

# Basic Gates and QTeleport

Cody M. Grant

(Dated: February 11, 2022)

## I. SINGLE QUBIT GATES

For single qubit gates we have several to define. No proofs here, just definitions. Firstly, I should note that the way we can write single qubit states:

$$\text{if } |q\rangle = |0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \quad \text{or if } |q\rangle = |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \quad (1)$$

### 1. Outer-Product Gates

$$\begin{aligned} |0\rangle\langle 0| &\equiv \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} & |0\rangle\langle 1| &\equiv \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \\ |1\rangle\langle 0| &\equiv \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} & |1\rangle\langle 1| &\equiv \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \end{aligned} \quad (2)$$

Notice that

$$\begin{aligned} \langle y|x \rangle &= \begin{cases} 0, & \text{if } x \neq y \\ 1, & \text{if } x = y \end{cases} \\ &= \delta_{xy} \end{aligned} \quad (3)$$

### 2. $SU(2)$ Basis Gates (Pauli Gates + Identity)

$$X \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = |0\rangle\langle 1| + |1\rangle\langle 0| \quad (4)$$

$$Y \equiv \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} = -i|0\rangle\langle 1| + i|1\rangle\langle 0| \quad (5)$$

$$Z \equiv \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = |0\rangle\langle 0| - |1\rangle\langle 1| \quad (6)$$

$$I \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = |0\rangle\langle 0| + |1\rangle\langle 1| \quad (7)$$

Also note that  $X^2 = Y^2 = Z^2 = I$

### 3. Hadamard

$$H \equiv \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = \frac{1}{\sqrt{2}} (|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| - |1\rangle\langle 1|) \equiv \frac{1}{\sqrt{2}} (X + Z) \quad (8)$$

Also, useful to note that  $H^2 = I$ , and there is a useful relation with  $H$ ,  $X$ , and  $Z$ :

$$HZH = \frac{1}{\sqrt{2}}(X + Z)Z\frac{1}{\sqrt{2}}(X + Z) = \frac{XZX + XZZ + ZZX + ZZZ}{2} \quad (9)$$

where  $XZZ + ZZX = 2X$ ,  $ZZZ = Z$ , and

$$\begin{aligned} ZXZ &= (|0\rangle\langle 1| + |1\rangle\langle 0|)(|0\rangle\langle 0| - |1\rangle\langle 1|)(|0\rangle\langle 1| + |1\rangle\langle 0|) \\ &= (|1\rangle\langle 0| - |0\rangle\langle 1|)(|0\rangle\langle 1| + |1\rangle\langle 0|) \\ &= (|1\rangle\langle 1| - |0\rangle\langle 0|) \equiv -Z \end{aligned} \quad (10)$$

Therefore

$$HZH = \frac{-Z + 2X + Z}{2} = X \quad (11)$$

And the same can be said for the opposite:  $HXH = H(HZH)H = H^2ZH^2 = Z$ .

### 4. P-Gate (phase gate)

$$P(\phi) \equiv \begin{bmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{bmatrix} = |0\rangle\langle 0| + e^{i\phi}|1\rangle\langle 1| \quad (12)$$

Note that  $\phi$  is a real number, and for  $P(\phi = \pi) = Z$ . It can also be shown that  $|P|^2 = PP^\dagger = P^\dagger P = I$

There are also a couple other special  $P$ - gates at special values for  $\phi$

$$\begin{aligned} S &\equiv P\left(\phi = \frac{\pi}{2}\right) \equiv \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/2} \end{bmatrix} \\ T &\equiv P\left(\phi = \frac{\pi}{4}\right) \equiv \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix} \end{aligned} \quad (13)$$

And obviously  $T^2 = S$ . We can also show that

$$\begin{aligned} SXS^\dagger &= (|0\rangle\langle 0| + e^{i\pi/2}|1\rangle\langle 1|)(|0\rangle\langle 1| + |1\rangle\langle 0|)(|0\rangle\langle 0| + e^{-i\pi/2}|1\rangle\langle 1|) \\ &= (|0\rangle\langle 0| + i|1\rangle\langle 1|)(|0\rangle\langle 1| + |1\rangle\langle 0|)(|0\rangle\langle 0| + (-i)|1\rangle\langle 1|) \\ &= (|0\rangle\langle 1| + i|1\rangle\langle 0|)(|0\rangle\langle 0| + (-i)|1\rangle\langle 1|) \\ &= (-i)|0\rangle\langle 1| + i|1\rangle\langle 0| \equiv Y \end{aligned} \quad (14)$$

