

# Ph 219A/CS 219A

## Exercises

Due: Friday 12 November 2021

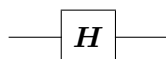
### 3.1 Universal quantum gates I

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

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

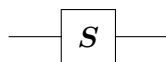
in quantum circuit notation, we denote the Hadamard gate as



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

$$\mathbf{S} = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} , \quad (2)$$

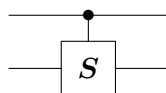
and is denoted



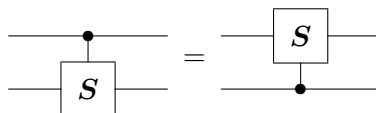
A two-qubit *controlled phase gate*  $\Lambda(\mathbf{S})$  acts in the standard basis  $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$  as the diagonal  $4 \times 4$  matrix

$$\Lambda(\mathbf{S}) = \text{diag}(1, 1, 1, i) \quad (3)$$

and can be denoted

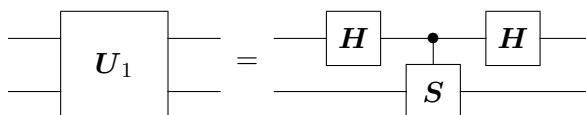


Despite this misleading notation, the gate  $\Lambda(\mathbf{S})$  actually acts symmetrically on the two qubits:

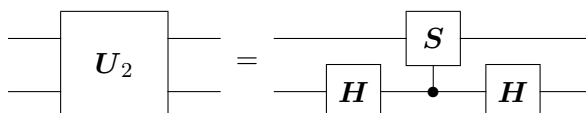


We will see that the two gates  $\mathbf{H}$  and  $\Lambda(\mathbf{S})$  comprise a *universal gate set* – any unitary transformation can be approximated to arbitrary accuracy by a quantum circuit built out of these gates.

a) Consider the two-qubit unitary transformations  $\mathbf{U}_1$  and  $\mathbf{U}_2$  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  $\mathbf{U}_1$  and  $\mathbf{U}_2$  as  $4 \times 4$  matrices in the standard basis. Show that  $\mathbf{U}_1$  and  $\mathbf{U}_2$  both act trivially on the states

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

b) Thus  $\mathbf{U}_1$  and  $\mathbf{U}_2$  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

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

and

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

- c) Now express the action of  $U_1$  and  $U_2$  on this two-dimensional subspace in the form

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

and

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

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  $\mathbf{H}$  and  $\Lambda(\mathbf{S})$ .) Show that it performs a rotation with half-angle  $\theta/2$  in the two-dimensional space spanned by the basis eq. (5), where  $\cos(\theta/2) = 1/4$ .

### 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  $\theta$  is not a rational multiple of  $\pi$ . Equivalently, we will show that

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

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

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

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  $\{a_0, a_1, \dots, a_n\}$  is 1.

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

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

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

$$A(x) = B(x)Q(x) + R(x) , \quad (13)$$

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

$$x^n - 1 = P(x)Q(x) . \quad (14)$$

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  $U_2^{-1}U_1$  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  $\mathbf{U}_1\mathbf{U}_2^{-1}$  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  $\mathbf{U}_1$  and  $\mathbf{U}_2$ .

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

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

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

$$\mathbf{H}\mathbf{X}\mathbf{H} = \mathbf{Z}, \quad \mathbf{H}\mathbf{Y}\mathbf{H} = -\mathbf{Y}, \quad \mathbf{H}\mathbf{Z}\mathbf{H} = \mathbf{X}, \quad (16)$$

and

$$\mathbf{S}\mathbf{X}\mathbf{S}^{-1} = \mathbf{Y}, \quad \mathbf{S}\mathbf{Y}\mathbf{S}^{-1} = -\mathbf{X}, \quad \mathbf{S}\mathbf{Z}\mathbf{S}^{-1} = \mathbf{Z}. \quad (17)$$

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

$$\mathbf{K}\mathbf{X}\mathbf{K} = \mathbf{Y}, \quad \mathbf{K}\mathbf{Y}\mathbf{K} = \mathbf{X}, \quad \mathbf{K}\mathbf{Z}\mathbf{K} = -\mathbf{Z}. \quad (18)$$

c) Construct circuits for  $\Lambda^2(\mathbf{Y})$  and  $\Lambda^2(\mathbf{Z})$  using the gate set  $\{\mathbf{H}, \mathbf{S}, \Lambda^2(\mathbf{X})\}$ .

Then complete the proof of universality for this gate set by constructing  $\Lambda(\mathbf{S}) \otimes \mathbf{I}$  using  $\Lambda^2(\mathbf{X})$ ,  $\Lambda^2(\mathbf{Y})$ , and  $\Lambda^2(\mathbf{Z})$ .

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

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

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

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

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

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

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

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

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

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

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

$$\mathbf{V}(\theta_x, \theta_y, \theta_z) = \exp [i(\theta_x \mathbf{X} \otimes \mathbf{X} + \theta_y \mathbf{Y} \otimes \mathbf{Y} + \theta_z \mathbf{Z} \otimes \mathbf{Z})] , \quad (22)$$

where

$$-\pi/4 < \theta_x \leq \theta_y \leq \theta_z \leq \pi/4 . \quad (23)$$

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

$$\mathbf{SWAP} (|\psi\rangle \otimes |\phi\rangle) = |\phi\rangle \otimes |\psi\rangle . \quad (24)$$

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

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

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

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

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

c) Show that:

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

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

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