September 11, 1997

II. Quantum Gates and Circuits

1 Quantum gates

Changes occurring to a quantum state vector can be modeled using a *quantum circuit*, composed of wires and elementary gates, much as normal electronic circuits are used to describe electrical and mechanical systems. We describe a basic set of quantum gates which are useful, and present several examples illustrating their application, including a circuit which attempts to copy, and a circuit which teleports qubits.

1.1 Single bit gates

Consider the class of single bit gates. Classically, the only non-trivial member of this class is the NOT gate, whose operation is defined by its *truth table*, in which $0 \to 1$ and $1 \to 0$.

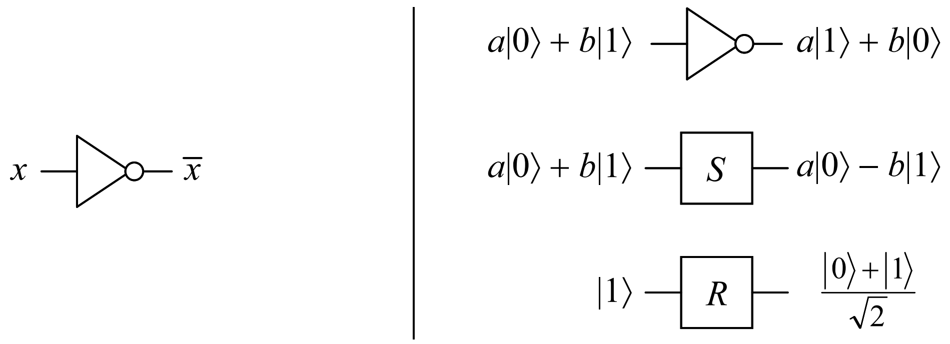


Figure 1: Single bit and qubit logic gates.

There is also a qubit NOT gate. It is defined by its *unitary operator*

$$U_{not} = \begin{array}{cc} \begin{array}{cc} |0\rangle & |1\rangle \end{array} & \\ \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} & \begin{array}{c} |0\rangle \\ |1\rangle \end{array} \end{array} \quad , \tag{1}$$

where – much like a classical truth table – the two columns refer to the inputs ($|0\rangle$ and $|1\rangle$) and the two rows the outputs. The transform must be unitary to preserve the norm of the state. The interesting thing is that there are many additional non-trivial single qubit gates. Two important ones which we shall use later are the phase shift

$$U_S = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} , \tag{2}$$

which leaves $|0\rangle$ alone, and only flips the phase of $|1\rangle$ to give $-|1\rangle$, and the Hadamard gate

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} . \tag{3}$$

This gate is also known as the "square-root of NOT" gate, and its action can be visualized as being similar to rotating the qubit sphere about the $\hat{y}$ axis by 90° (Fig. 2)[1] . This shows how a definite state like $|1\rangle$ can be transformed by H into the *superposition* state $\left[|0\rangle - |1\rangle\right]/\sqrt{2}$, which gives 0 or 1 with equal probability when measured along the computational basis.

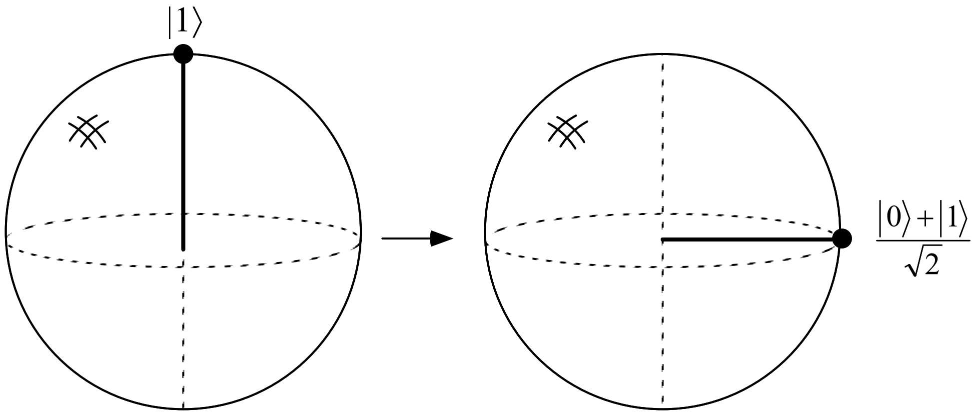


Figure 2: Visualization of "$\sqrt{\text{NOT}}$" logic gate on the qubit sphere.