### 5. $U$ -Gate (general gate)

The most general single-qubit gate you can have is defined as

$$U(\theta, \phi, \lambda) \equiv \begin{bmatrix} \cos\left(\frac{\theta}{2}\right) & -e^{i\lambda} \sin\left(\frac{\theta}{2}\right) \\ e^{i\phi} \sin\left(\frac{\theta}{2}\right) & e^{i(\phi+\lambda)} \cos\left(\frac{\theta}{2}\right) \end{bmatrix} \quad (15)$$

For instance  $U(\pi/2, 0, \pi) = H$  and  $U(0, 0, \lambda) = P$ . All known single qubit gates are special cases of this  $U$ -gate. For instance  $U(\theta, 0, 0) \equiv R_y(\theta)$ . As it turns out,

$$\begin{aligned} R_y\left(-\frac{\pi}{4}\right) X R_y\left(\frac{\pi}{4}\right) &= \begin{bmatrix} \cos\left(-\frac{\pi}{8}\right) & -\sin\left(-\frac{\pi}{8}\right) \\ \sin\left(-\frac{\pi}{8}\right) & \cos\left(-\frac{\pi}{8}\right) \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} \cos\left(\frac{\pi}{8}\right) & -\sin\left(\frac{\pi}{8}\right) \\ \sin\left(\frac{\pi}{8}\right) & \cos\left(\frac{\pi}{8}\right) \end{bmatrix} \\ &= \begin{bmatrix} \cos\left(\frac{\pi}{8}\right) & \sin\left(\frac{\pi}{8}\right) \\ -\sin\left(\frac{\pi}{8}\right) & \cos\left(\frac{\pi}{8}\right) \end{bmatrix} \begin{bmatrix} \sin\left(\frac{\pi}{8}\right) & \cos\left(\frac{\pi}{8}\right) \\ \cos\left(\frac{\pi}{8}\right) & -\sin\left(\frac{\pi}{8}\right) \end{bmatrix} \\ &= \begin{bmatrix} 2\cos\left(\frac{\pi}{8}\right)\sin\left(\frac{\pi}{8}\right) & \cos^2\left(\frac{\pi}{8}\right) - \sin^2\left(\frac{\pi}{8}\right) \\ \cos^2\left(\frac{\pi}{8}\right) - \sin^2\left(\frac{\pi}{8}\right) & -2\cos\left(\frac{\pi}{8}\right)\sin\left(\frac{\pi}{8}\right) \end{bmatrix} \\ &= \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix} \equiv H \end{aligned} \quad (16)$$

## II. TWO QUBIT CONTROLLED GATES

For multiple qubits, for instance 2, you perform tensor multiplication on their states. So something like  $|q_1\rangle \otimes |q_0\rangle$ . 2-qubit controlled gates (like CNOT/CX, CY, CZ,etc.) usually mean that if the control qubit is 0, you do nothing to the target qubit. However, if the control qubit is 1, you apply the single qubit gate that is specified. In matrix form the control qubit is denoted by some of the matrices found in Eq. 3.

$$CX(0,1) = I \otimes |0\rangle\langle 0| + (\text{Gate}) \otimes |1\rangle\langle 1| \quad (17)$$

### 1. CNOT/CX

The most important or basic gate is the CNOT/CX gate where the control qubit is  $q_0$  and the target is  $q_1$ :

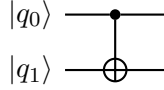


FIG. 1: CX (or CNOT) gate

and in math notation, that's

$$CX(0,1) = I \otimes |0\rangle\langle 0| + X \otimes |1\rangle\langle 1| \quad (18)$$

I personally like keeping the multi-qubit gates in this form because they take up less space and are easier to understand for me. Otherwise, all 2 qubit gates make a 4x4 matrix, and a 3 qubit gate makes 8x8 and you start taking up a lot of space for one thing.

For instance one could make a CZ gate from what we know about a CX gate and that  $HXH = Z$ .

