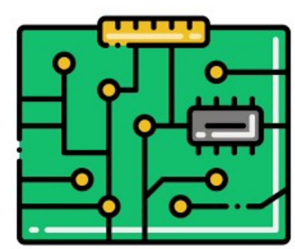
Quantum...

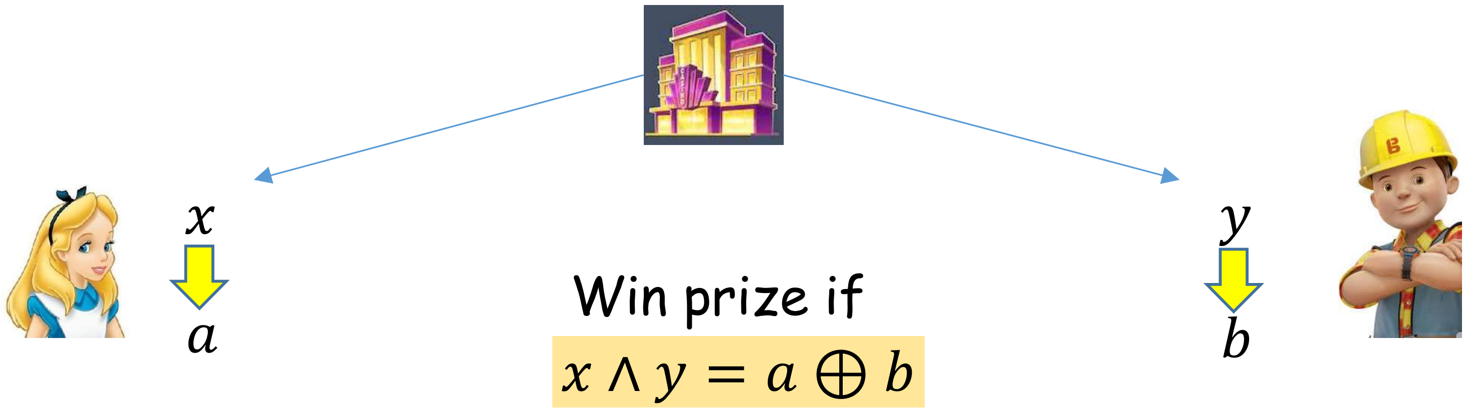
Computing

God, Gates and Circuits




HOW'S YOUR QUANTUM COMPUTER PROTOTYPE COMING ALONG?
GREAT!
Dilbert.com DilbertCartoonist@gmail.com
THE PROJECT EXISTS IN A SIMULTANEOUS STATE OF BEING BOTH TOTALLY SUCCESSFUL AND NOT EVEN STARTED.
4-17-12 ©2012 Scott Adams, Inc./Dist. by Universal Uclick
CAN I OBSERVE IT?
THAT'S A TRICKY QUESTION.

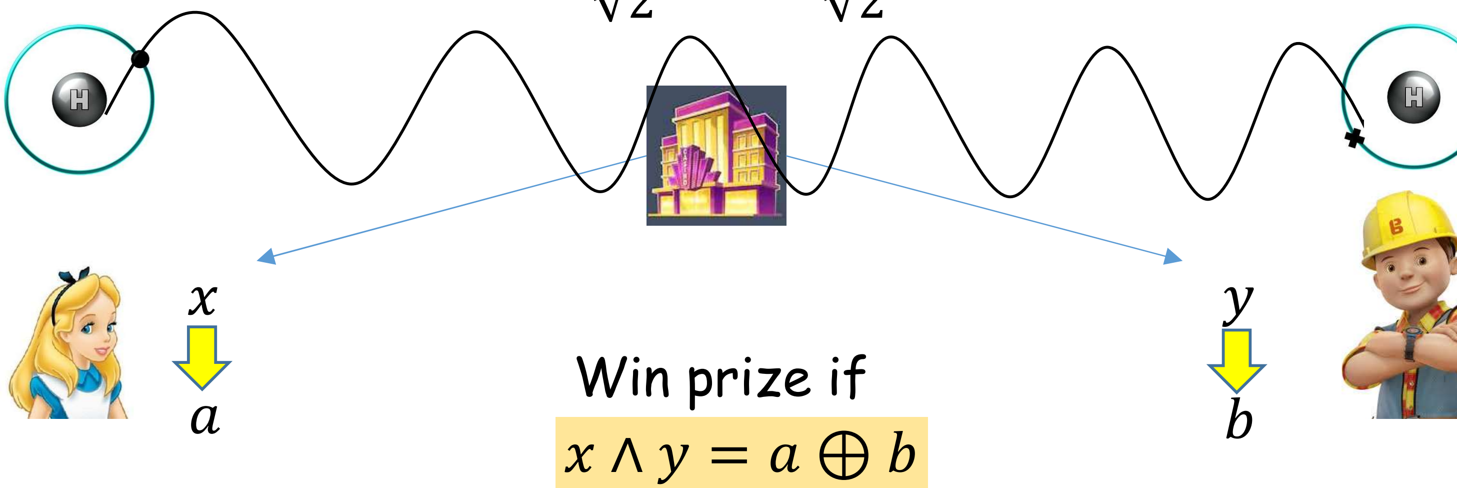
The CHSH game



- Alice and Bob live in separate cities and may not communicate
- The casino sends each of them a random bit
  - Need not be identical
- They must inspect their bit and output a value
  - Alice outputs a, Bob outputs b
- They get a prize of \$1.00 if:
  - Both got “1” from the casino and their outputs are such that $a \neq b$
  - Any other condition ([0,1], [1,0], [0,0]) they must output $a == b$
- What is the best strategy, and what is their expected earning?

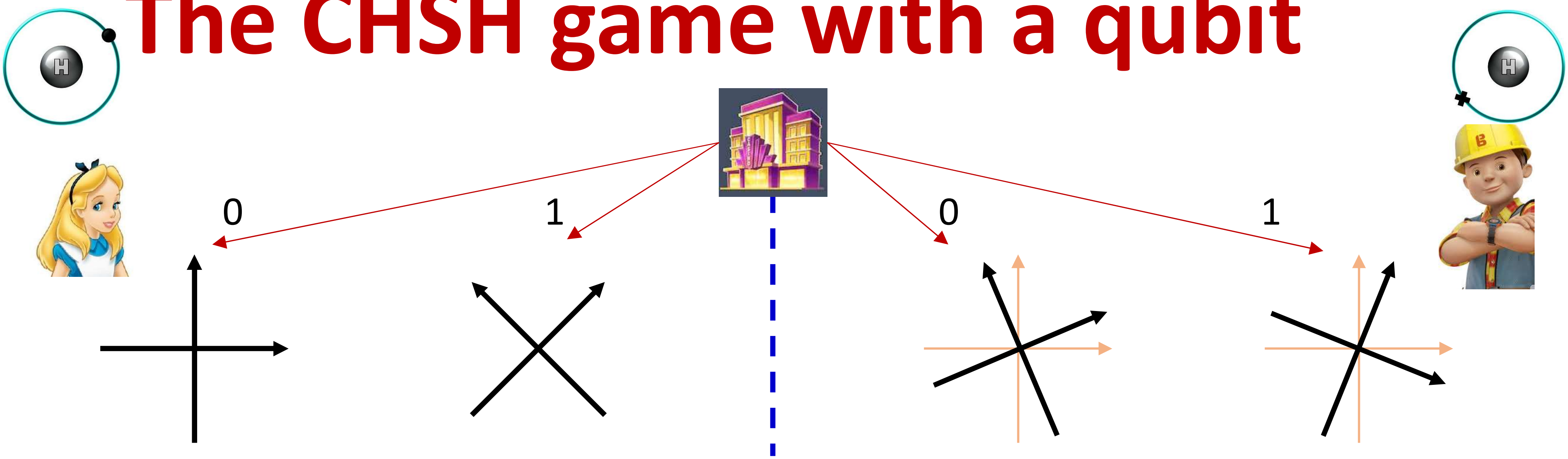
The CHSH game with a qubit

$$|\psi\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$$



- Before moving to separate cities, Alice and Bob split a pair of entangled bits in the Bell State
- Now what is their best strategy?

The CHSH game with a qubit



- Alice uses two sets of bases for measurement: 0/1 and +/- (at 45°)
  - If Alice gets a 0 from the casino she measures using 0/1 and outputs the value
  - Else she measures using +/- and outputs the value
- Bob uses two sets of bases: at $\left[\frac{\pi}{8}, \frac{5\pi}{8}\right]$ and $\left[\frac{-\pi}{8}, \frac{3\pi}{8}\right]$
  - If Bob gets a 0 from the casino, he measures using $\left[\frac{\pi}{8}, \frac{5\pi}{8}\right]$ and outputs the value
  - Else he measures using the $\left[\frac{-\pi}{8}, \frac{3\pi}{8}\right]$ and outputs the value

The CHSH inequality

- The Clauser Horne Shimony Holt (1969):
- For classical computers

$$E[0,0] + E[0,1] + E[1,0] - E[1,1] \leq 2$$

  - where $E[x, y]$ is the probability that Alice and Bob "agree" (i.e. $a = b$) when they receive x and y respectively
    - Note: The maximum possible value under perfect knowledge is 3. The closer you are to 3, the more money you make
- Using quantum entanglement

$$E[0,0] + E[0,1] + E[1,0] - E[1,1] \leq 2\sqrt{2}$$

  - Regardless of the actual qubit shared
  - Over any policy / measurement strategy
  - This is 2.8, which is very close to the max possible value of 3
- Qubits, which are useless for communication, can still be used to create *correlations* which can be exploited
  - They can "enhance" asymmetries in the system

Lesson – you cannot communicate

- But you can correlate

- And correlation can be used for profit…

The Determinism Conundrum

- Schroedingers equation

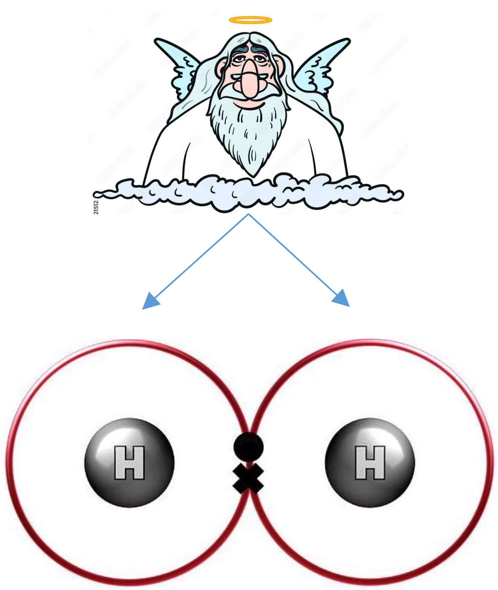
$$i\hbar \frac{\partial}{\partial t} \Psi(\boldsymbol{x}, t) = \left[-\frac{\hbar^2}{2m} \nabla^2 + V(\boldsymbol{x}, t) \right] \Psi(\boldsymbol{x}, t)$$

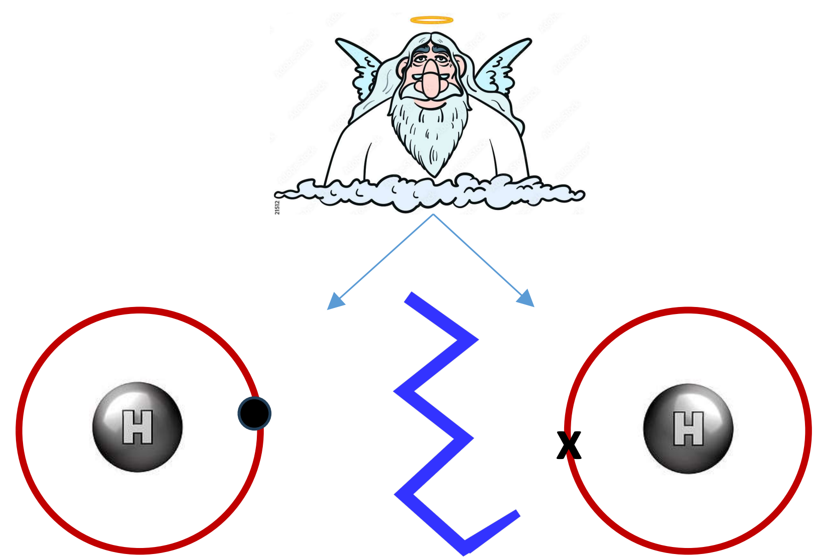
- The term in the square brackets is the *Hamiltonian.*
    - It includes a *potential* term $V(\boldsymbol{x}, t)$ which can be manipulated to manipulate the Hamiltonian itself
- ∇^2 is the *Laplacian*
- $\boldsymbol{x}$ is 3D position
- $\Psi(\boldsymbol{x}, t)$ is the wave function for a particle

Is there a Higher Knower?

- $\Psi(x, t)$, when measured, collapses into one of the many possible states
- *Was this state fore-ordained?*

- Einsten, Podelsky and Rosen (EPR) – yes!
  - ***Local realism:*** The fate of one qubit cannot affect another faster than light
  - Ergo: The "entangled" qubits were *foreordained* to their state by some (possibly ancient) latent variable. There is no "entanglement" per-se…





Is there a Higher Knower?