In general, there are infinitely many single qubit gates, all of which can be generated from *rotations*,

$$U_R(\theta) = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} , \tag{4}$$

and *phase shifts*,

$$U_P(\phi_1, \phi_2) = \begin{pmatrix} e^{i\phi_1} & 0 \\ 0 & e^{i\phi_2} \end{pmatrix} . \tag{5}$$

Mathematically, single qubit transformations are described by $SU(2)$ matrices. It is important to note that although a continuous range of rotations is possible in principle, for quantum computation, only finitely many rotation angles are necessary. It has been shown that a single rotation of nearly any angle is sufficient to allow efficient generation of an arbitrary qubit rotation angle to a precision good enough for the known quantum algorithms to work.

[1] Mathematically, this looks like a 45° rotation; however, in the Bloch sphere picture we use here, the convention is that $R(\theta, \hat{n}) = \exp(i\theta\, \hat{n} \cdot \vec{\sigma}/2)$.

Bloch's Theorem

According to Bloch's theorem for solid body rotations in three dimensions, any arbitrary 2×2 unitary matrix may be written as

$$U = e^{i\gamma}\begin{bmatrix} e^{i\alpha} & 0 \\ 0 & e^{-i\alpha} \end{bmatrix}\begin{bmatrix} \cos\theta & i\sin\theta \\ i\sin\theta & \cos\theta \end{bmatrix}\begin{bmatrix} e^{i\beta} & 0 \\ 0 & e^{-i\beta} \end{bmatrix} \tag{6}$$

$$= e^{i\gamma}e^{i\alpha\sigma_z}e^{i\theta\sigma_x}e^{i\beta\sigma_z}\,, \tag{7}$$

where γ, α, θ, and β are real-valued, and σ_i are the Pauli matrices,

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \tag{8}$$

$$\sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \tag{9}$$

$$\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{10}$$

All single qubit operations may conveniently be expressed in terms of spinor rotations. For example, $U_R = \exp(\pi i\sigma_y/4)$. This will later be useful in connecting such transforms with physical Hamiltonians.

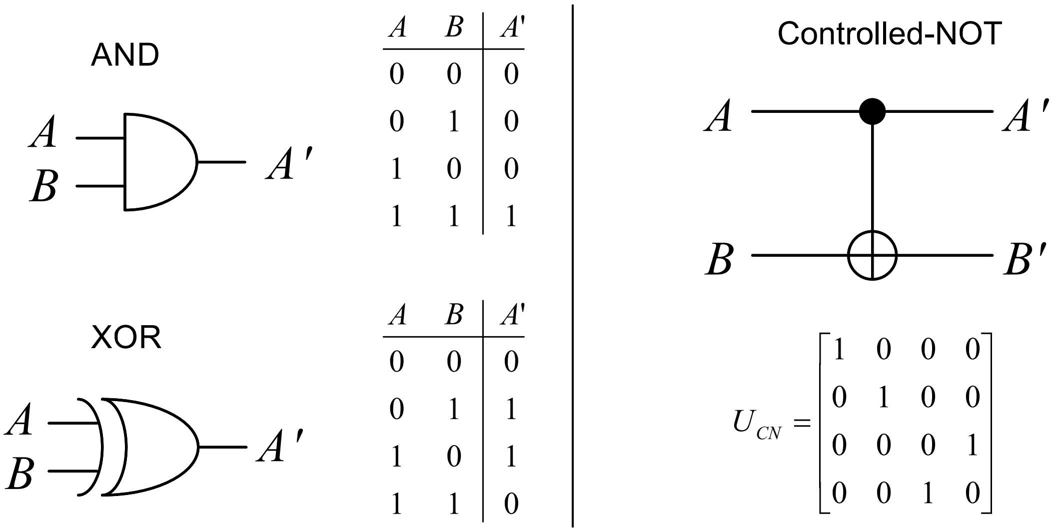
1.2 Multiple bit gates

What can we do with multiple bits? Of the class of multiple bit classical gates, two notable ones are the AND and XOR (exclusive-OR) gates (Fig. 3). An important result of the theory of Boolean algebra is that any Boolean function can be realized from the composition of AND and NOT gates alone, and they are thus said to form a *universal set* of gates. It is interesting, however, that the XOR alone is not universal (it leaves the parity invariant).