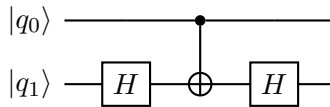


FIG. 2: CX (or CNOT) gate

and in math notation, that's

$$\begin{aligned}
CZ(0,1) &= (H \otimes I)CX(0,1)(H \otimes I) \\
&= (H \otimes I)(I \otimes |0\rangle\langle 0| + X \otimes |1\rangle\langle 1|)(H \otimes I) \\
&= (HI \otimes I|0\rangle\langle 0| + HX \otimes I|1\rangle\langle 1|)(H \otimes I) \\
&= (H I H \otimes I|0\rangle\langle 0| + H X H \otimes I|1\rangle\langle 1|) \\
&= (H^2 \otimes |0\rangle\langle 0| + H X H \otimes |1\rangle\langle 1|) \\
&= (I \otimes |0\rangle\langle 0| + Z \otimes |1\rangle\langle 1|)
\end{aligned} \tag{19}$$

which is what you would expect for the definition of  $CZ$ . We can use Eqn. 14 and Eqn. 16 to make a  $CY$  and  $CH$  gate, respectively. However, we could also just use their matrix definitions inside the basic 2-qubit control gate definition to complete the tasks as well. We mainly show this to state that  $CX$  is our most basic multi-qubit gate and will build all other gates off of it.

## 2. SWAP gate

Built of CX gates, we have the SWAP gate

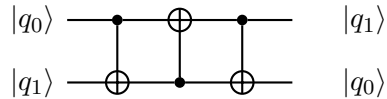


FIG. 3: SWAP Gate decomposed

Mathematically, we have

$$\begin{aligned}
SWAP &= (I \otimes |0\rangle\langle 0| + X \otimes |1\rangle\langle 1|)(|0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X)(I \otimes |0\rangle\langle 0| + X \otimes |1\rangle\langle 1|) \\
&= (I \otimes |0\rangle\langle 0| + X \otimes |1\rangle\langle 1|)(|0\rangle\langle 0| \otimes |0\rangle\langle 0| + |1\rangle\langle 1| \otimes |1\rangle\langle 0| + |0\rangle\langle 1| \otimes |1\rangle\langle 1| + |1\rangle\langle 0| \otimes |0\rangle\langle 1|) \\
&= (|0\rangle\langle 0| \otimes |0\rangle\langle 0| + |1\rangle\langle 0| \otimes |0\rangle\langle 1| + |0\rangle\langle 1| \otimes |1\rangle\langle 0| + |1\rangle\langle 1| \otimes |1\rangle\langle 1|)
\end{aligned} \tag{20}$$

which clearly shows the qubit's final state is the other qubit's initial state.

### III. TOFFOLI GATE

Our basic 3 qubit gate is called a Toffoli gate. You only perform an  $X$  gate on the target qubit as long as both control qubits are 1.

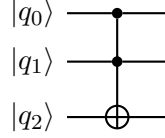


FIG. 4: CCX or Toffoli gate

or the mathematical expression

$$\begin{aligned}
 CCX(0, 1, 2) &= I \otimes |0\rangle\langle 0| \otimes |0\rangle\langle 0| + I \otimes |1\rangle\langle 1| \otimes |0\rangle\langle 0| + I \otimes |0\rangle\langle 0| \otimes |1\rangle\langle 1| + X \otimes |1\rangle\langle 1| \otimes |1\rangle\langle 1| \\
 &= I \otimes I \otimes |0\rangle\langle 0| + I \otimes |0\rangle\langle 0| \otimes |1\rangle\langle 1| + X \otimes |1\rangle\langle 1| \otimes |1\rangle\langle 1| \\
 &= I \otimes I \otimes |0\rangle\langle 0| + CX(1, 2) \otimes |1\rangle\langle 1|
 \end{aligned} \tag{21}$$

One way to make this gate out of 1- and 2-qubit gates is the following:

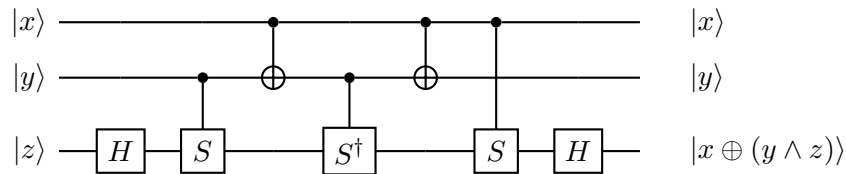


FIG. 5: Decomposition of the Toffoli gate

We can use the Toffoli gate to recreate some of the basic classical gates.