- $\Psi(x, t)$, when measured, collapses into one of the many possible states
- *Was this state fore-ordained?*
- The CHSH game uses entangled qubits to prove otherwise
  - Einstein, Podolsky, Rosen: The two cubits were independently fore-ordained by a common cause to fall the same way
  - Bell: If so, their individual measurements (and their bases) should not have any influence on the other if they are randomly chosen
    - P(match) <= 0.75
  - P = 0.85 implies actual entanglement, and genuine randomness in measurement

What does the higher-knower know?

- The *probability distribution in* $\Psi(\boldsymbol{x}, t)$ may be known for all x at some t.

- But

$$i\hbar \frac{\partial}{\partial t}\Psi(\boldsymbol{x}, t) = \left[-\frac{\hbar^2}{2m}\nabla^2 + V(\boldsymbol{x}, t)\right]\Psi(\boldsymbol{x}, t)$$

- This is solveable.

- If $\Psi(\boldsymbol{x}, t)$ is known at any time it is known for all time!!!
  - The wavefunction is fully determined for all time
  - The universe is deterministic in probability

Quantum gates

$$|\varphi\rangle = U|\psi\rangle$$

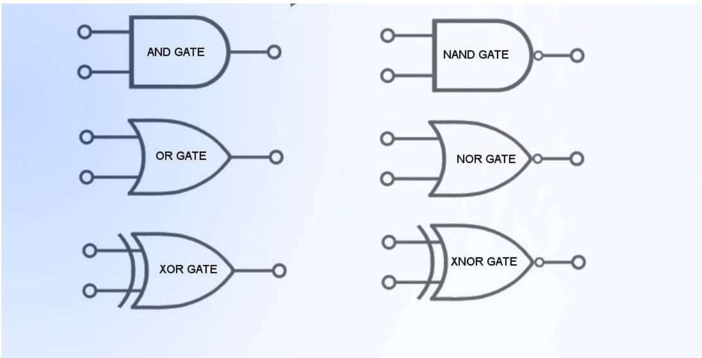
$$|\psi\rangle = \begin{bmatrix} a_0 \\ \vdots \\ a_N \end{bmatrix} \qquad |\varphi\rangle = \begin{bmatrix} b_0 \\ \vdots \\ b_N \end{bmatrix}$$

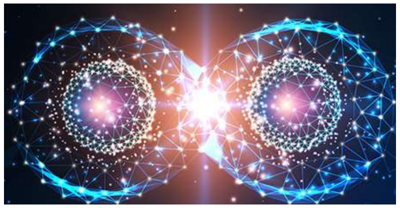
$$\begin{bmatrix} b_0 \\ \vdots \\ b_N \end{bmatrix} = U \begin{bmatrix} a_0 \\ \vdots \\ a_N \end{bmatrix}$$

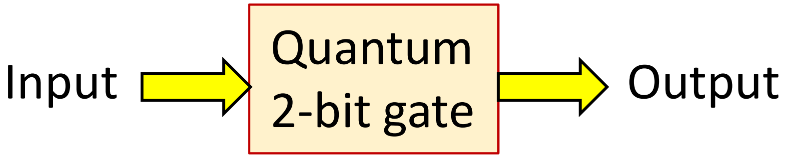
- Operate on N-Dimensional phasors
  - In a complex N-D complex Hilbert space
  - The input is an N-D phasor, the output too is an N-D phasor
- The “gate” is itself a transform
  - **A *unitary* transform**
- So how many inputs does the gate have, and how many outputs?

TWO QUBIT GATES

Classical two-bit gates







- Two-bit classical gates take in 2 bits, and output one or two bits
  - They operate on a two-dimensional input space
- What dimensionality of space do two-qubit quantum gates operate on

TWO QUBIT GATES

$$|\psi\rangle = a_{00}|00\rangle + a_{01}|01\rangle + a_{10}|10\rangle + a_{11}|11\rangle \rightarrow \boxed{\begin{array}{c}\text{Quantum}\\ \text{2-bit gate}\end{array}} \rightarrow |\varphi\rangle = b_{00}|00\rangle + b_{01}|01\rangle + b_{10}|10\rangle + b_{11}|11\rangle$$

$$\begin{array}{c} \text{qubit} \rightarrow \\ \text{qubit} \rightarrow \end{array} \boxed{\begin{array}{c}\text{Quantum}\\ \text{2-bit gate}\end{array}} \begin{array}{c} \rightarrow \text{qubit} \\ \rightarrow \text{qubit} \end{array}$$

- Two-bit classical gates take in 2 bits, and output one or two bits
  - They operate on a two-dimensional input space
- What dimensionality of space do two-qubit quantum gates operate on
  - Four dimensional inputs and outputs
  - But physically still represented by two qubits (thanks quantum!)

Two-qubit gates

$$|\psi\rangle = a_{00}|00\rangle + a_{01}|01\rangle + a_{10}|10\rangle + a_{11}|11\rangle \rightarrow \boxed{\begin{array}{c}\text{Quantum}\\ \text{2-bit gate}\end{array}} \rightarrow |\varphi\rangle = b_{00}|00\rangle + b_{01}|01\rangle + b_{10}|10\rangle + b_{11}|11\rangle$$

$$U$$

$$\begin{bmatrix} b_{00} \\ b_{01} \\ b_{10} \\ b_{11} \end{bmatrix} = \begin{bmatrix} u_{00} & u_{01} & u_{02} & u_{03} \\ u_{10} & u_{11} & u_{12} & u_{13} \\ u_{20} & u_{21} & u_{22} & u_{23} \\ u_{30} & u_{31} & u_{23} & u_{33} \end{bmatrix} \begin{bmatrix} a_{00} \\ a_{01} \\ a_{10} \\ a_{11} \end{bmatrix}$$

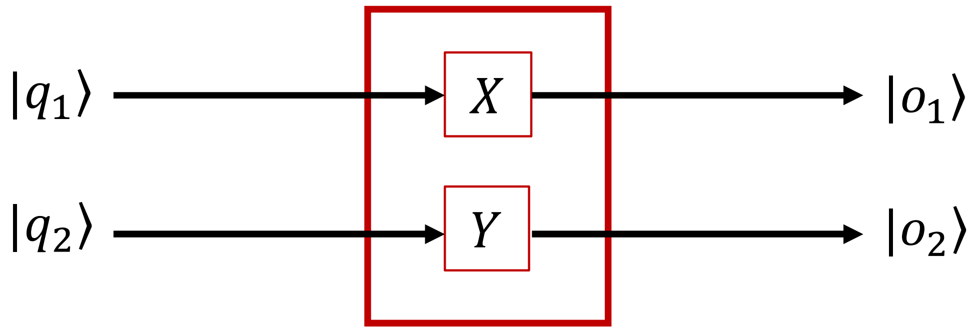
- A single two-qubit gate U operates on the phasor

  $a_{00}|00\rangle + a_{01}|01\rangle + a_{10}|10\rangle + a_{11}|11\rangle$ to output $b_{00}|00\rangle + b_{01}|01\rangle + b_{10}|10\rangle + b_{11}|11\rangle$

  $$U(a_{00}|00\rangle + a_{01}|01\rangle + a_{10}|10\rangle + a_{11}|11\rangle) = b_{00}|00\rangle + b_{01}|01\rangle + b_{10}|10\rangle + b_{11}|11\rangle$$

- U is is a 4x4 matrix.
  - It is a unitary transform
  - Its columns are orthogonal and form a new basis set
- Examples coming up

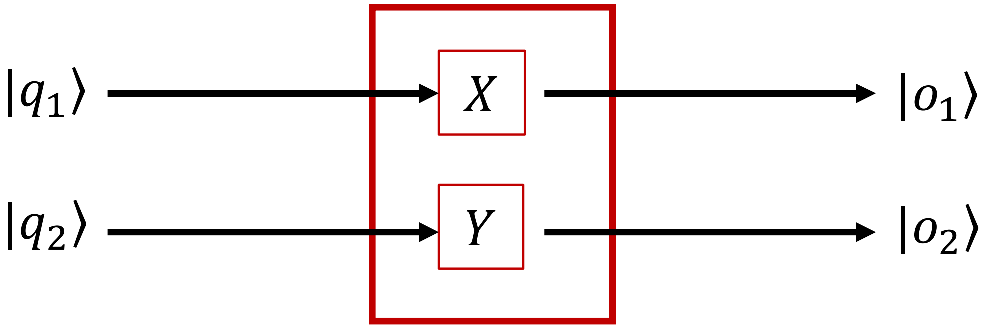
The simplest 2-qubit gate

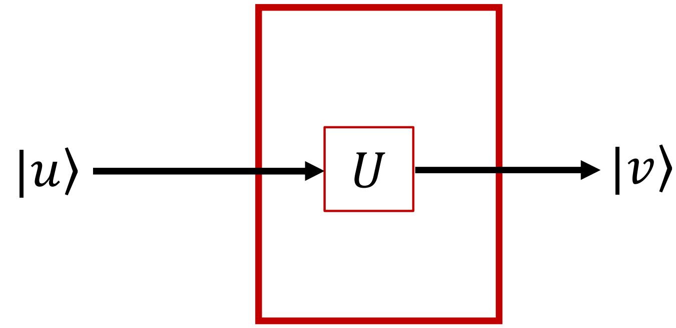


- Each qubit is independently operated on by a one-qubit gate
  - Note: This is still a two qubit system operating on two qubits and producing two qubits

- What is the resulting 2-qubit gate?

2-qubit gate





$|q_1\rangle = a_0|0\rangle + a_1|1\rangle$ $\qquad$ $|o_1\rangle = c_0|0\rangle + c_1|1\rangle$

$|q_2\rangle = b_0|0\rangle + c_1|1\rangle$ $\qquad$ $|o_2\rangle = d_0|0\rangle + d_1|1\rangle$

$|u\rangle = |q_1\rangle \otimes |q_2\rangle = |q_1 q_2\rangle$

$|v\rangle = |o_1\rangle \otimes |o_2\rangle = |o_1 o_2\rangle$

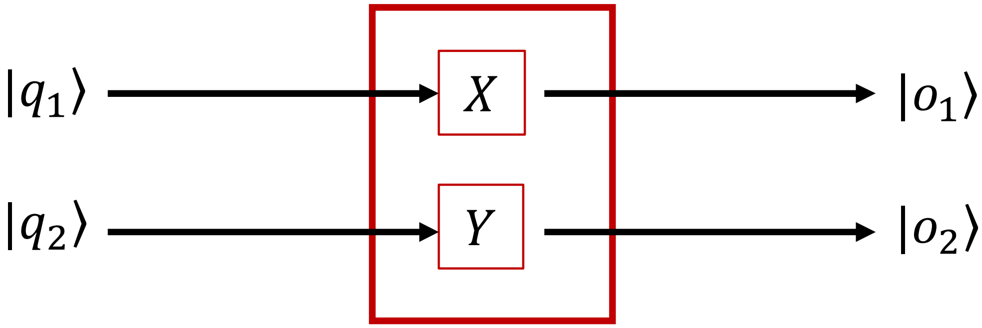
$$\begin{bmatrix} c_0 \\ c_1 \end{bmatrix} = \begin{bmatrix} x_{00} & x_{01} \\ x_{10} & x_{11} \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \end{bmatrix}$$

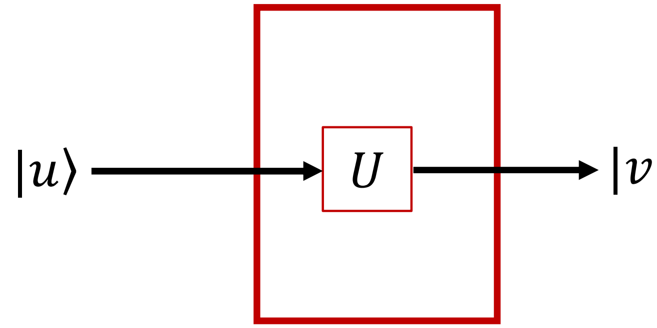
$$\begin{bmatrix} d_0 \\ d_1 \end{bmatrix} = \begin{bmatrix} y_{00} & y_{01} \\ y_{10} & y_{11} \end{bmatrix} \begin{bmatrix} d_0 \\ d_1 \end{bmatrix}$$

$$\begin{bmatrix} v_{00} \\ v_{01} \\ v_{10} \\ v_{11} \end{bmatrix} = \begin{bmatrix} u_{00} & u_{01} & u_{02} & u_{03} \\ u_{10} & u_{11} & u_{12} & u_{13} \\ u_{20} & u_{21} & u_{22} & u_{23} \\ u_{30} & u_{31} & u_{23} & u_{33} \end{bmatrix} \begin{bmatrix} u_{00} \\ u_{01} \\ u_{10} \\ u_{11} \end{bmatrix}$$