The quantum-mechanical analog of the XOR gate is known as the *controlled*-NOT or CNOT gate. This gate is particularly different from the classical two bit gate, however, in that it has two outputs. This is necessary because all quantum logic gates must be *reversible* logic gates[FT82, Ben82, Per85]. We shall return to the subject of reversible logic later when we discuss functions. The key observation here is the following:

> *Theorem 1.1*: Any multiple qubit logic gate may be composed from CNOT and single qubit gates.
>
> *Proof:* See [BBC$^+$95].□

This is one of the most striking results about quantum logic gates, since there exists no universal two-bit reversible classical logic gate.



A	B	A'
0	0	0
0	1	0
1	0	0
1	1	1

A	B	A'
0	0	0
0	1	1
1	0	1
1	1	0

$$U_{CN} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

Figure 3: Multiple bit and qubit gates. The basis elements for U_{CN} are $|00\rangle$, $|01\rangle$, $|10\rangle$, and $|11\rangle$, from left to right and top to bottom.

2 Quantum Circuits

We shall find it useful to use quantum circuits as natural extensions of classical circuits. These consist of quantum gates interconnected without fanout[2] or feedback[BBC+95], by quantum wires. Each wire represents the path of a single qubit (in time or space, forward from left to right), and is described by a state in a two-dimensional Hilbert space with basis $|0\rangle$ and $|1\rangle$.

Aside from the single and multiple qubit gates already introduced, another useful class of gates is shown in Fig. 4. These controlled-operation gates are natural extensions of the controlled-NOT, in which one qubit (labeled by a black dot) serves as the control and the remaining qubits are the targets. Only when the control qubit is 1 will the operation be performed on the target. We will return to such circuits later when we study Kitaev's quantum algorithm.

We shall find quantum circuits useful as models of all quantum processes, including but not limited to computation and decoherence. Several simple examples illustrate this below.

2.1 Qubit Copying Circuit?

The CNOT gate is useful for demonstrating one particularly unique and fundamental property of quantum information. Consider the task of copying a classical bit. This may be done using

[2]Fanin and fanout are electrical engineering terms which refer to the joining and branching of wires. Sometimes n wires are joined together; this provides a "wired-or" and is known as a fanin of n. Also, often logic device outputs drive n wires with the same signal; this provides broadcasting, and is known as a fanout of n.

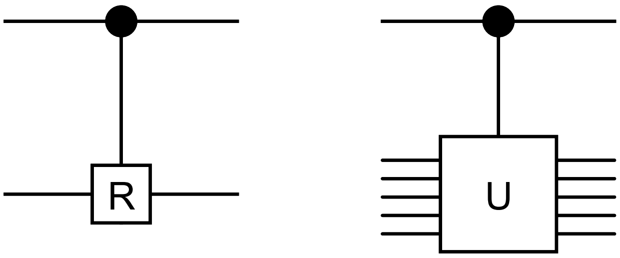


Figure 4: Controlled quantum operations. The gate on the left is a controlled rotation operation, and is denoted as $\Lambda(R)$. Similarly, the controlled (multiple-bit) unitary operation on the right is $\Lambda(U)$.

an XOR gate, which takes in the bit to copy (in some unknown state x) and a "scratchpad" bit initialized to logical zero (Fig. 5). The output is two bits, both of which are in the same state x.

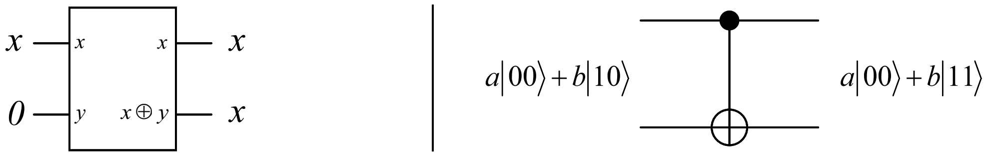


Figure 5: Classical and quantum circuits to copy an unknown bit.

