Ph 219b/CS 219b

Exercises
Due: Friday 3 February 2006

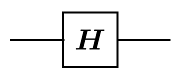
5.1 Universal quantum gates I

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

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

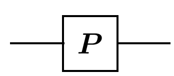
in quantum circuit notation, we denote the Hadamard gate as



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

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

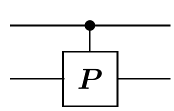
and is denoted



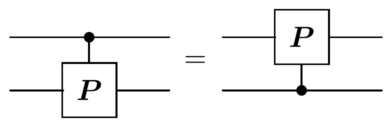
A two-qubit *controlled phase gate* $\Lambda(\boldsymbol{P})$ acts in the standard basis $\{|00\rangle, 01\rangle, |10\rangle, |11\rangle\}$ as the diagonal 4×4 matrix

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

and can be denoted

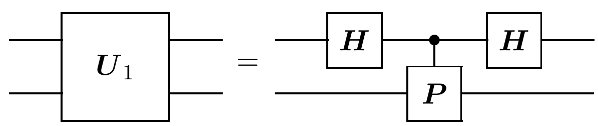


Despite this misleading notation, the gate $\Lambda(\boldsymbol{P})$ actually acts symmetrically on the two qubits:

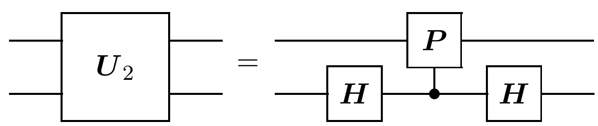


We will see that the two gates $\boldsymbol{H}$ and $\Lambda(\boldsymbol{P})$ comprise a *universal gate set* – any unitary transformation can be approximated to arbitrary accuracy by a quantum circuit built out of these gates.

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. (5), where $\cos(\theta/2) = 1/4$.

5.2 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 this angle 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 not 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 $SU(2)$, spanned by

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

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.

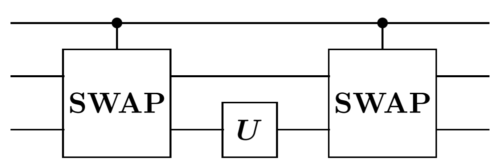
Therefore, the circuits constructed from the gate set $\{\boldsymbol{H}, \Lambda(\boldsymbol{P})\}$ are dense in $SU(4)$ — we can approximate any two-qubit gate to arbitrary accuracy, which we know suffices for universal quantum computation. Whew!

5.3 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) The three-qubit controlled-swap gate $\Lambda(\mathbf{SWAP})$ swaps its two target qubits when the control qubit is $|1\rangle$ and acts trivially if the control qubit is $|0\rangle$. Use the Toffoli gate $\Lambda^2(\boldsymbol{X})$ to construct a circuit for $\Lambda(\mathbf{SWAP})$.

b) Use $\Lambda(\mathbf{SWAP})$, $\boldsymbol{P}$, and a constant qubit to construct a circuit for $\Lambda(\boldsymbol{P})$. **Hint**: What does the following circuit do?



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 compose 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

$$|\psi\rangle = \sum_x \psi_x|x\rangle \mapsto |\tilde{\psi}\rangle = \sum_x (\mathrm{Re}\ \psi_x)|x,0\rangle + (\mathrm{Im}\ \psi_x)|x,1\rangle\ , \qquad (16)$$

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

$$\begin{aligned} U_R: \qquad & |x,0\rangle \mapsto (\mathrm{Re}\ U)|x\rangle \otimes |0\rangle + (\mathrm{Im}\ U)|x\rangle \otimes |1\rangle \\ & |x,1\rangle \mapsto -(\mathrm{Im}\ U)|x\rangle \otimes |0\rangle + (\mathrm{Re}\ U)|x\rangle \otimes |1\rangle\ . \end{aligned} \qquad (17)$$

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 $\boldsymbol{H}$.

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

d) 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.

5.4 Entanglement of typical bipartite pure states

In our sketchy discussion of the proof of the mother resource inequality, we used an important property of bipartite entanglement: If $d_A/d_B \ll 1$, then if a pure state of AB is chosen at random, the density operator of A is likely to be very nearly maximally mixed. The purpose of this problem is to derive this property.

