Ph 219b/CS 219b

Exercises
Due: Thursday 21 November 2019

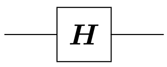
3.1 Universal quantum gates I

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

$$\boldsymbol{H} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} ; \tag{1}$$

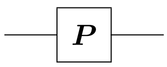
in quantum circuit notation, we denote the Hadamard gate as



The single-qubit *phase gate* $\boldsymbol{P}$ acts in the standard basis as

$$\boldsymbol{P} = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} , \tag{2}$$

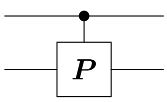
and is denoted



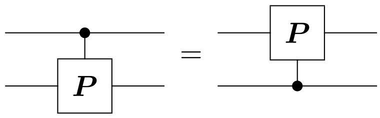
A two-qubit *controlled phase gate* $\Lambda(\boldsymbol{P})$ acts in the standard basis $\{|00\rangle, 01\rangle, |10\rangle, |11\rangle\}$ as the diagonal 4×4 matrix

$$\Lambda(\boldsymbol{P}) = \mathrm{diag}(1, 1, 1, i) \tag{3}$$

and can be denoted

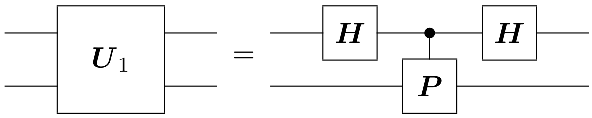


Despite this misleading notation, the gate $\Lambda(\boldsymbol{P})$ actually acts symmetrically on the two qubits:

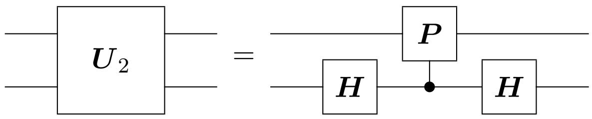


We will see that the two gates $\boldsymbol{H}$ and $\Lambda(\boldsymbol{P})$ comprise a *universal gate set* – any unitary transformation can be approximated to arbitrary accuracy by a quantum circuit built out of these gates.

a) Consider the two-qubit unitary transformations $\boldsymbol{U}_1$ and $\boldsymbol{U}_2$ defined by quantum circuits



and



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 $\boldsymbol{U}_1$ and $\boldsymbol{U}_2$ as 4×4 matrices in the standard basis. Show that $\boldsymbol{U}_1$ and $\boldsymbol{U}_2$ both act trivially on the states

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

b) Thus $\boldsymbol{U}_1$ and $\boldsymbol{U}_2$ act nontrivially only in the two-dimensional space spanned by

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

Show that, expressed in this basis, they are

$$\boldsymbol{U}_1 = \frac{1}{4}\begin{pmatrix} 3+i & \sqrt{3}(-1+i) \\ \sqrt{3}(-1+i) & 1+3i \end{pmatrix} \ , \tag{6}$$

and

$$\boldsymbol{U}_2 = \frac{1}{4}\begin{pmatrix} 3+i & \sqrt{3}(1-i) \\ \sqrt{3}(1-i) & 1+3i \end{pmatrix} \ . \tag{7}$$

c) Now express the action of $\boldsymbol{U}_1$ and $\boldsymbol{U}_2$ on this two-dimensional subspace in the form

$$\boldsymbol{U}_1 = \sqrt{i}\left(\frac{1}{\sqrt{2}} - i\frac{1}{\sqrt{2}}\hat{n}_1 \cdot \vec{\boldsymbol{\sigma}}\right) , \tag{8}$$

and

$$\boldsymbol{U}_2 = \sqrt{i}\left(\frac{1}{\sqrt{2}} - i\frac{1}{\sqrt{2}}\hat{n}_2 \cdot \vec{\boldsymbol{\sigma}}\right) . \tag{9}$$

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

d) Consider the transformation $\boldsymbol{U}_2^{-1}\boldsymbol{U}_1$ (Note that $\boldsymbol{U}_2^{-1}$ can also be constructed from the gates $\boldsymbol{H}$ and $\Lambda(\boldsymbol{P})$.) Show that it performs a rotation with half-angle $\theta/2$ in the two-dimensional space spanned by the basis eq. (**??**), where $\cos(\theta/2) = 1/4$.

3.2 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 θ is not a rational multiple of π. Equivalently, we will show that

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

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

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

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

$$P(x) = x^2 - \frac{1}{2}x + 1 . \tag{12}$$

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

$$A(x) = B(x)Q(x) + R(x) \ , \tag{13}$$

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

$$x^n - 1 = P(x)Q(x) \ . \tag{14}$$

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 $a_r b_s$ 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 $\boldsymbol{U}_2^{-1}\boldsymbol{U}_1$ is a rotation by an irrational multiple of π, the powers of $\boldsymbol{U}_2^{-1}\boldsymbol{U}_1$ are dense in a $U(1)$ subgroup.

Similar reasoning shows that $\boldsymbol{U}_1\boldsymbol{U}_2^{-1}$ 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 $\boldsymbol{U}_1$ and $\boldsymbol{U}_2$.