Suppose we try to copy a qubit in the unknown state $|\psi\rangle = a\,|0\rangle + b\,|1\rangle$ in the same manner by using a CNOT gate. The input state of the two qubits may be written as

$$\Big[a\,|0\rangle + b\,|1\rangle\Big] \otimes |0\rangle = a\,|00\rangle + b\,|10\rangle\,, \tag{11}$$

where $\otimes$ is the usual direct (Kronecker) product. The function of CNOT is to negate the second qubit only when the first is one, and thus the output is simply $|\mathrm{out}\rangle = a\,|00\rangle + b\,|11\rangle$. The two qubits are now in the same state! However, consider what happens when we measure one of the qubits. As previously described, we obtain either 0 or 1 with probabilities $|a|^2$ and $|b|^2$. However, once one qubit is measured, the state of the other one is completely determined, and no additional information is gained about a and b. In this sense, the extra hidden information carried in the original qubit $|\psi\rangle$ was lost in the first measurement, and cannot be accessed twice. This means that in fact, the hidden information has not been copied! Fundamentally, this property, that qubits cannot be copied, is known as the *no-cloning* theorem[WZ82, Die82, Per93].

No-Cloning Theorem

Theorem 2.2: There does not exist a unitary transform U such that

$$U|\psi\rangle|0\rangle = |\psi\rangle|\psi\rangle \tag{12}$$

for arbitrary $|\psi\rangle$.

Proof: Suppose there exists U such that

$$\begin{aligned} U|\psi\rangle|0\rangle &= |\psi\rangle|\psi\rangle && (13) \\ U|\phi\rangle|0\rangle &= |\phi\rangle|\phi\rangle && (14) \end{aligned}$$

for arbitrary ψ, ϕ. U would represent a quantum cloning machine if this were possible. However, unitarity implies that

$$\langle\psi|\phi\rangle\langle 0|0\rangle = \langle\psi|\phi\rangle\langle\psi|\phi\rangle \tag{15}$$

but this may be violated by choosing

$$0 < \langle\psi|\phi\rangle < 1\,. \tag{16}$$

Thus, such a U may not exist.$\square$

This result can be extended to include non-unitary transforms (arbitrary quantum operations) as well; see [BCF$^+$96].

Although the two qubits in $|\text{out}\rangle$ appear to be identical, they are not independent copies of $|\psi\rangle$. Rather, they are two *entangled* qubits, which together carry only one qubit of quantum information. There is no classical analog to entangled states; in the extreme limit, they are non-separable states which have observable properties that violate predictions of theories of local classical physics (Bell's inequality). Entanglement is a fundamental property of quantum systems, and is essential to the operation of a quantum computer[3].

2.2 Example: EPR Pairs

Let us now consider a slightly more complicated circuit, shown in Fig. 6, which has a Hadamard gate followed by a CNOT. This circuit transforms the four classical basis states as given in Table 1. Note how this works: first, the Hadamard transform puts the top qubit in a superposition; this then acts as a control input to the CNOT, and the target gets inverted only when the control is 1. The states $|\Psi^{\pm}\rangle$, $|\Phi^{\pm}\rangle$ are known as the Bell states, and will later be important as we

[3] To be precise, it can be shown that no exponential speedup can be achieved by a quantum algorithm without using entangled states. An important open question is exactly why entanglement is important, and how it should be used for computation and communication.

In	Out
00	$\|00\rangle + \|11\rangle \equiv \|\Psi^+\rangle$
01	$\|01\rangle - \|10\rangle \equiv \|\Phi^-\rangle$
10	$\|00\rangle - \|11\rangle \equiv \|\Psi^-\rangle$
11	$\|01\rangle + \|10\rangle \equiv \|\Phi^+\rangle$

Table 1: Quantum "truth table" for EPR circuit. The $\sqrt{2}$ normalization in the output states is supressed for clarity.

study entanglement of qubits.

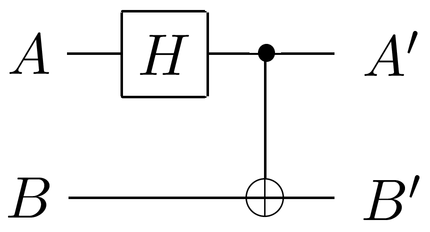


Figure 6: Quantum circuit to create EPR pairs

2.3 Example: Teleportation

In 1993, Bennett, Brassard, Crepau, Jozsa, Peres, and W. Wootters reported a new discovery[BBC+93]: a theoretical technique by which an unknown quantum state can be transmitted using only a few bits of classical information. This ability to perform "quantum teleportation" comes about because of the properties of entanglement between quantum states. The following scenario describes how it works. Alice and Bob met once long ago, but now live far apart. While they were together, they generated an EPR pair, and each took one qubit away. Now, many years later, Bob is in hiding, and Alice needs to deliver a certain qubit $|\psi\rangle$ to him. She does not know its state, and moreover, is allowed to send only two *classical* bits of information to Bob. How can she do this?