- How does U relate to X and Y

2-qubit gate





$$X = \begin{bmatrix} x_{00} & x_{01} \\ x_{10} & x_{11} \end{bmatrix}$$

$$Y = \begin{bmatrix} y_{00} & y_{01} \\ y_{10} & y_{11} \end{bmatrix}$$

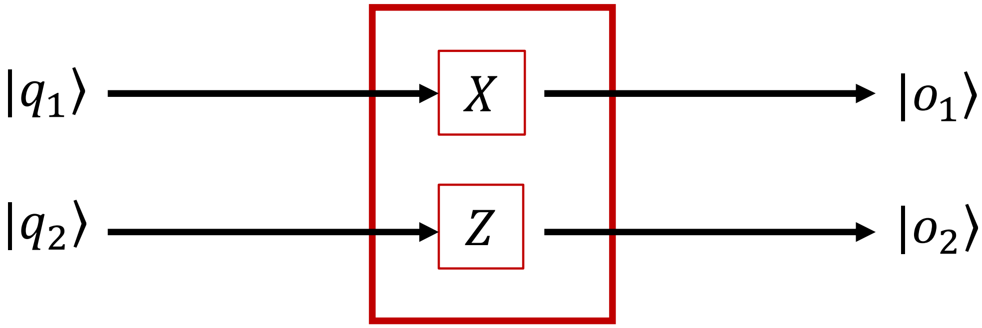
$$U = X \otimes Y$$

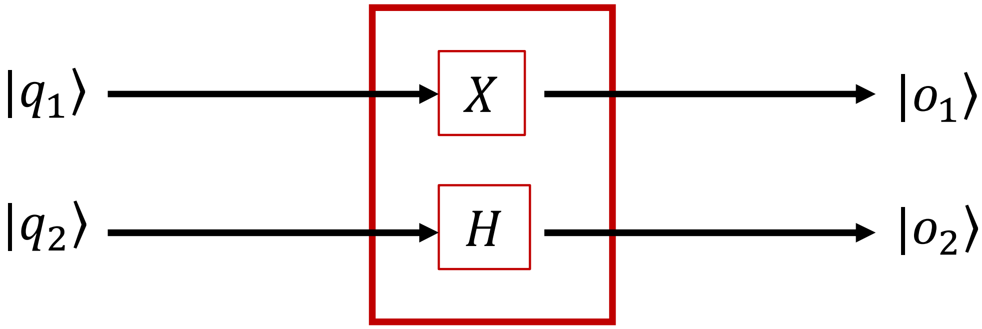
$$U = X \otimes Y = \begin{bmatrix} x_{00} \begin{bmatrix} y_{00} & y_{01} \\ y_{10} & y_{11} \end{bmatrix} & x_{01} \begin{bmatrix} y_{00} & y_{01} \\ y_{10} & y_{11} \end{bmatrix} \\ x_{10} \begin{bmatrix} y_{00} & y_{01} \\ y_{10} & y_{11} \end{bmatrix} & x_{11} \begin{bmatrix} y_{00} & y_{01} \\ y_{10} & y_{11} \end{bmatrix} \end{bmatrix}$$

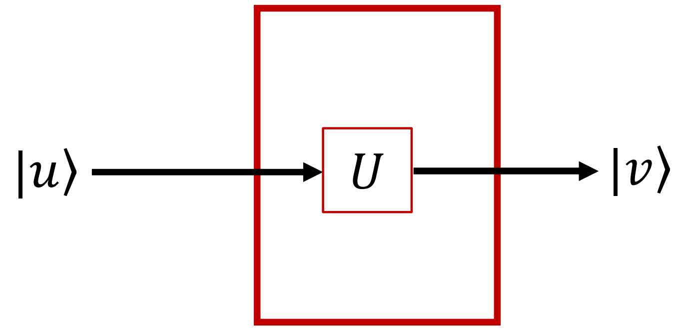
- How does U relate to X and Y *when the qubits don't interact*
  - I.e. no entanglement
  - Verify that U is unitary

$$U = \begin{bmatrix} x_{00}y_{00} & x_{00}y_{01} & x_{01}y_{00} & x_{01}y_{01} \\ x_{00}y_{10} & x_{00}y_{11} & x_{01}y_{10} & x_{01}y_{11} \\ x_{10}y_{00} & x_{10}y_{01} & x_{11}y_{00} & x_{11}y_{01} \\ x_{10}y_{10} & x_{10}y_{11} & x_{11}y_{10} & x_{11}y_{11} \end{bmatrix}$$

2-qubit gate

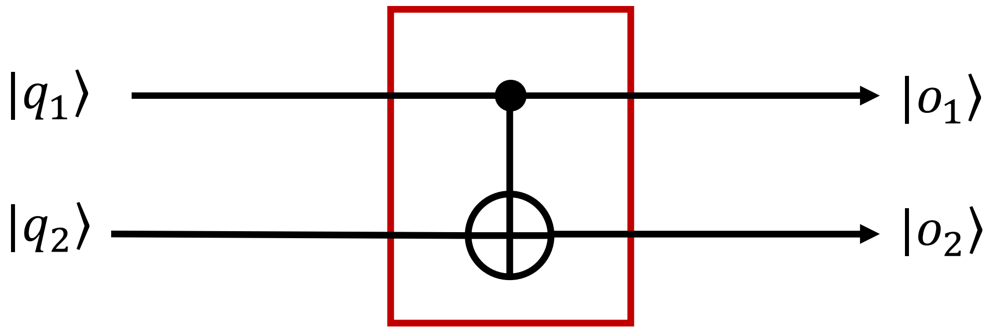






- What is U?
- What is the structure of the transform?
  - Can you generalize to more than 2 non-interacting bits?

The CNOT gate

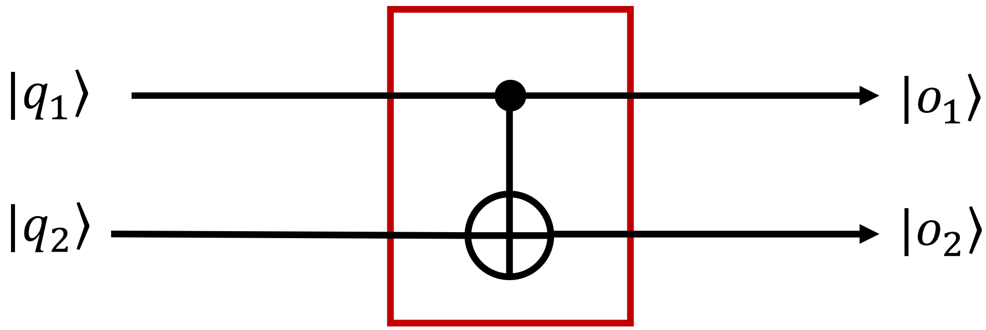


$$|o_1 o_2\rangle = CNOT(|q_1 q_2\rangle)$$

$$o_1 = q_1 \qquad\qquad o_2 = q_1 \oplus q_2$$

- $o_1 = q_1$
  - The first input is always unchanged
- $o_2 = q_2$ if $q_1 = |0\rangle$ (is 0), otherwise $o_2 = X(q_2)$
  - It bit-flips if the first input is 1
- **q_1 is the *control* bit and q_2 is the *target* bit**

The CNOT gate



$|o_1 o_2\rangle = CNOT(|q_1 q_2\rangle)$

$$\begin{bmatrix} u_{00} \\ u_{01} \\ u_{11} \\ u_{10} \end{bmatrix} = [CNOT] \begin{bmatrix} u_{00} \\ u_{01} \\ u_{10} \\ u_{11} \end{bmatrix}$$

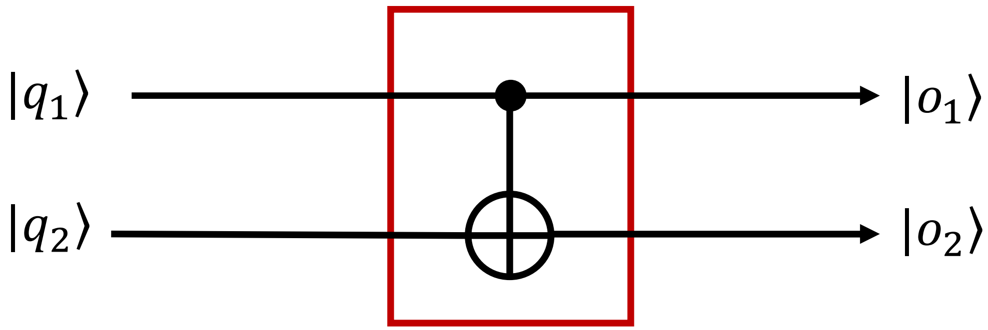
$$CNOT = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

Verify that this is unitary

$$CNOT(a_{00}|00\rangle + a_{01}|01\rangle + a_{10}|10\rangle + a_{11}|11\rangle) = a_{00}\,|00\rangle + a_{01}|01\rangle + a_{11}|10\rangle + a_{10}|11\rangle$$

- **Are o_1 and o_2 entangled?**

The CNOT gate



$$|o_1 o_2\rangle = CNOT(|q_1 q_2\rangle)$$

$$\begin{bmatrix} u_{00} \\ u_{01} \\ u_{11} \\ u_{10} \end{bmatrix} = [CNOT] \begin{bmatrix} u_{00} \\ u_{01} \\ u_{10} \\ u_{11} \end{bmatrix}$$

$$CNOT = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

$$CNOT(a_{00}|00\rangle + a_{01}|01\rangle + a_{10}|10\rangle + a_{11}|11\rangle) = a_{00}\,|00\rangle + a_{01}|01\rangle + a_{11}|10\rangle + a_{10}|11\rangle$$

- **Are o_1 and o_2 entangled?**

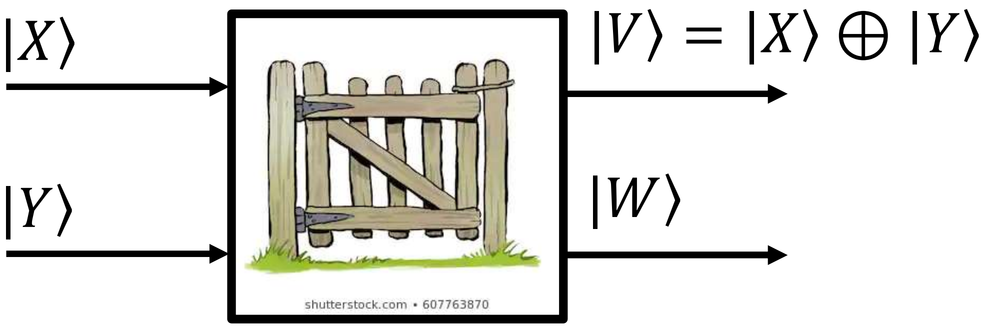
CNOT IS AN ENTANGLING GATE!!

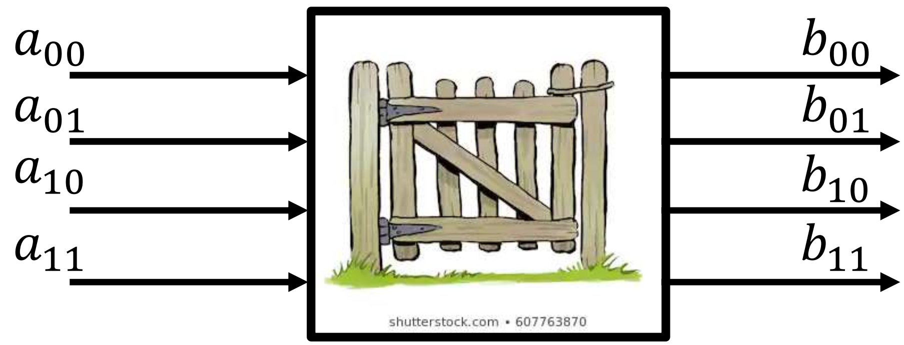
Lets try some simple gates

- So we know how to construct simple 2-qubit quantum gates

- So now, lets try to build them for the following 2-input Boolean operations
  - $X \oplus Y$
  - $X\ (AND)\ Y$

XOR



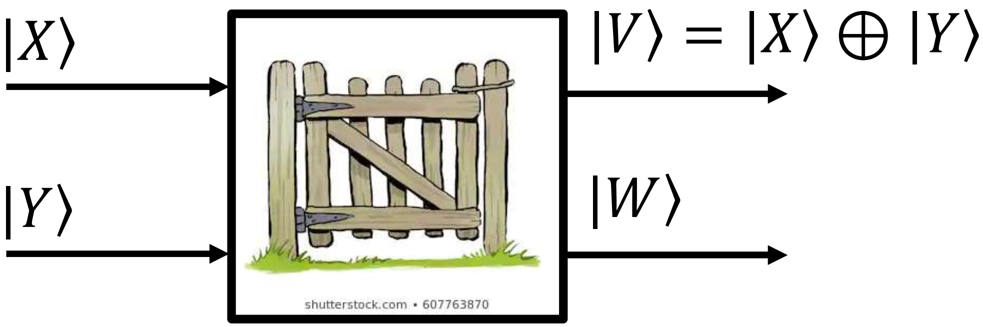


$$|VW\rangle = U|XY\rangle$$

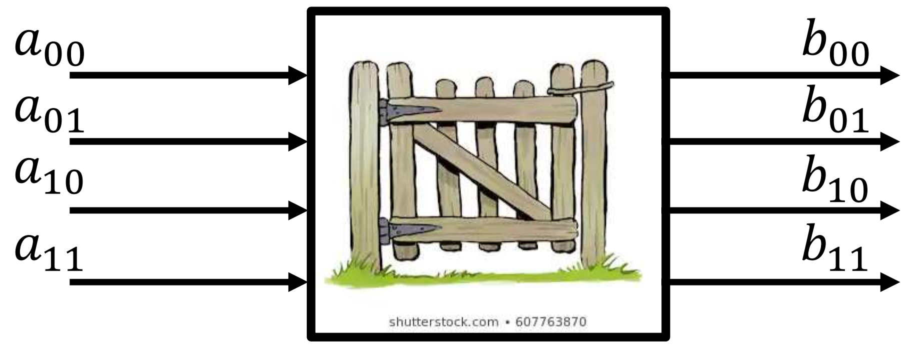
- We don't care what W is
- Create U such that the truth table to the right is produced