To begin with, we will calculate the value of $\langle \mathrm{tr}\ \rho_A^2 \rangle$, where $\langle \cdot \rangle$ denotes the average over all pure states $\{|\varphi\rangle\}$ of AB, and $\rho_A = \mathrm{tr}_B\left(|\varphi\rangle\langle\varphi|\right)$.

a) It is convenient to evaluate $\mathrm{tr}\ \rho_A^2$ using a trick. Imagine introducing a copy $A'B'$ of the system AB. Show that

$$\mathrm{tr}_A\ \rho_A^2 = \mathrm{tr}_{ABA'B'}\left[\left(S_{AA'} \otimes I_{BB'}\right)\left(|\varphi\rangle\langle\varphi|\right)_{AB} \otimes |\varphi\rangle\langle\varphi|_{A'B'})\right] \ , \tag{18}$$

where $S_{AA'}$ denotes the swap operator

$$S_{AA'} : |\varphi\rangle_A \otimes |\psi\rangle_{A'} \mapsto |\psi\rangle_A \otimes |\varphi\rangle_{A'} \ . \tag{19}$$

b) We wish to average the expression found in (*a*) over all pure states $|\varphi\rangle$. Rather than go into the details of how such an average is defined, I will simply assert that

$$\langle |\varphi\rangle\langle\varphi|_A \otimes |\varphi\rangle\langle\varphi|_{A'} \rangle = C\ \Pi_{AA'} \ , \tag{20}$$

where C is a constant and $\Pi_{AA'}$ denotes the projector onto the subspace of AA' that is *symmetric* under interchange of A and A'. Eq. (20) can be proved using invariance properties of the average and some group representation theory, but I hope you will regard it as obvious. The state being averaged is symmetric, and the average should not distinguish any symmetric state from any other symmetric state. Express the constant C in terms of the dimension $d \equiv d_A = d_{A'}$.

c) Use the property $\Pi_{AA'} = \frac{1}{2}\left(I_{AA'} + S_{AA'}\right)$ to evaluate the expression found in (*a*). Show that

$$\left\langle \mathrm{tr}\ \rho_A^2 \right\rangle = \frac{d_A + d_B}{d_A d_B + 1} \ . \tag{21}$$

d) Now estimate the average L^2 distance of ρ_A from the maximally mixed density operator $\frac{1}{d_A} I_A$, where $\| M \|_2 = \sqrt{\mathrm{tr} M^\dagger M}$. First show that

$$\left\langle \|\rho_A - \frac{1}{d_A} I_A\|_2^2 \right\rangle \leq \frac{1}{d_B} \ . \tag{22}$$

(**Hint**: Use the obvious property $\langle \rho_A \rangle = \frac{1}{d_A} I_A$.) Next show that for any nonnegative function f, it follows from the Cauchy-Schwarz inequality that $\left\langle \sqrt{f} \right\rangle \leq \sqrt{\langle f \rangle}$; thus

$$\left\langle \| \rho_A - \frac{1}{d_A} I_A \|_2 \right\rangle \leq \frac{1}{\sqrt{d_B}} \ . \tag{23}$$

e) Finally, estimate the average L^1 distance of ρ_A from the maximally mixed density operator, where $\| M \|_1 = \mathrm{tr}\ \sqrt{M^\dagger M}$. Use the Cauchy-Schwarz inequality to show that $\| M \|_1 \leq \sqrt{d} \| M \|_2$, if M is a $d \times d$ matrix, and that therefore

$$\left\langle \| \rho_A - \frac{1}{d_A} I_A \|_1 \right\rangle \leq \sqrt{\frac{d_A}{d_B}} \ . \tag{24}$$

It follows from (d) that the average entanglement entropy of A and B is close to maximal for $d_A/d_B \ll 1$: $\langle H(A) \rangle \geq \log_2 d_A - d_A/2d_B \ln 2$, though you are not asked to prove this bound. Thus, if for example A is 50 qubits and B is 100 qubits, the typical entropy deviates from maximal by only about $2^{-50} \approx 10^{-15}$.