Here is the solution in brief: Alice will interact $|\psi\rangle$ with her half of the EPR pair, and then measure the two qubits. She will obtain one of four possible classical results, 00, 01, 10, and 11, and send this information to Bob. Depending on Alice's result, Bob will perform one of four operations on his half of the EPR pair, and thus obtain $|\psi\rangle$. This happens because of the entanglement provided by the EPR pair.

The quantum circuit shown in Fig. 7 implements this teleportation scheme. The input state $|\psi_0\rangle$ is

$$|\psi_0\rangle = (\alpha|0\rangle + \beta|1\rangle)|\Phi^+\rangle \tag{17}$$

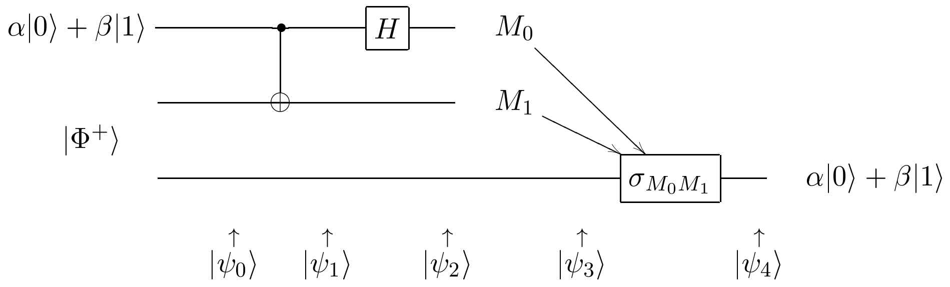


Figure 7: Quantum circuit for teleporting a qubit

$$= \frac{1}{\sqrt{2}}\Big[\alpha|0\rangle(|00\rangle + |11\rangle) + \beta|1\rangle(|00\rangle + |11\rangle)\Big] . \tag{18}$$

Note how the least-significant bit (the rightmost one) belongs to Bob, and the two others to Alice. Alice sends her bits through a CNOT gate, obtaining

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}\Big[\alpha|0\rangle(|00\rangle + |11\rangle) + \beta|1\rangle(|10\rangle + |01\rangle)\Big] . \tag{19}$$

She then sends the first qubit through a Hadamard trasnform, to get

$$|\psi_2\rangle = \frac{1}{2}\Big[\alpha(|0\rangle + |1\rangle)(|00\rangle + |11\rangle) + \beta(|0\rangle - |1\rangle)(|10\rangle + |01\rangle)\Big] . \tag{20}$$

This state may be re-written in the following way, simply by regrouping terms:

$$|\psi_2\rangle = \frac{1}{2}\Big[|00\rangle(\alpha|0\rangle + \beta|1\rangle) + |01\rangle(\alpha|1\rangle + \beta|0\rangle) + |10\rangle(\alpha|0\rangle - \beta|1\rangle) + |11\rangle(\alpha|1\rangle - \beta|0\rangle)\Big] . \tag{21}$$

Alice then measures her two qubits, obtaining four possible results, and their corresponding post-measurement states,

$$00 \longmapsto |\psi_3(00)\rangle = \frac{1}{\sqrt{2}}\Big[\alpha|0\rangle + \beta|1\rangle\Big] \tag{22}$$

$$01 \longmapsto |\psi_3(01)\rangle = \frac{1}{\sqrt{2}}\Big[\alpha|1\rangle + \beta|0\rangle\Big] \tag{23}$$

$$10 \longmapsto |\psi_3(10)\rangle = \frac{1}{\sqrt{2}}\Big[\alpha|0\rangle - \beta|1\rangle\Big] \tag{24}$$

$$11 \longmapsto |\psi_3(11)\rangle = \frac{1}{\sqrt{2}}\Big[\alpha|1\rangle - \beta|0\rangle\Big] . \tag{25}$$

Bob's qubit thus collapses into four possible states – and when he receives the two classical bits Alice sends him, Bob will know what has happened, and can apply the appropriate transform

$\sigma_{M_0 M_1}$ to fix his qubit, and obtain the final output state

$$|\psi_4\rangle = \alpha|0\rangle + \beta|1\rangle \,, \tag{26}$$

which, as desired, is the unknown qubit that Alice wanted to send.