X	Y	V	W
0	0	0	
0	1	1	
1	0	1	
1	1	0	

XOR



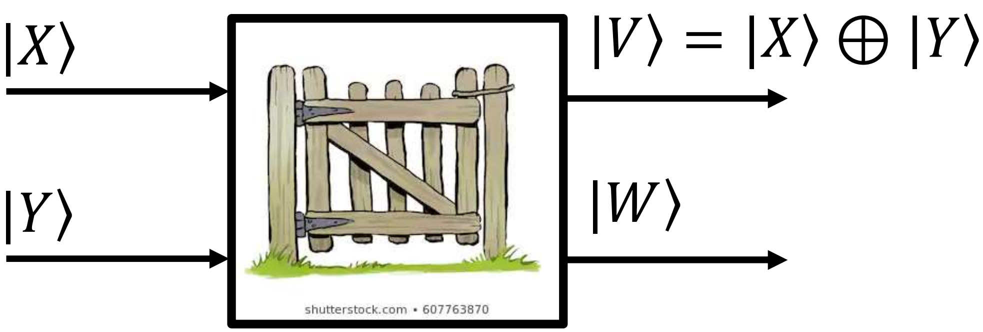
$|VW\rangle = U|XY\rangle$

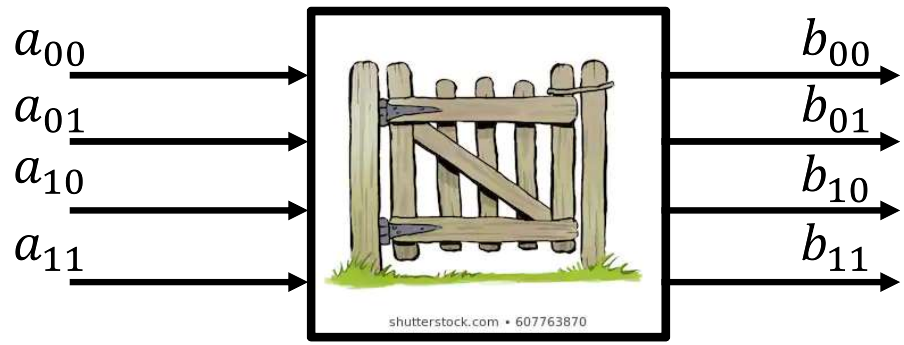


- $U|00\rangle = |0 *\rangle$
- How do we select W to construct a U for this?

X	Y	V	W
0	0	0	
0	1	1	
1	0	1	
1	1	0	

XOR



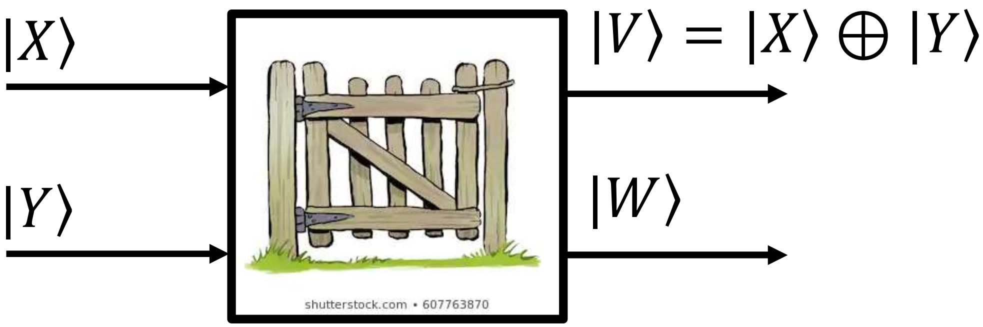


$$|VW\rangle = U|XY\rangle$$

X	Y	V	W
0	0	0	0
0	1	1	0
1	0	1	1
1	1	0	1

- $U|00\rangle = |0\ *\rangle$
- How do we select W to construct a U for this?
- Invertibility: Every orange row must be unique (or the function is not invertible)
  - Create W for this
- Design a U for the chosen W

XOR



$$|VW\rangle = U|XY\rangle$$

X	Y	V	W
0	0	0	0
0	1	1	0
1	0	1	1
1	1	0	1

- $U|00\rangle = |00\rangle, U|01\rangle = |10\rangle, U|10\rangle = |11\rangle, U|11\rangle = |01\rangle$

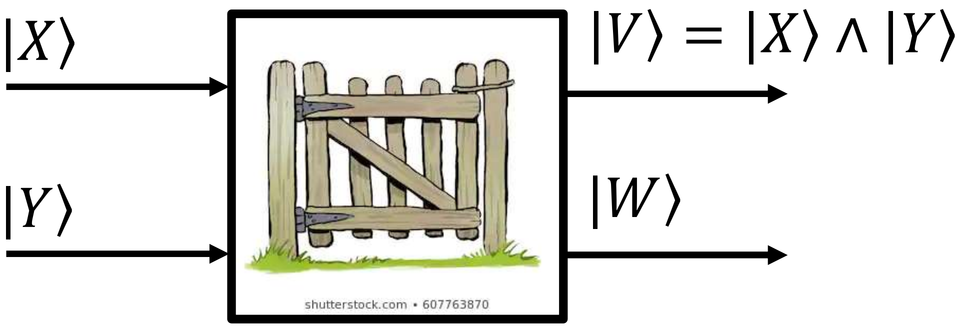
$$\begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} u_{00} & u_{01} & u_{02} & u_{03} \\ u_{10} & u_{11} & u_{12} & u_{13} \\ u_{20} & u_{21} & u_{22} & u_{23} \\ u_{30} & u_{31} & u_{23} & u_{33} \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

$$\begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} u_{00} & u_{01} & u_{02} & u_{03} \\ u_{10} & u_{11} & u_{12} & u_{13} \\ u_{20} & u_{21} & u_{22} & u_{23} \\ u_{30} & u_{31} & u_{23} & u_{33} \end{bmatrix} \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}$$

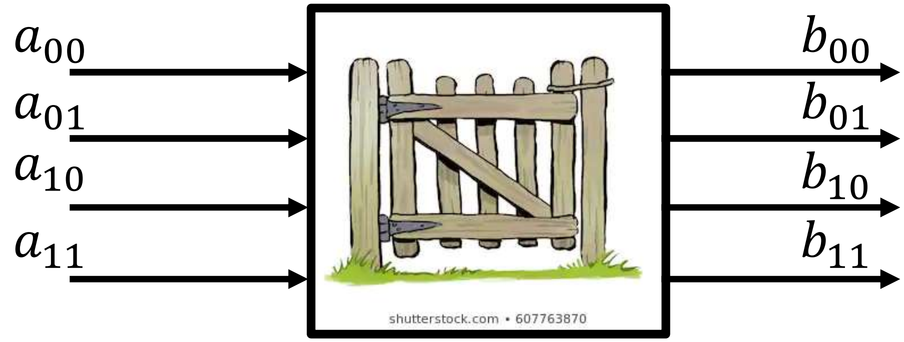
$$\begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} u_{00} & u_{01} & u_{02} & u_{03} \\ u_{10} & u_{11} & u_{12} & u_{13} \\ u_{20} & u_{21} & u_{22} & u_{23} \\ u_{30} & u_{31} & u_{23} & u_{33} \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}$$

$$\begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} u_{00} & u_{01} & u_{02} & u_{03} \\ u_{10} & u_{11} & u_{12} & u_{13} \\ u_{20} & u_{21} & u_{22} & u_{23} \\ u_{30} & u_{31} & u_{23} & u_{33} \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}$$

AND



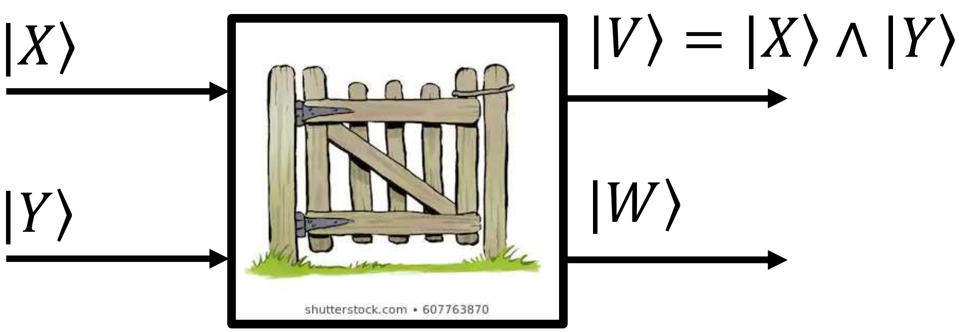
$|VW\rangle = U|XY\rangle$

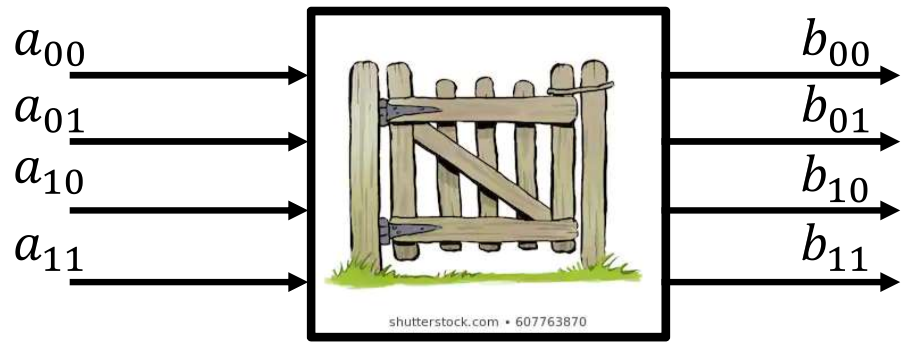


- How do we select W to be able to construct a U for this table?

X	Y	V	W
0	0	0	*
0	1	0	*
1	0	0	*
1	1	1	*

AND



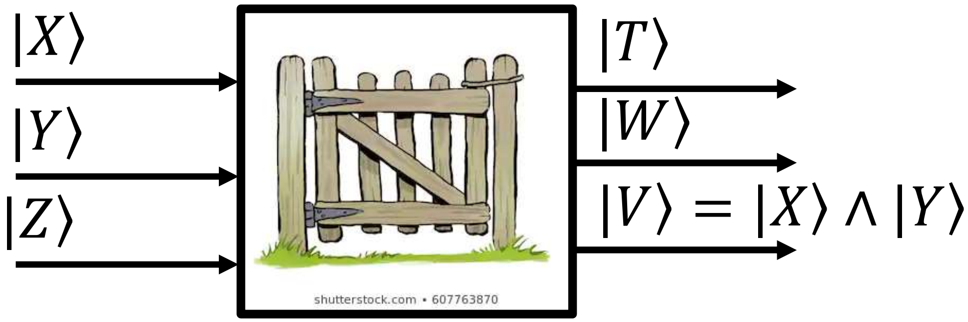


$$|VW\rangle = U|XY\rangle$$

X	Y	V	W
0	0	0	*
0	1	0	*
1	0	0	*
1	1	1	*

- How do we select W to be able to construct a U for this table?
- You cannot!!!
  - Which other gates are similarly impossible to model?

So how do you do an AND

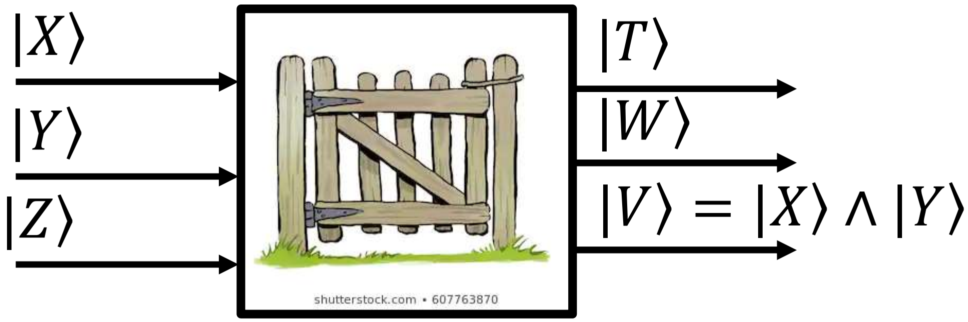


$$|VW\rangle = U|XY\rangle$$

X	Y	Z	T	W	V
0	0	0	*	*	*
0	0	1	*	*	*
0	1	0	*	*	*
0	1	1	*	*	*
1	0	0	*	*	*
1	0	1	*	*	*
1	1	0	*	*	*
1	1	1	*	*	*

- You add an *output qubit*
  - The fact is, the output is not manufactured from thin air
  - Its actually an entire qubit
- Does this help?