#### 1. Quantum AND gate

If the z-qubit is initially the  $|0\rangle$  state, then after the Toffoli, it'll be the "and" state of the x- and y-qubit:

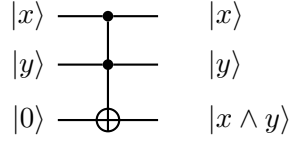


FIG. 6: Classical "And" gate using the Toffoli gate

If you look at the Toffoli gate and its effect on a 3-qubit state, where the  $z$  qubit is in the 0-state, you see that after the Toffoli gate the  $z$  qubit is in the 1-state only if both the  $x$  and  $y$  qubits were in the 1-state before the gate was applied, which is exactly what would happen with the classical AND gate

$$|0\rangle \otimes |y\rangle \otimes |x\rangle = |0yx\rangle = \begin{pmatrix} 000 \\ 001 \\ 010 \\ 011 \end{pmatrix} \xrightarrow{\text{qAND}} \begin{pmatrix} 000 \\ 001 \\ 010 \\ 111 \end{pmatrix} \quad (22)$$

## 2. Quantum OR gate

With the addition of a new single qubit NOT or X gates, and using a similiar process to before, the 3rd qubit becomes the "or" state of the  $x$ - and  $y$ -qubit:

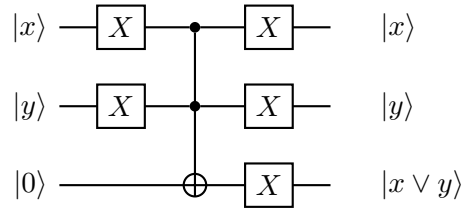


FIG. 7: Classical "Or" gate using the Toffoli gate



Finding the mathematical expression:

$$\begin{aligned}
(\text{OR}) &= (I \otimes X \otimes X) \\
&\times (I \otimes |0\rangle\langle 0| \otimes |0\rangle\langle 0| + I \otimes |1\rangle\langle 1| \otimes |0\rangle\langle 0| + I \otimes |0\rangle\langle 0| \otimes |1\rangle\langle 1| + X \otimes |1\rangle\langle 1| \otimes |1\rangle\langle 1|) \\
&\times (X \otimes X \otimes X) \\
&= (I \otimes |1\rangle\langle 0| \otimes |1\rangle\langle 0| + I \otimes |0\rangle\langle 1| \otimes |1\rangle\langle 0| + I \otimes |1\rangle\langle 0| \otimes |0\rangle\langle 1| + X \otimes |0\rangle\langle 1| \otimes |0\rangle\langle 1|) \\
&\times (X \otimes X \otimes X) \\
&= (X \otimes |1\rangle\langle 1| \otimes |1\rangle\langle 1| + X \otimes |0\rangle\langle 0| \otimes |1\rangle\langle 1| + X \otimes |1\rangle\langle 1| \otimes |0\rangle\langle 0| + I \otimes |0\rangle\langle 0| \otimes |0\rangle\langle 0|)
\end{aligned} \tag{23}$$

And applying this to 3 qubit state, where the  $z$  qubit initially is zero, the gate on this qubit acts just like the classical OR gate

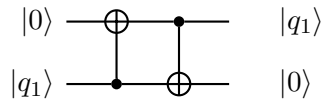
$$|0\rangle \otimes |y\rangle \otimes |x\rangle = |0yx\rangle = \begin{pmatrix} 000 \\ 001 \\ 010 \\ 011 \end{pmatrix} \xrightarrow{\text{qOR}} \begin{pmatrix} 000 \\ 101 \\ 110 \\ 111 \end{pmatrix} \tag{24}$$

#### IV. QUANTUM STATE TELEPORTATION

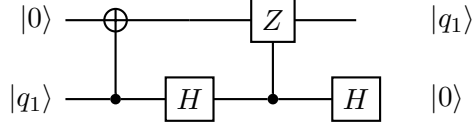
There are a couple "simple" 2-qubit state teleporation algorithms. They are called  $X$ -type and  $Z$ -type.

##### 1. $Z$ -type

Starting with the SWAP gate, if  $q_0$  is in the 0-state, then the first cnot does nothing, so we can simplify it slightly.



Then on the second  $CX$  gate, we can equivalently write  $X = HZH$ , and note that the  $CZ$  gate is the exact same whether the  $q_0$  is the target or control qubit, so we can write:



We only care about preserving the first qubit's final state, so before performing the last Hadamard gate on the second qubit, we will just measure it instead, resulting in

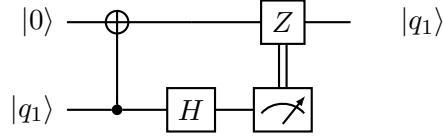
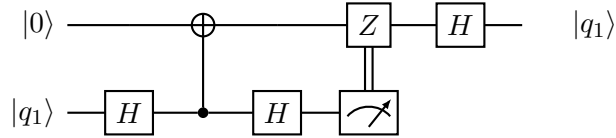


FIG. 8: Z-type quantum state teleportation

## 2. X-type

Starting from Z-type state teleporation circuit, if we state that  $|q_1\rangle = H|q'_1\rangle$ ,



