4.1 Universal quantum gates I

In this exercise and the two that follow, we will establish that several simple sets of gates are universal for quantum computation.

The Hadamard transformation $H$ is the single-qubit gate that acts in the standard basis $\{|0\rangle, |1\rangle\}$ as

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix};$$  \hspace{1cm} (1)

in quantum circuit notation, we denote the Hadamard gate as

\begin{center}
\begin{tikzpicture}
\node[draw,thick] (H) {H};
\end{tikzpicture}
\end{center}

The single-qubit phase gate $P$ acts in the standard basis as

$$P = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix},$$  \hspace{1cm} (2)

and is denoted

\begin{center}
\begin{tikzpicture}
\node[draw,thick] (P) {P};
\end{tikzpicture}
\end{center}

A two-qubit controlled phase gate $\Lambda(P)$ acts in the standard basis $\{ |00\rangle, |01\rangle, |10\rangle, |11\rangle \}$ as the diagonal $4 \times 4$ matrix

$$\Lambda(P) = \text{diag}(1, 1, 1, i)$$  \hspace{1cm} (3)

and can be denoted

\begin{center}
\begin{tikzpicture}
\node[draw,thick] (P) {P};
\end{tikzpicture}
\end{center}
Despite this misleading notation, the gate $\Lambda(P)$ actually acts symmetrically on the two qubits:

$$\begin{array}{c}
\text{P} = \text{P} \\
\text{P} = \text{P}
\end{array}$$

We will see that the two gates $H$ and $\Lambda(P)$ comprise a universal gate set – any unitary transformation can be approximated to arbitrary accuracy by a quantum circuit built out of these gates.

\(a\) Consider the two-qubit unitary transformations $U_1$ and $U_2$ defined by quantum circuits

$$\begin{array}{c}
\text{U}_1 = \text{H} \quad \text{P} \\
\text{U}_2 = \text{P} \quad \text{H}
\end{array}$$

and

$$\begin{array}{c}
\text{U}_1 = \text{H} \quad \text{P} \\
\text{U}_2 = \text{P} \quad \text{H}
\end{array}$$

Let $|ab\rangle$ denote the element of the standard basis where $a$ labels the upper qubit in the circuit diagram and $b$ labels the lower qubit. Write out $U_1$ and $U_2$ as $4 \times 4$ matrices in the standard basis. Show that $U_1$ and $U_2$ both act trivially on the states

$$|00\rangle, \quad \frac{1}{\sqrt{3}}(|01\rangle + |10\rangle + |11\rangle) \quad . \quad (4)$$

\(b\) Thus $U_1$ and $U_2$ act nontrivially only in the two-dimensional space spanned by

$$\left\{ \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle), \frac{1}{\sqrt{6}}(|01\rangle + |10\rangle - 2|11\rangle) \right\} . \quad (5)$$

Show that, expressed in this basis, they are

$$U_1 = \frac{1}{4} \begin{pmatrix} 3 + i & \sqrt{3}(1 + i) \\ \sqrt{3}(-1 + i) & 1 + 3i \end{pmatrix} , \quad (6)$$

and

$$U_2 = \frac{1}{4} \begin{pmatrix} 3 + i & \sqrt{3}(1 - i) \\ \sqrt{3}(1 - i) & 1 + 3i \end{pmatrix} . \quad (7)$$
c) Now express the action of $U_1$ and $U_2$ on this two-dimensional subspace in the form

$$U_1 = \sqrt{i} \left( \frac{1}{\sqrt{2}} - i \frac{1}{\sqrt{2}} \hat{n}_1 \cdot \vec{\sigma} \right),$$ \hspace{1cm} (8)

and

$$U_2 = \sqrt{i} \left( \frac{1}{\sqrt{2}} - i \frac{1}{\sqrt{2}} \hat{n}_2 \cdot \vec{\sigma} \right).$$ \hspace{1cm} (9)

What are the unit vectors $\hat{n}_1$ and $\hat{n}_2$?

d) Consider the transformation $U_2^{-1}U_1$ (Note that $U_2^{-1}$ can also be constructed from the gates $H$ and $\Lambda(P)$.) Show that it performs a rotation with half-angle $\theta/2$ in the two-dimensional space spanned by the basis eq. (5), where $\cos(\theta/2) = 1/4$.