Furthermore, products of $\Lambda(\boldsymbol{P})\boldsymbol{U}_2^{-1}\boldsymbol{U}_1\Lambda(\boldsymbol{P})^{-1}$ and $\Lambda(\boldsymbol{P})\boldsymbol{U}_1\boldsymbol{U}_2^{-1}\Lambda(\boldsymbol{P})^{-1}$ are dense in another $SU(2)$, acting on the span of

$$\left\{\frac{1}{\sqrt{2}}(|01\rangle - |10\rangle), \frac{1}{\sqrt{6}}(|01\rangle + |10\rangle - 2i|11\rangle)\right\} . \tag{15}$$

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

3.3 Universal quantum gates III

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

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

$$\boldsymbol{HXH} = \boldsymbol{Z} , \quad \boldsymbol{HYH} = -\boldsymbol{Y} , \quad \boldsymbol{HZH} = \boldsymbol{X} , \tag{16}$$

and

$$\boldsymbol{PXP}^{-1} = \boldsymbol{Y} , \quad \boldsymbol{PYP}^{-1} = -\boldsymbol{X} , \quad \boldsymbol{PZP}^{-1} = \boldsymbol{Z} . \tag{17}$$

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

$$\boldsymbol{KXK} = \boldsymbol{Y} , \quad \boldsymbol{KYK} = \boldsymbol{X} , \quad \boldsymbol{KZK} = -\boldsymbol{Z} . \tag{18}$$

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

The Toffoli gate $\Lambda^2(\boldsymbol{X})$ 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 $\boldsymbol{H}$ and $\boldsymbol{P}$, together with the Toffoli gate, are adequate for reaching any unitary transformation. But in fact, just $\boldsymbol{H}$ and $\Lambda^2(\boldsymbol{X})$ suffice to efficiently simulate any quantum computation.

Of course, since $\boldsymbol{H}$ and $\Lambda^2(\boldsymbol{X})$ 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

$$|\psi\rangle = \sum_x \psi_x |x\rangle \mapsto |\tilde{\psi}\rangle = \sum_x (\text{Re } \psi_x)|x,0\rangle + (\text{Im } \psi_x)|x,1\rangle \ , \qquad (19)$$

and the action of the unitary transformation $\boldsymbol{U}$ can be represented by a real orthogonal matrix $\tilde{U}_R$ defined as

$$\begin{aligned} U_R : \qquad & |x,0\rangle \mapsto (\text{Re } U)|x\rangle \otimes |0\rangle + (\text{Im } U)|x\rangle \otimes |1\rangle \ , \\ & |x,1\rangle \mapsto -(\text{Im } U)|x\rangle \otimes |0\rangle + (\text{Re } U)|x\rangle \otimes |1\rangle \ . \end{aligned} \qquad (20)$$

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

d) Verify that $\Lambda(\boldsymbol{P})_R = \Lambda^2(\boldsymbol{XZ})$.

e) Use $\Lambda^2(\boldsymbol{X})$ and $\boldsymbol{H}$ to construct a circuit for $\Lambda^2(\boldsymbol{XZ})$.

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.

3.4 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 $\boldsymbol{U}$ and $\boldsymbol{V}$ are *locally equivalent* if one can be transformed to the other by local gates:

$$\boldsymbol{V} = (\boldsymbol{A} \otimes \boldsymbol{B})\boldsymbol{U}(\boldsymbol{C} \otimes \boldsymbol{D}) \ . \tag{21}$$

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

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

where

$$-\pi/4 < \theta_x \leq \theta_y \leq \theta_z \leq \pi/4 \ . \tag{23}$$

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

$$\textbf{SWAP}\left(|\psi\rangle \otimes |\phi\rangle\right) = |\phi\rangle \otimes |\psi\rangle \ . \tag{24}$$

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

As discussed in the lecture notes, the CNOT gate $\Lambda(\boldsymbol{X})$ 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 $\boldsymbol{U}$, when combined with arbitrary single-qubit gates, suffices for universality *unless* $\boldsymbol{U}$ is either local or locally equivalent to **SWAP**.

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

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

You will prove the Lemma in the rest of this exercise.

c) Show that:

$$\begin{aligned}
(\boldsymbol{I} \otimes \boldsymbol{X})\boldsymbol{V}(\theta_x, \theta_y, \theta_z)(\boldsymbol{I} \otimes \boldsymbol{X})\boldsymbol{V}(\theta_x, \theta_y, \theta_z) &= \boldsymbol{V}(2\theta_x, 0, 0) \ , \\
(\boldsymbol{I} \otimes \boldsymbol{Y})\boldsymbol{V}(\theta_x, \theta_y, \theta_z)(\boldsymbol{I} \otimes \boldsymbol{Y})\boldsymbol{V}(\theta_x, \theta_y, \theta_z) &= \boldsymbol{V}(0, 2\theta_y, 0) \ , \\
(\boldsymbol{I} \otimes \boldsymbol{Z})\boldsymbol{V}(\theta_x, \theta_y, \theta_z)(\boldsymbol{I} \otimes \boldsymbol{Z})\boldsymbol{V}(\theta_x, \theta_y, \theta_z) &= \boldsymbol{V}(0, 0, 2\theta_z) \ .
\end{aligned} \tag{25}$$

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

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