So how do you do an AND

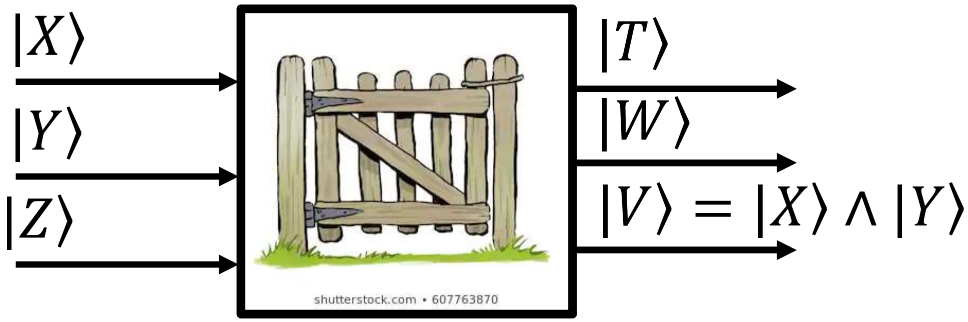


$$|VW\rangle = U|XY\rangle$$

X	Y	Z	T	W	V
0	0	0	*	*	0
0	0	1	*	*	0
0	1	0	*	*	0
0	1	1	*	*	0
1	0	0	*	*	0
1	0	1	*	*	0
1	1	0	*	*	1
1	1	1	*	*	1

- You can't in general
    - If you want V to give you the right input regardless of Z

So how do you do an AND

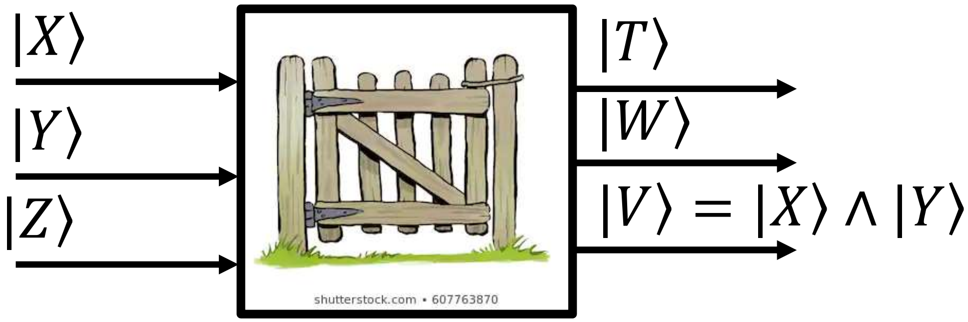


$$|VW\rangle = U|XY\rangle$$

- You can't in general
  - If you want V to give you the right input regardless of Z
- But it only has to work for *one value of Z*
  - This gives you a lot more freedom to "design" your transform

X	Y	Z	T	W	V
0	0	0	*	*	0
0	0	1	*	*	*
0	1	0	*	*	0
0	1	1	*	*	*
1	0	0	*	*	0
1	0	1	*	*	*
1	1	0	*	*	1
1	1	1	*	*	*

So how do you do an AND

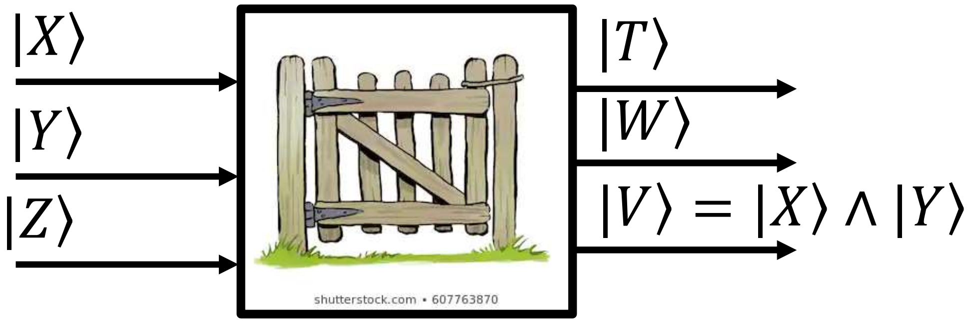


$$|VW\rangle = U|XY\rangle$$

X	Y	Z	T	W	V
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	1	0
1	1	0	1	0	1
1	1	1	1	1	1

- You can't in general
  - If you want V to give you the right input regardless of Z
- But it only has to work for *one value of Z*
  - This gives you a lot more freedom to "design" your transform

The CSWAP (or FREDKIN) Gate

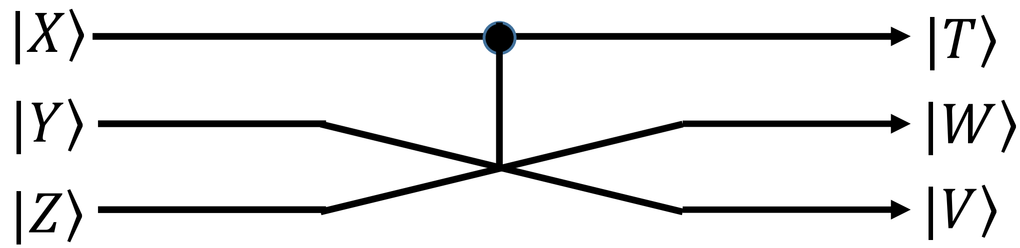


$$|VW\rangle = U|XY\rangle$$

$$U = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

X	Y	Z	T	W	V
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	1	0
1	1	0	1	0	1
1	1	1	1	1	1

The CSWAP gate

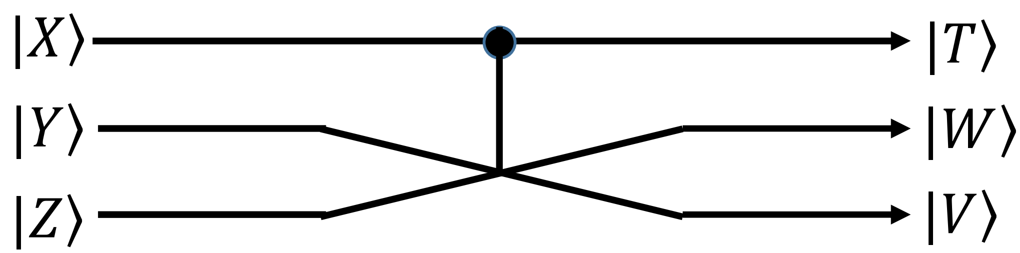


- The controlled swap gate
  - If the "control" X is 0, Y and Z go through in the same order
  - If X is 1, Y and Z swap
- Verify that when Z = 0, V = X AND Y
- What other Boolean functions can you get by varying Z?
  - And at what output variable?
- What would the output be for *superposed* states?

The CSWAP gate

Note: The CSWAP, combined with a NOT is a universal gate!!

Why??

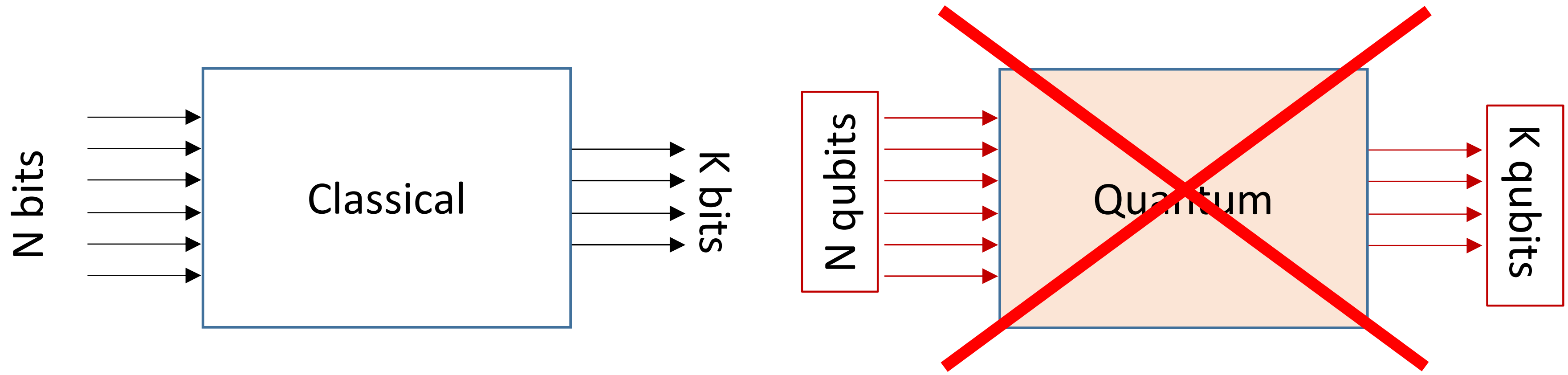


- The controlled swap gate
  - If the “control” X is 0, Y and Z go through in the same order
  - If X is 1, Y and Z swap
- Verify that when Z = 0, V = X AND Y
- What other Boolean functions can you get by varying Z?
  - And at what output variable?
- What would the output be for *superposed* states?

Lesson for the day

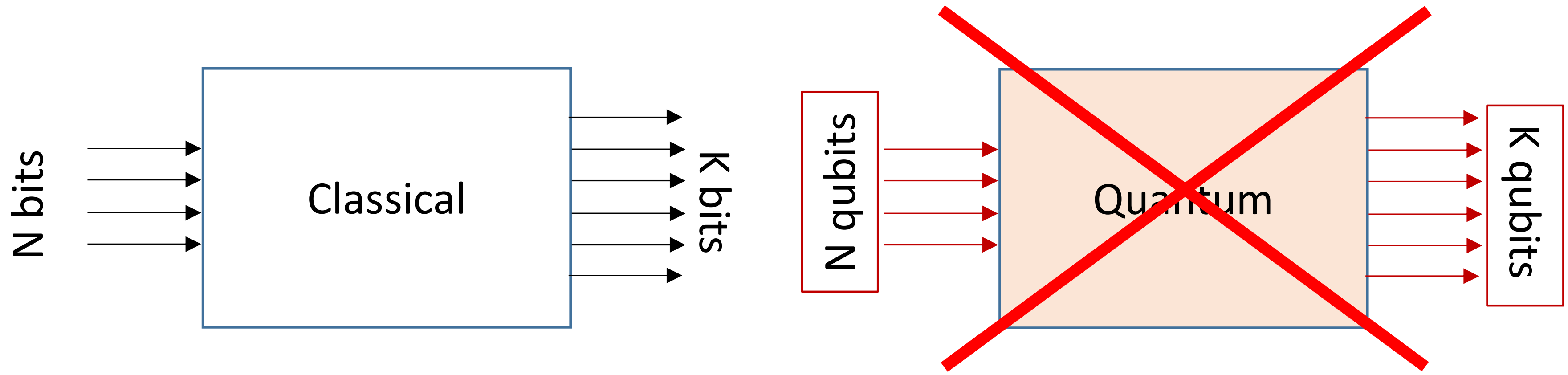
- You cannot simply emulate N-bit classical gates with an N-bit quantum circuit
- You will have to add extra qubits to hold the output
- And still more qubits to hold other necessary variables
    - AKA “junk”

Classical vs Quantum circuits



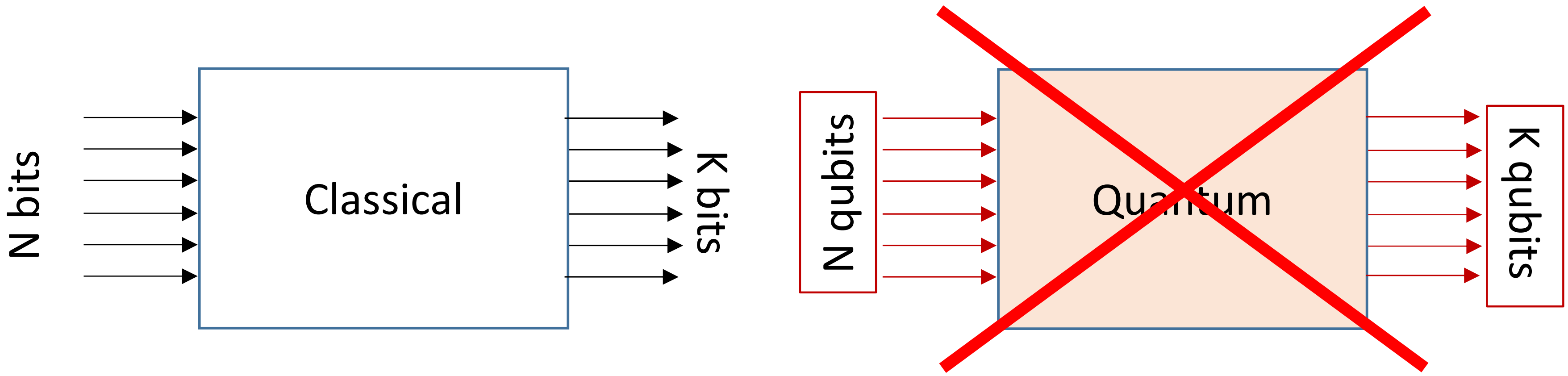
- Classical circuits:
    - N bits go in
    - K bits come out
- Quantum circuits:
    - Can often not directly emulate the classical circuit (with N input qubits and K output qubits)
    - For $K < N$, can *definitely* not emulate the classical circuit directly

Classical vs Quantum circuits



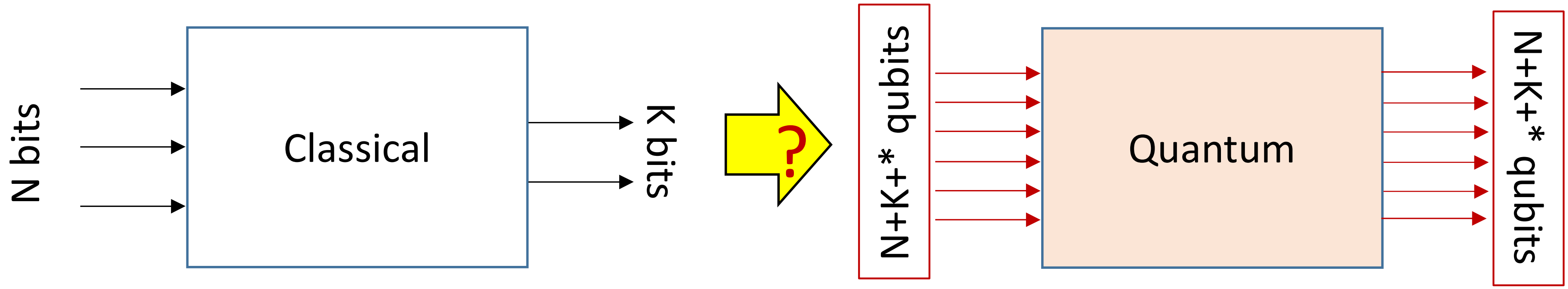
- Classical circuits:
  - N bits go in
  - K bits come out
- Quantum circuits:
  - Can often not directly emulate the classical circuit (with N input qubits and K output qubits)
  - For $K < N$, can *definitely* not emulate the classical circuit directly
  - Can definitely also not emulate the classical circuit if $K > N$!