4.2 Universal quantum gates II

We have now seen how to compose our fundamental quantum gates to perform, in a two-dimensional subspace of the four-dimensional Hilbert space of two qubits, a rotation with $\cos(\theta/2) = 1/4$. In this exercise, we will show that the angle $\theta$ is not a rational multiple of $\pi$. Equivalently, we will show that

$$e^{i\theta/2} \equiv \cos(\theta/2) + i \sin(\theta/2) = \frac{1}{4} \left( 1 + i \sqrt{15} \right)$$ \hspace{1cm} (10)

is not a root of unity: there is no finite integer power $n$ such that $(e^{i\theta/2})^n = 1$.

Recall that a polynomial of degree $n$ is an expression

$$P(x) = \sum_{k=0}^{n} a_k x^k$$ \hspace{1cm} (11)

with $a_n \neq 0$. We say that the polynomial is rational if all of the $a_k$'s are rational numbers, and that it is monic if $a_n = 1$. A polynomial is integral if all of the $a_k$'s are integers, and an integral polynomial is primitive if the greatest common divisor of $\{a_0, a_1, \ldots, a_n\}$ is 1.

a) Show that the monic rational polynomial of minimal degree that has $e^{i\theta/2}$ as a root is

$$P(x) = x^2 - \frac{1}{2} x + 1.$$ \hspace{1cm} (12)
The property that $e^{i\theta/2}$ is not a root of unity follows from the result 
(a) and the

**Theorem** If $a$ is a root of unity, and $P(x)$ is a monic rational polynomial of minimal degree with $P(a) = 0$, then $P(x)$ is integral.

Since the minimal monic rational polynomial with root $e^{i\theta/2}$ is not integral, we conclude that $e^{i\theta/2}$ is not a root of unity. In the rest of this exercise, we will prove the theorem.

b) By “long division” we can prove that if $A(x)$ and $B(x)$ are rational polynomials, then there exist rational polynomials $Q(x)$ and $R(x)$ such that

$$A(x) = B(x)Q(x) + R(x),$$

where the “remainder” $R(x)$ has degree less than the degree of $B(x)$. Suppose that $a^n = 1$, and that $P(x)$ is a rational polynomial of minimal degree such that $P(a) = 0$. Show that there is a rational polynomial $Q(x)$ such that

$$x^n - 1 = P(x)Q(x).$$

c) Show that if $A(x)$ and $B(x)$ are both primitive integral polynomials, then so is their product $C(x) = A(x)B(x)$. **Hint:** If $C(x) = \sum_k c_k x^k$ is not primitive, then there is a prime number $p$ that divides all of the $c_k$’s. Write $A(x) = \sum_l a_l x^l$, and $B(x) = \sum_m b_m x^m$, let $a_r$ denote the coefficient of lowest order in $A(x)$ that is not divisible by $p$ (which must exist if $A(x)$ is primitive), and let $b_s$ denote the coefficient of lowest order in $B(x)$ that is not divisible by $p$. Express the product $a_rb_s$ in terms of $c_{r+s}$ and the other $a_l$’s and $b_m$’s, and reach a contradiction.

d) Suppose that a monic integral polynomial $P(x)$ can be factored into a product of two monic rational polynomials, $P(x) = A(x)B(x)$. Show that $A(x)$ and $B(x)$ are integral. **Hint:** First note that we may write $A(x) = (1/r) \cdot \tilde{A}(x)$, and $B(x) = (1/s) \cdot \tilde{B}(x)$, where $r, s$ are positive integers, and $\tilde{A}(x)$ and $\tilde{B}(x)$ are primitive integral; then use (c) to show that $r = s = 1$.

e) Combining (b) and (d), prove the theorem.