3 Summary

We have learned that qubits admit many more interesting logic gates than do classical bits. In particular, because of the richness of possible single qubit transforms, the quantum analog of the XOR gate, the controlled-NOT gate, together with arbitrary single qubit operawtions forms a universal set of gates. That is, any transformation on a quantum state vector can be accomplished by cascading these gates. Furthermore, although any classical function can be implemented with quantum bits, a much wider variety of transforms is also possible. That will be explored next time.

References

[BBC+93] C. H. Bennett, G. Brassard, C. Crepau, R. Jozsa, A. Peres, and W. Wootters. Teleporting and unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Phys. Rev. Lett.*, 70(13):1895, 1993.

[BBC+95] A. Barenco, C. Bennett, R. Cleve, D. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. Smolin, and H. Weinfurter. Elementary gates for quantum computation. *Phys. Rev. A*, 52:3457, 1995.

[BCF+96] H. Barnum, C. M. Caves, C. A. Fuchs, R. Jozsa, and B. Schumacher. Noncommuting mixed states cannot be broadcast. *Phys. Rev. Lett.*, 76(15):2828–21, 1996.

[Ben82] Paul A. Benioff. Quantum mechanical hamiltonian models of discrete processes that erase their own histories: Application to Turing machines. *Int. J. of Theor. Physics*, 21(3/4):177, 1982.

[Die82] D. Dieks. *Phys. Letters*, A92:271, 1982.

[FT82] Edward Fredkin and Tommaso Toffoli. Conservative logic. *Int. J. of Theor. Physics*, 21(3/4):219, 1982.

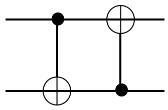
[Per85] Asher Peres. Reversible logic and quantum computers. *Phys. Rev. A*, 32(6):3266, 1985.

[Per93] A. Peres. *Quantum Theory: Concepts and Methods.* Kluwer Academic, Dordrecht, 1993.

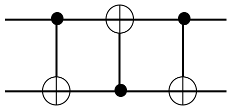
[WZ82] W. K. Wooters and W. H. Zurek. *Nature*, 299:802, 1982.

4 Problems

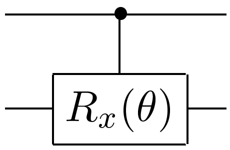
1. **Fun with controlled-NOT gates**: What does the following circuit do?



How about this one?



2. **Controlled-rotation gates**: This gate,



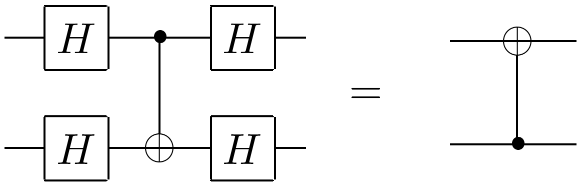
rotates the target (lower) qubit by $R_x(\theta)$ (angle θ about the $\hat{x}$ axis, if the control (upper) qubit is $|1\rangle$, otherwise it does nothing. The unitary transform can be written in matrix form as

$$\Lambda_1(R_x(\theta)) = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \cos\frac{\theta}{2} & i\sin\frac{\theta}{2} \\ 0 & 0 & i\sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{bmatrix} \tag{27}$$

Show how this gate can be implemented using two controlled-NOT gates and two single qubit rotations.

3. **Hadamard gates**: How can one construct a Hadamard gate, Eq.(3), from rotation gates $U_R(\theta)$, Eq.(4), and phase shift gates, $U_P(\phi_1, \phi_2)$, Eq.(5)?