Classical vs Quantum circuits



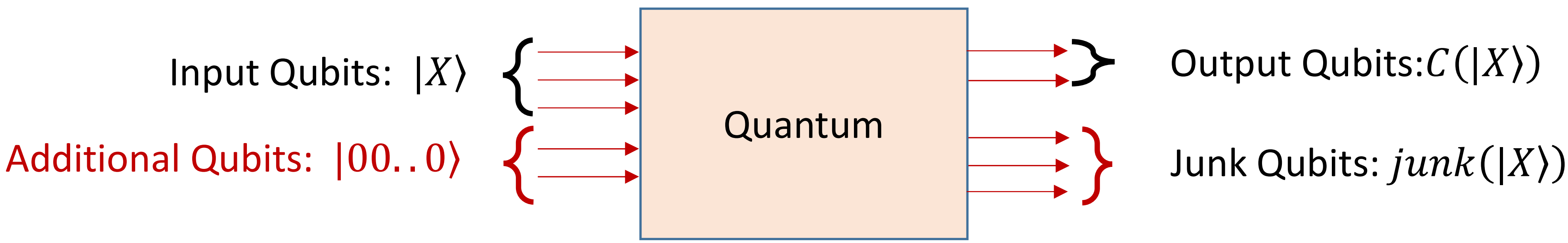
- Classical circuits:
  - N bits go in
  - K bits come out
- Quantum circuits:
  - Can often not directly emulate the classical circuit (with N input qubits and K output qubits)
  - For $K < N$, can *definitely* not emulate the classical circuit directly
  - Can definitely also not emulate the classical circuit if $K > N$!
  - Even for $K = N$, often need additional inputs and outputs

Classical vs Quantum circuits



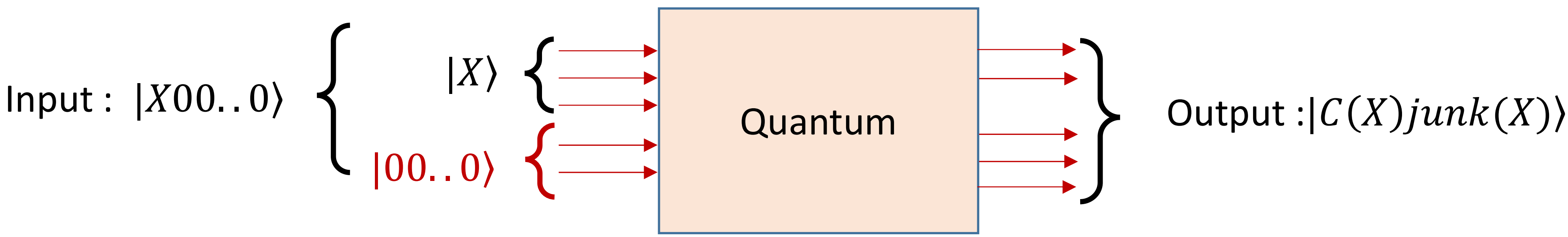
- Classical circuits:
  - N bits go in
  - K bits come out
- What principles do we use to design them?
  - Is there a *generic* method?
  - And what must we watch out for?
- Quantum circuits:
  - Can often not directly emulate the classical circuit (with N input qubits and K output qubits)
  - For $K < N$, can *definitely* not emulate the classical circuit directly
  - Can definitely also not emulate the classical circuit if $K > N$!
  - Even for $K = N$, often need additional inputs and outputs

Making a classical circuit quantum



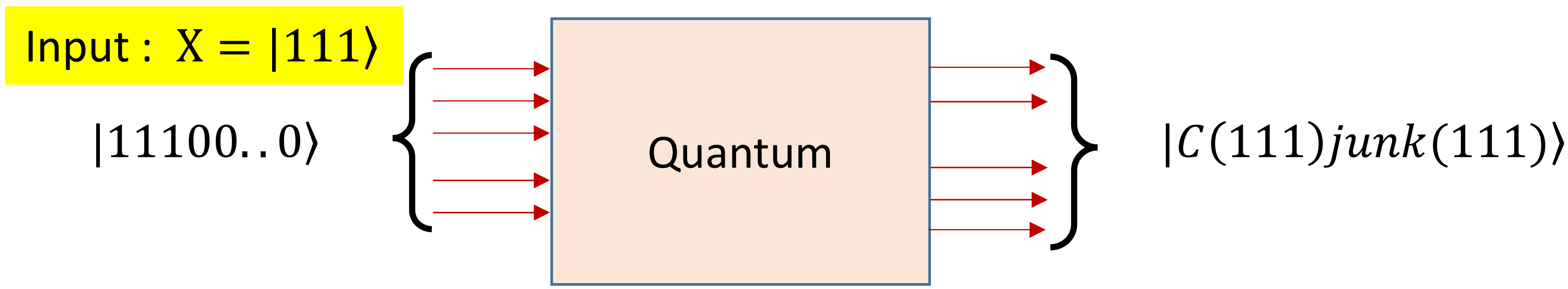
- First, make it reversible
  - Total number of input qubits = Total number of output qubits
- Output bits don't just emerge from the ether, they were always there
  - So, actual circuit has as input "$X\ bits$ | $Y\ bits$"
  - The output is actually "$C(X)$ | $junk(X)$"
    - The input bits too may get modified
  - No. of qubits in $junk(X)$ = no. of qubits in X
- But... Not so simple...

Making a classical circuit quantum



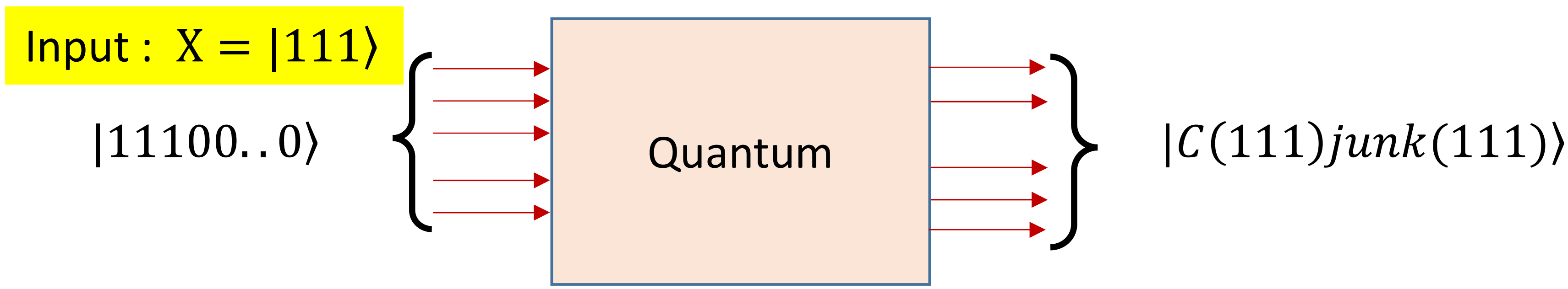
- The output is not $C(X) \otimes junk(X)$
  - It is actually $|C(X)junk(X)\rangle$
  - I.e. for any given input X you will not be able to obtain all possible combinations of $C(X)$ and all 2^N possible values of $junk(X)$ simply by manipulating the *input* values of the output bits Y
    - Why is this the case?

Making a classical circuit quantum



- The output is not $C(X) \otimes junk(X)$
  - It is actually $|C(X)junk(X)\rangle$
- When you fix X, the values of $junk(X)$ are restricted
  - Only K bits available to manipulate N bits
- In other words, when you fix $C(X)$, the values of $junk(X)$ are restricted
  - The target output bits and the junk output bits are *entangled!!!*

Making a classical circuit quantum



Why is this a problem?

- The output is not $C(X) \otimes junk(X)$
  - It is actually $|C(X)junk(X)\rangle$
- When you fix X, the values of $junk(X)$ are restricted
  - Only K bits available to manipulate N bits
- In other words, when you fix $C(X)$, the values of $junk(X)$ are restricted
  - The target output bits and the junk output bits are *entangled!!!*

The trouble with junk – an example

$$U = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$X \xrightarrow{\text{classical}} Y = X$

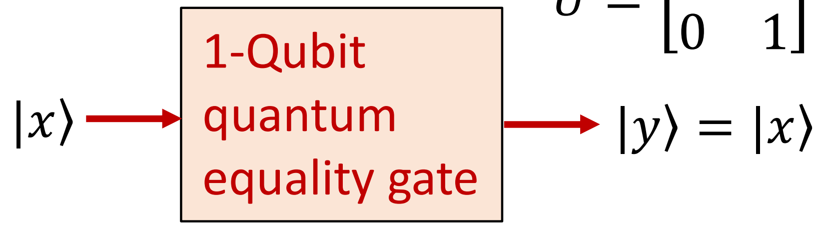
$|x\rangle \xrightarrow{\text{1-Qubit quantum equality gate}} |y\rangle = |x\rangle$

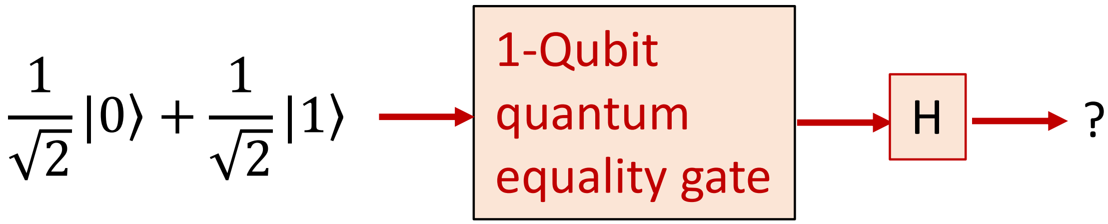
$$\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \xrightarrow{\text{1-Qubit quantum equality gate}} \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

- Consider a 1-bit equality gate
  - Classically $y = x$
- This can in fact be implemented using a 1-qubit quantum gate with $U = I$
  - More generally, if $x = a_0|0\rangle + a_1|1\rangle$, then the output $y = a_0|0\rangle + a_1|1\rangle$
- We input the sign basis $|x\rangle = |+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$
  - Output is $|y\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$

The trouble with junk – an example

$$U = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

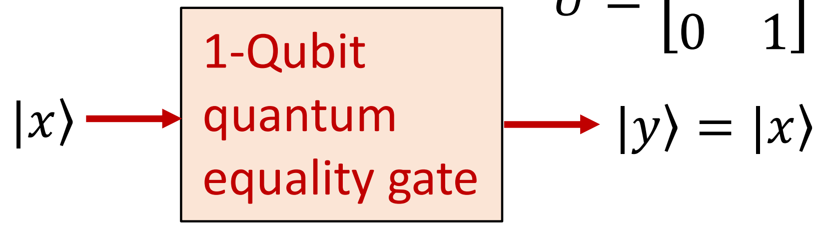


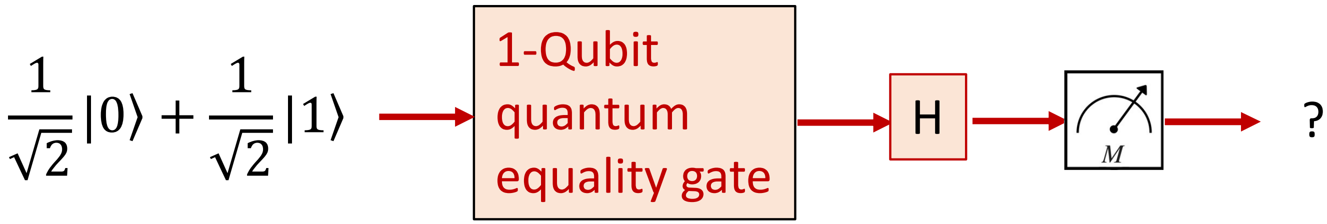


- Consider a 1-bit equality gate
  - Classically $y = x$
- This can in fact be implemented using a 1-qubit quantum gate with $U = I$
  - More generally, if $x = a_0|0\rangle + a_1|1\rangle$, then the output $y = a_0|0\rangle + a_1|1\rangle$
- We input the sign basis $|x\rangle = |+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$
  - Output is $|y\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$
- Now we put a Hadamard gate at the output
  - What is the output?
  - What will we get if we measure it?