What have we shown? Since $U_2^{-1}U_1$ is a rotation by an irrational multiple of $\pi$, the powers of $U_2^{-1}U_1$ are dense in a $U(1)$ subgroup.
Similar reasoning shows that $U_1U_2^{-1}$ is a rotation by the same angle about a different axis, and therefore its powers are dense in another $U(1)$ subgroup. Products of elements of these two noncommuting $U(1)$ subgroups are dense in the $SU(2)$ subgroup that contains both $U_1$ and $U_2$.

Furthermore, products of $\Lambda(P)U_1^{-1}U_1\Lambda(P)^{-1}$ and $\Lambda(P)U_1U_2^{-1}\Lambda(P)^{-1}$ are dense in another $SU(2)$, spanned by

\[
\left\{ \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle), \frac{1}{\sqrt{6}}(|01\rangle + |10\rangle - 2i|11\rangle) \right\} .
\]

Together, these two $SU(2)$ subgroups close on the $SU(3)$ subgroup that acts on the three-dimensional space orthogonal to $|00\rangle$. Conjugating this $SU(3)$ by $H \otimes H$ we obtain another $SU(3)$ acting on the three-dimensional space orthogonal to $|+, +\rangle$, where $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. The only subgroup of $SU(4)$ that contains both of these $SU(3)$ subgroups is $SU(4)$ itself.

Therefore, the circuits constructed from the gate set $\{H, \Lambda(P)\}$ are dense in $SU(4)$ — we can approximate any two-qubit gate to arbitrary accuracy, which we know suffices for universal quantum computation. Whew!

### 4.3 Universal quantum gates III

We have shown that the gate set $\{H, \Lambda(P)\}$ is universal. Thus any gate set from which both $H$ and $\Lambda(P)$ can be constructed is also universal. In particular, we can see that $\{H, P, \Lambda^2(X)\}$ is a universal set.

- It is sometimes convenient to characterize a quantum gate by specifying the action of the gate when it conjugates a Pauli operator. Show that $H$ and $P$ have the properties

\[
H X H = Z , \quad H Y H = -Y , \quad H Z H = X ,
\]

and

\[
P X P^{-1} = Y , \quad P Y P^{-1} = -X , \quad P Z P^{-1} = Z .
\]

- Note that, since $P^{-1} = P^3$, the gate $K = H P^{-1} H P H$ can be constructed using $H$ and $P$. Show that

\[
K X K = Y , \quad K Y K = X , \quad K Z K = -Z .
\]
c) Construct circuits for $\Lambda^2(Y)$ and $\Lambda^2(Z)$ using the gate set \{\(H, P, \Lambda^2(X)\)\}. Then complete the proof of universality for this gate set by constructing $\Lambda(P) \otimes I$ using $\Lambda^2(X)$, $\Lambda^2(Y)$, and $\Lambda^2(Z)$.

The Toffoli gate $\Lambda^2(X)$ is universal for reversible classical computation. What must be added to realize the full power of quantum computing? We have just seen that the single-qubit gates $H$ and $P$, together with the Toffoli gate, are adequate for reaching any unitary transformation. But in fact, just $H$ and $\Lambda^2(X)$ suffice to efficiently simulate any quantum computation.

Of course, since $H$ and $\Lambda^2(X)$ are both real orthogonal matrices, a circuit composed from these gates is necessarily real — there are complex $n$-qubit unitaries that cannot be constructed with these tools. But a $2^n$-dimensional complex vector space is isomorphic to a $2^{n+1}$-dimensional real vector space. A complex vector can be encoded by a real vector according to

$$|\psi\rangle = \sum_x \psi_x |x\rangle \mapsto |\tilde{\psi}\rangle = \sum_x (\text{Re} \, \psi_x) |x,0\rangle + (\text{Im} \, \psi_x) |x,1\rangle ,$$

and the action of the unitary transformation $U$ can be represented by a real orthogonal matrix $U_R$ defined as

$$U_R : |x,0\rangle \mapsto (\text{Re} \, U) |x\rangle \otimes |0\rangle + (\text{Im} \, U) |x\rangle \otimes |1\rangle ,$$

$$|x,1\rangle \mapsto -(\text{Im} \, U) |x\rangle \otimes |0\rangle + (\text{Re} \, U) |x\rangle \otimes |1\rangle .$$

To show that the gate set \{\(H, \Lambda^2(X)\)\} is “universal,” it suffices to demonstrate that the real encoding $\Lambda(P)_R$ of $\Lambda(P)$ can be constructed from $\Lambda^2(X)$ and $H$.

d) Verify that $\Lambda(P)_R = \Lambda^2(XZ)$.
e) Use $\Lambda^2(X)$ and $H$ to construct a circuit for $\Lambda^2(XZ)$.