4. **Basis transformations**: Unlike ideal classical gates, ideal quantum gates do not have high-impedance inputs. In fact, the role of "control" and "target" are arbitrary – they depend on what basis you think of a device as operating in. We have given the truth table for a CNOT and shown how the control qubit does not get changed in the classical 00, 01, 10, 11 basis. However, in reality, the control qubit *does* change: its phase is flipped depending on the state of the "target" qubit! Show that



5. **Pauli Matrices**: The Pauli matrices σ_x, σ_y, and σ_z are very important in the mathematics of quantum computation, because they are generators for the group of single-qubit transformations. Mathematically, this is the $SU(2)$ group, of 2×2 complex unitary matrices (those for which $(M^T)^* \equiv M^\dagger = M^{-1}$) with determinant $+1$, which describe solid body rotations in three dimensions.

   a. Using

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \tag{28}$$

$$\sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \tag{29}$$

$$\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \tag{30}$$

   and recalling that

$$e^{i\lambda M} = \sum_k \frac{(i\lambda)^k}{k!} M^k \tag{31}$$

   show that

$$R_x(2\theta) \equiv e^{i\theta\sigma_x} = \begin{pmatrix} \cos\theta & i\sin\theta \\ i\sin\theta & \cos\theta \end{pmatrix} \tag{32}$$

$$R_y(2\theta) \equiv e^{i\theta\sigma_y} = \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix} \tag{33}$$

$$R_z(2\theta) \equiv e^{i\theta\sigma_z} = \begin{pmatrix} \cos\theta + i\sin\theta & 0 \\ 0 & \cos\theta - i\sin\theta \end{pmatrix} \tag{34}$$

   It is useful to note that $\sigma_i^2 = I$, the identity matrix.

   b. Suppose you want $R_z(\theta)$, but only have gates which perform $R_x(\pi/2)$ and $R_y(\theta)$. Show how to compose these gates to accomplish the desired rotation.

   c. The Pauli matrices have wonderful commutation properties which are important in their role as the generators of $SU(2)$. Show that

$$\sigma_x\sigma_y - \sigma_y\sigma_x = 2i\sigma_z \tag{35}$$

$$\begin{aligned} \sigma_y\sigma_z - \sigma_z\sigma_y &= 2i\sigma_x \quad (36)\\ \sigma_z\sigma_x - \sigma_x\sigma_z &= 2i\sigma_y\,. \quad (37) \end{aligned}$$

Also show that

$$\sigma_i\sigma_j + \sigma_j\sigma_i = 0\,, \quad (38)$$

for $i \neq j$. These *commutation* and *anti-commutation* relations are fundamental to the Lie Algebra for $SU(2)$. They are often written concisely as

$$\begin{aligned} [\sigma_i, \sigma_j] &= 2i\epsilon_{ijk}\sigma_k \quad (39)\\ \{\sigma_i, \sigma_j\} &= 2\delta_{ij}I\,, \quad (40) \end{aligned}$$

where ϵ_{ijk} is a totally antisymmetric pseudovector known as the Levi-Civita symbol.

6. **The Bloch sphere**: The state of a qubit can be visualized as being a point on the unit sphere in three dimensions. Specifically, any qubit can be expressed as

$$\cos\frac{\theta}{2}\,|0\rangle + e^{i\phi}\sin\frac{\theta}{2}\,|1\rangle\,, \quad (41)$$

where θ and ϕ are the angle subtended from the $\hat{z}$ axis and the angle in the $\hat{x} - \hat{y}$ plane from the $\hat{x}$ axis – the usual spherical coordinate system. The reason this identification is useful is because it provides an isomorphism between single qubit operations, $U(2)$ and solid body rotations, $O(3)$. This can be understood from the following exercise.

a. Calculate the eigenvectors of σ_x, σ_y, and σ_z. These represent qubit states; what points do they correspond to on the unit sphere?

b. What does $R_x(\theta)$ do to the state $(|0\rangle + |1\rangle)/\sqrt{2}$?

*c. Show that $e^{i\vec{n}\cdot\vec{\sigma}/2}$, where $\vec{n}$ is a real three-dimensional vector, and $\vec{\sigma} = \sigma_x\hat{x}+\sigma_y\hat{y}+\sigma_z\hat{z}$, is a rotation about the vector $\hat{n} = \vec{n}/|\vec{n}|$, by the angle $|\vec{n}|$.

7. **Odd Angles**: Suppose you wish to perform a rotation $R_x(\alpha)$, where α is a given arbitrary angle, but you have only the single gate $R_x(\theta)$, where

$$\theta = \sum_k \frac{2\pi}{2^{2^k}}\,. \quad (42)$$

Show that by cascading $\mathcal{O}(n)$ of these gates, you can construct a rotation gate whose angle comes to within $\mathcal{O}(1/\mathrm{poly}(n))$ of α.