1\}$.

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?

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 $r = 4$.

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} (mod$N$) 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.

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?

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

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.

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.

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 $|x\rangle \to |x^{2^k} \bmod N\rangle$?

Extra problem: SWAP Test

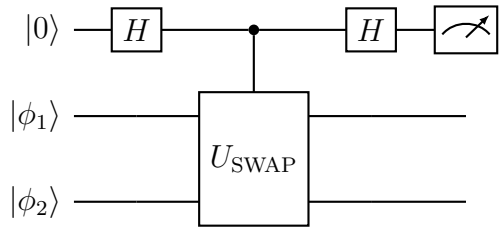
Given the two-qubit SWAP gate:

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

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 $U_{\text{SWAP}}\,|\phi_1\rangle \otimes |\phi_2\rangle = |\phi_2\rangle \otimes |\phi_1\rangle$

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.

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 $P(0) - P(1)$.