From  $HZH = X$ , we can show that  $ZH = HX$ , altering the  $CZ$  gate. We can also move the Hadamard gate through the  $CX$  gate in a similar fashion  $XH = HZ$ . Finally  $H(CZ)H = CX$  and we arrive at

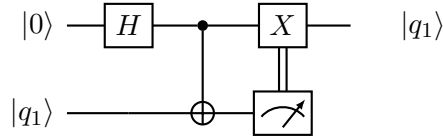


FIG. 9: X-type quantum state teleportation

### 3. Long-distance state teleportation

Needing both to have valid quantum state teleportation between alice and bob, naively we write:

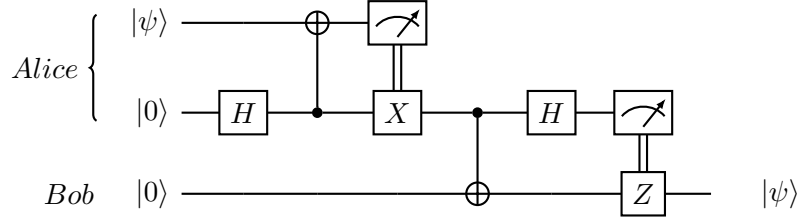
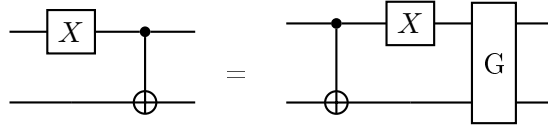


FIG. 10: Naive long-distance state teleportation

However, the last  $CX$  gate is not valid because the qubits from Bob and Alice have already been separated. If we can commute that  $CX$  gate to the front, and entangle those two states before separation, then that is valid. Looking at the following:



And we need to figure out what the mystery gate,  $G$ , is, mathematically

$$\begin{aligned}
 (I \otimes X)(CX(0,1)) &= (CX(0,1))(I \otimes X)(G) \\
 (I \otimes X)^\dagger(CX(0,1))^\dagger(I \otimes X)(CX(0,1)) &= G
 \end{aligned}
 \tag{25}$$

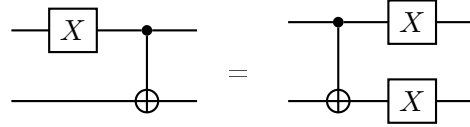
And it turns out that both  $(I \otimes X)^\dagger = (I \otimes X)$  and  $(CX(0,1))^\dagger = (CX(0,1))$ . So to find  $G$ , we first find

$$(I \otimes X)(CX(0,1)) = (I \otimes X)(I \otimes |0\rangle\langle 0| + X \otimes |1\rangle\langle 1|) = (I \otimes |1\rangle\langle 0| + X \otimes |0\rangle\langle 1|)$$

then simply

$$\begin{aligned}
(I \otimes X)(CX(0, 1))(I \otimes X)(CX(0, 1)) &= (I \otimes |1\rangle \langle 0| + X \otimes |0\rangle \langle 1|)(I \otimes |1\rangle \langle 0| + X \otimes |0\rangle \langle 1|) \\
&= (X \otimes |0\rangle \langle 0| + X \otimes |1\rangle \langle 1|) = (X \otimes I)
\end{aligned} \tag{26}$$

This means



Meaning that we can prepare an entangled state at the beginning with the single Hadamard gate and the first  $CX$  gate, then separate the qubits. Afterwards, Alice only needs to send Bob the two classical bits to see if he has to apply the  $X$  and  $Z$  gate to his qubit to find the same state.

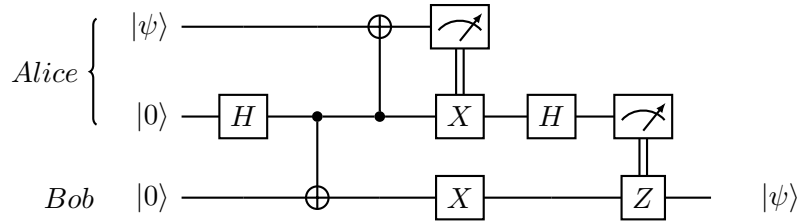


FIG. 11: Valid long-distance state teleportation

Something similar can be done by implementing the X-type switch on Alice's qubits, then a Z-type on the entangled states. The only change is, the  $G$  gate in that case is something a little different since you're commuting a  $CX$  through a  $Z$  gate (rather than an  $X$  gate like we did in the above example).

---