The trouble with junk – an example

$$U = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

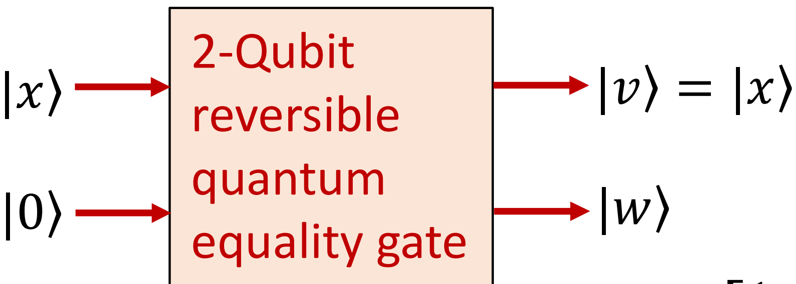




- Consider a 1-bit equality gate
  - Classically $y = x$
- This can in fact be implemented using a 1-qubit quantum gate with $U = I$
  - More generally, if $x = a_0|0\rangle + a_1|1\rangle$, then the output $y = a_0|0\rangle + a_1|1\rangle$
- We input the sign basis $|x\rangle = |+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$
  - Output is $|y\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$
- Now we put a Hadamard gate at the output
  - What is the output?
  - **What will we get if we measure it?**

The reversible 2-qubit equality gate

X	Y	V	W
0	0	0	0
0	1	0	1
1	0	1	1
1	1	1	0

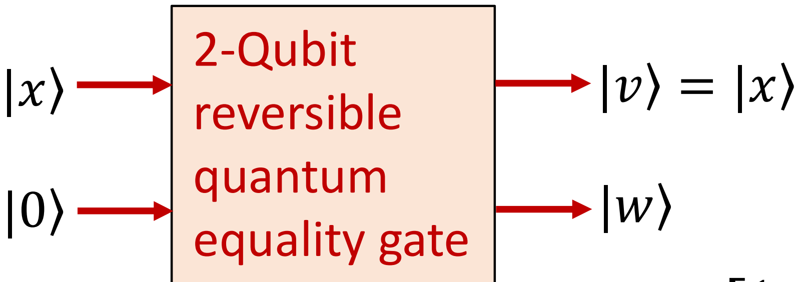


$$U = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

- Now we convert it to a reversible gate using the earlier formula
  - Add a second input and second output
  - We construct the truth table above:
- The equality gate is obtained by setting the second input to 0
  - For $|y\rangle = |0\rangle$, the output $|v\rangle$ is $|v\rangle = |x\rangle$

The reversible 2-qubit equality gate

X	Y	V	W
0	0	0	0
0	1	0	1
1	0	1	1
1	1	1	0

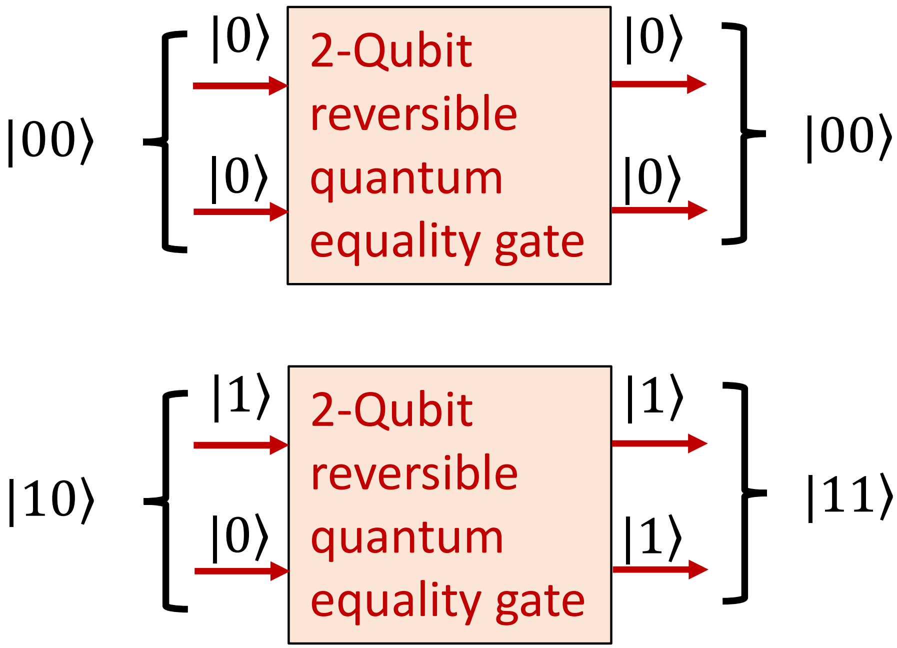


$$U = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & & & \\ 0 & & & \\ 0 & & & \end{bmatrix}$$

Note that this is not necessary for this gate; this exercise is meant for illustrating the problem with junk

- Now we convert it to a reversible gate using the earlier formula
  - Add a second input and second output
  - We construct the truth table above:
- The equality gate is obtained by setting the second input to 0
  - For $|y\rangle = |0\rangle$, the output $|v\rangle$ is $|v\rangle = |x\rangle$

Looking closer

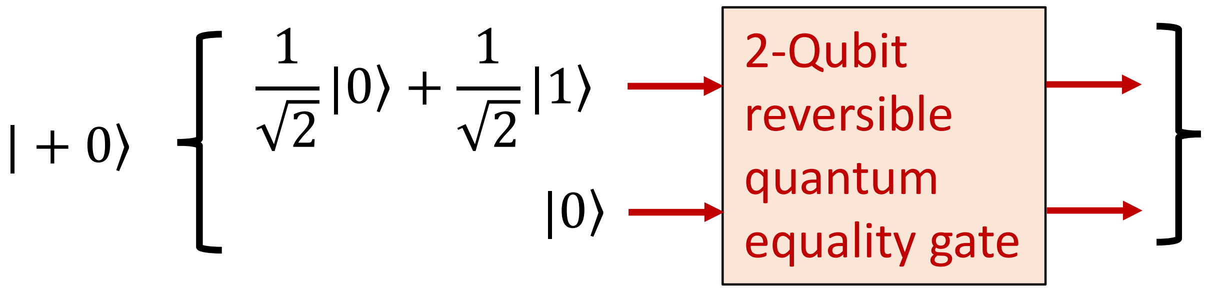


X	Y	V	W
0	0	0	0
0	1	0	1
1	0	1	1
1	1	1	0

- The equality gate is obtained by setting the second input to 0
- For $|y\rangle = |0\rangle$, the output $|v\rangle$ is *apparently* $|v\rangle = |x\rangle$
- The *actual* complete output is,

$$\text{for } |xy\rangle = |00\rangle, \quad \Rightarrow \quad |vw\rangle = |00\rangle$$
$$\text{for } |xy\rangle = |10\rangle, \quad \Rightarrow \quad |vw\rangle = |11\rangle$$

Lets input a + basis

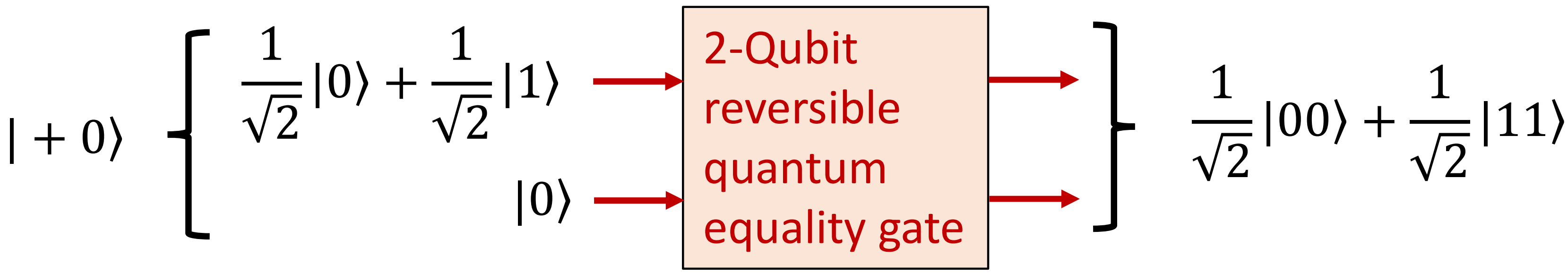


- The input is:

$$|x0\rangle = |+0\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|10\rangle$$

- The complete output is:

Lets input a + basis



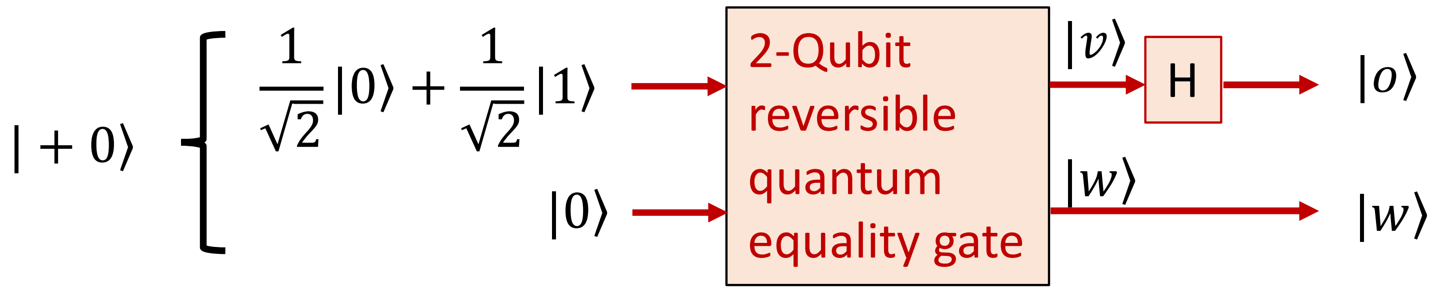
- The input is:

$$|x0\rangle = |+0\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|10\rangle$$

- The complete output is:

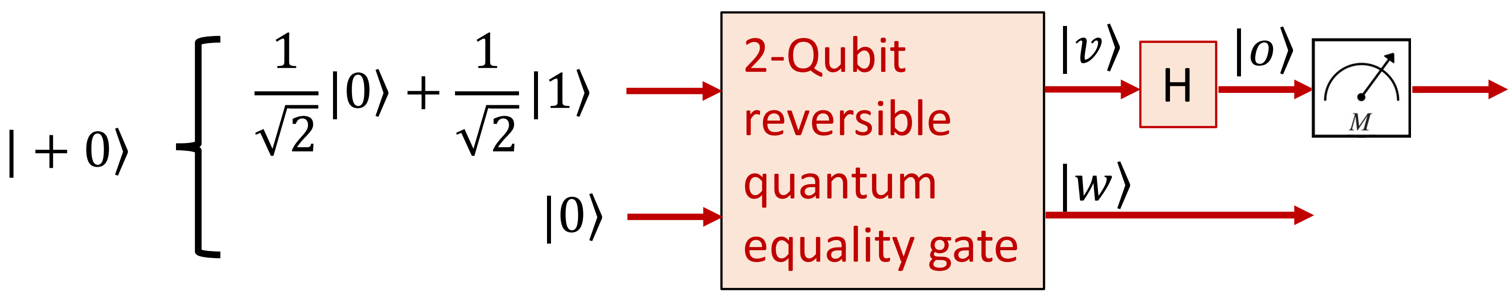
$$|vw\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$$

Collapsing the equality of the reversible 2-qubit equality gate



- Now add a Hadamard to the first qubit
- Note that this is effectively the same situation as we had with the one-qubit gate
- But is the output the same as for the 1-qubit gate?