Thus, the classical Toffoli gate does not need much help to unleash the power of quantum computing. In fact, any nonclassical single-qubit gate (one that does not preserve the computational basis), combined with the Toffoli gate, is sufficient.
4.4 Universality from any entangling two-qubit gate

We say that a two-qubit unitary quantum gate is local if it is a tensor product of single-qubit gates, and that the two-qubit gates $U$ and $V$ are locally equivalent if one can be transformed to the other by local gates:

$$ V = (A \otimes B)U(C \otimes D) . $$  \hspace{1cm} (21)

It turns out (you are not asked to prove this) that every two-qubit gate is locally equivalent to a gate of the form:

$$ V(\theta_x, \theta_y, \theta_z) = \exp \left[ i (\theta_x X \otimes X + \theta_y Y \otimes Y + \theta_z Z \otimes Z) \right] , $$  \hspace{1cm} (22)

where

$$ -\pi/4 < \theta_x \leq \theta_y \leq \theta_z \leq \pi/4 . $$  \hspace{1cm} (23)

a) Show that $V(\pi/4, \pi/4, \pi/4)$ is (up to an overall phase) the SWAP operation that interchanges the two qubits:

$$ \text{SWAP} (|\psi\rangle \otimes |\phi\rangle) = |\phi\rangle \otimes |\psi\rangle . $$  \hspace{1cm} (24)

b) Show that $V(0,0,\pi/4)$ is locally equivalent to the CNOT gate $\Lambda(X)$.

As discussed in the lecture notes, the CNOT gate $\Lambda(X)$ together with arbitrary single-qubit gates form a universal gate set. But in fact there is nothing special about the the CNOT gate in this regard. Any two-qubit gate $U$, when combined with arbitrary single-qubit gates, suffices for universality unless $U$ is either local or locally equivalent to SWAP.

To demonstrate that $U$ is universal when assisted by local gates it suffices to construct $\Lambda(X)$ using a circuit containing only local gates and $U$ gates.

**Lemma** If $U$ is locally equivalent to $V(\theta_x, \theta_y, \theta_z)$, then $\Lambda(X)$ can be constructed from a circuit using local gates and $U$ gates except in two cases: (1) $\theta_x = \theta_y = \theta_z = 0$ ($U$ is local), (2) $\theta_x = \theta_y = \theta_z = \pi/4$ ($U$ is locally equivalent to SWAP).

You will prove the Lemma in the rest of this exercise.
c) Show that:

\[(I \otimes X)V(\theta_x, \theta_y, \theta_z)(I \otimes X)V(\theta_x, \theta_y, \theta_z) = V(2\theta_x, 0, 0),\]
\[(I \otimes Y)V(\theta_x, \theta_y, \theta_z)(I \otimes Y)V(\theta_x, \theta_y, \theta_z) = V(0, 2\theta_y, 0),\]
\[(I \otimes Z)V(\theta_x, \theta_y, \theta_z)(I \otimes Z)V(\theta_x, \theta_y, \theta_z) = V(0, 0, 2\theta_z).\]

(d) Show that \(V(0, 0, \theta)\) is locally equivalent to the controlled rotation \(\Lambda[R(\hat{n}, 4\theta)]\), where \(R(\hat{n}, 4\theta) = \exp[-2i\theta(\hat{n} \cdot \sigma)]\), for an arbitrary axis of rotation \(\hat{n}\). (Here \(\sigma = (X, Y, Z)\).)

e) Now use the results of (c) and (d) to prove the Lemma.