The trouble with junk



- The actual output before the Hadamard is

$$|vw\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$$

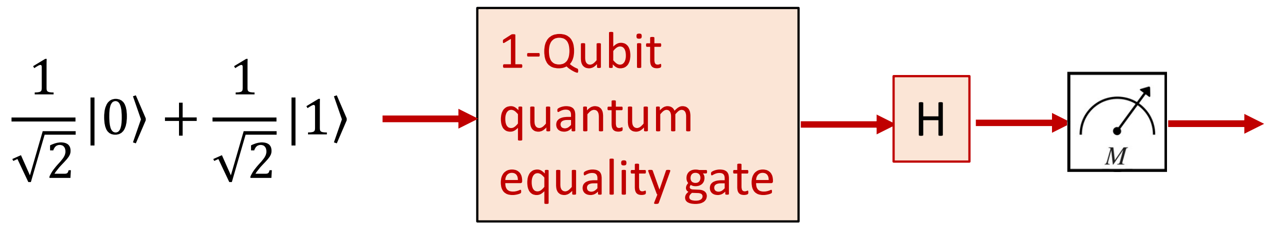
- The output after the Hadamard is:

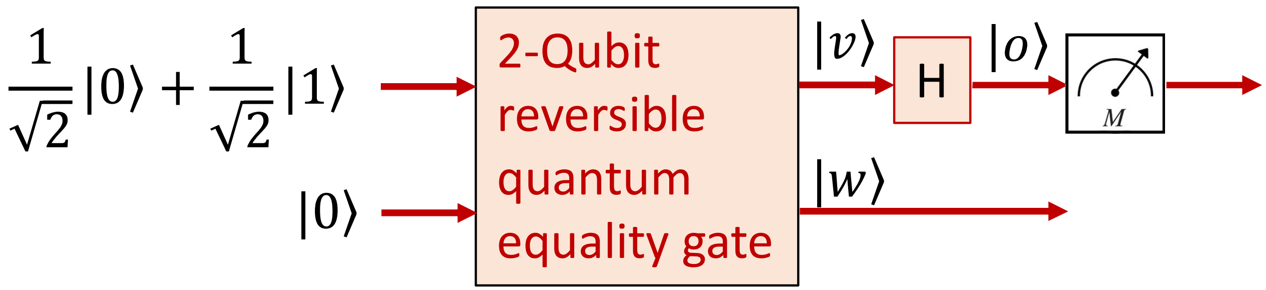
$$|ov\rangle = \frac{1}{\sqrt{2}}\left|\left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right)0\right\rangle + \frac{1}{\sqrt{2}}\left|\left(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle\right)1\right\rangle$$

$$|ov\rangle = \frac{1}{2}(|00\rangle + |10\rangle + |01\rangle - |11\rangle)$$

- The output is no longer deterministic. In fact the probability of measuring a 1 on the first bit is (what?)

The trouble with junk

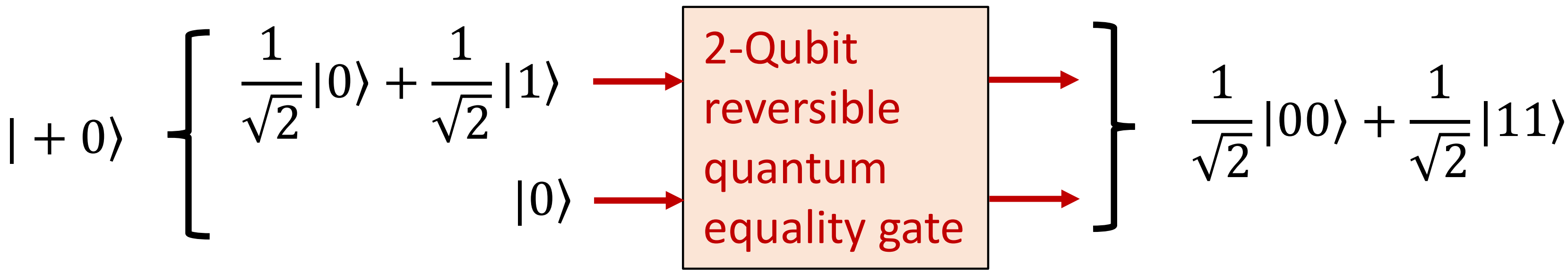




- Comparison:
  - Using the 1-qubit gate the measured output is $|1\rangle$
  - Using the 2-qubit gate, the probability of measuring $|1\rangle$ is 0.5

- Simply having the junk bit destroyed our equality gate!!

Lets input a + basis

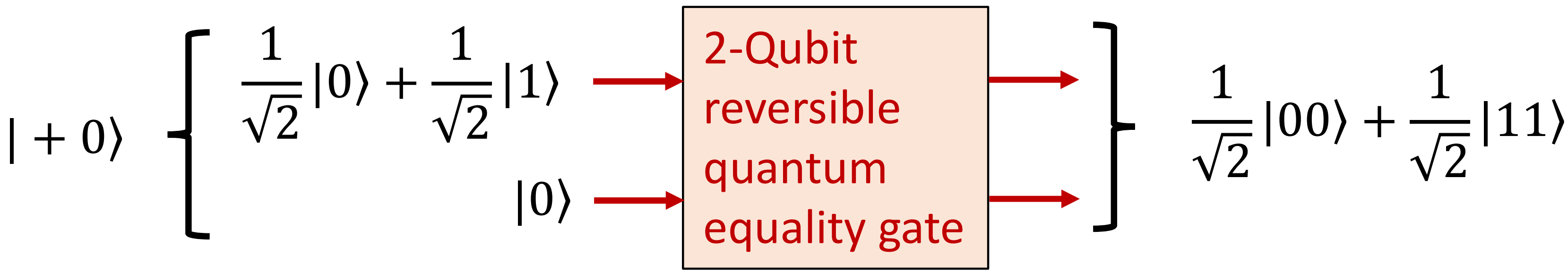


- The output is:

$$|vw\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$$

- If you measure w and get a 0, what is v?
- If you measure w and get a 1, what is v?

Lets input a + basis



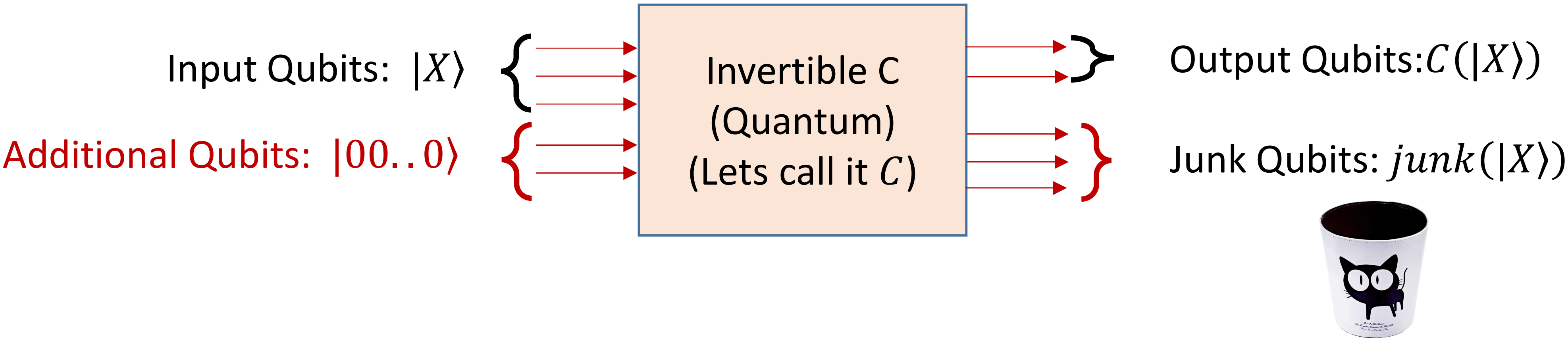
- The output is:

$$|vw\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$$

- If you measure w and get a 0, what is v?
- If you measure w and get a 1, what is v?

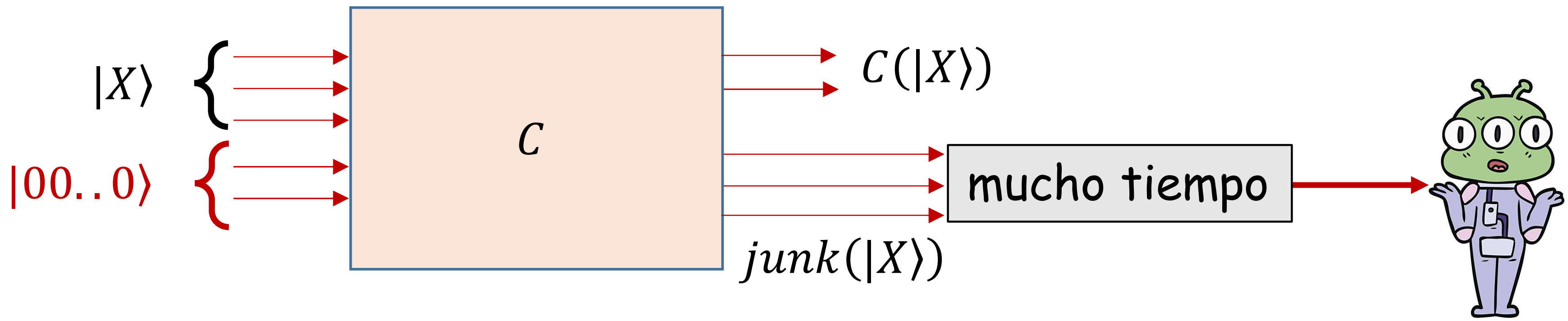
What we measure on the junk bit affects what you measure on output

So why don’t we just “junk” our junk bits?



- Account for them in our arithmetic and ignore them…
- You can’t

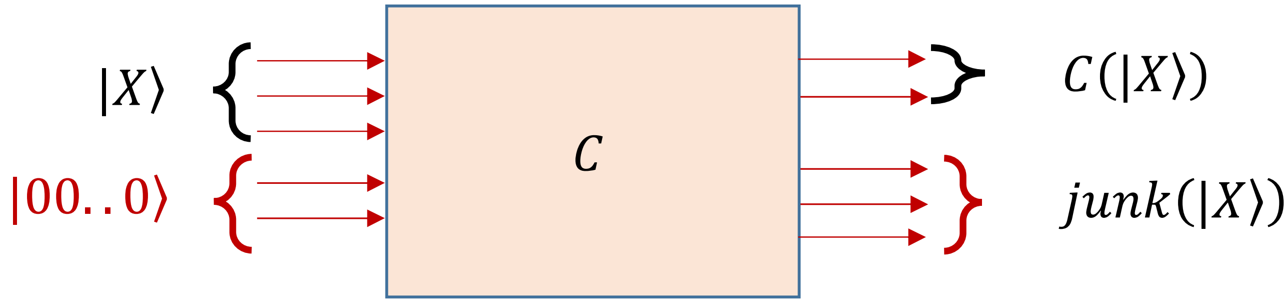
Remember the time machine?



- Someone, somewhere, somewhen may measure the junk bits
  - Today or in the year 20,000,000AD
  - This someone could simply be nature

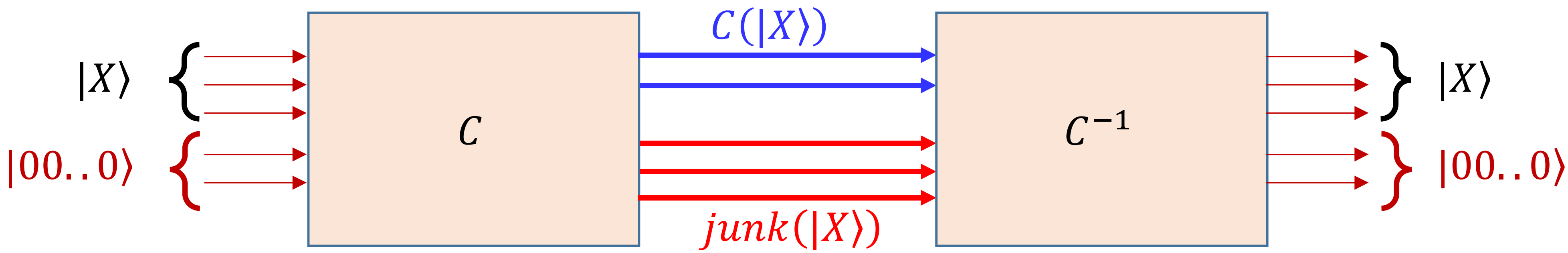
- What they measure will influence your measurement today
  - You cannot trust the output of your computation
  - You cannot simply assume the junk will never be measured, and you cannot assume what it will be measured as

So how do we deal with the junk?



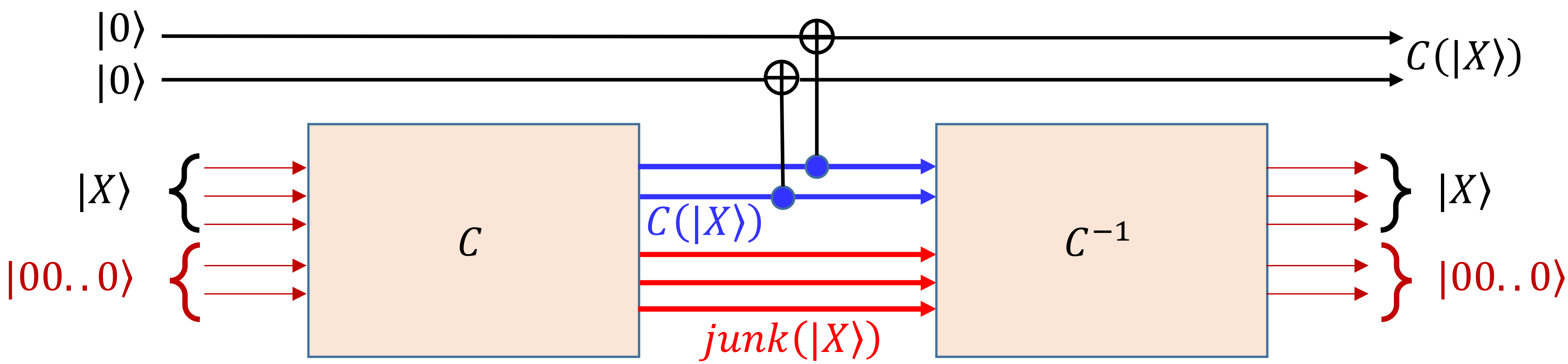
- The junk bits cannot just be discarded.
  - So how do we handle them?
- Desideratum : They must be "disentangled" from the actual output, somehow
- Hint: The circuit is invertible…

Eliminating the junk



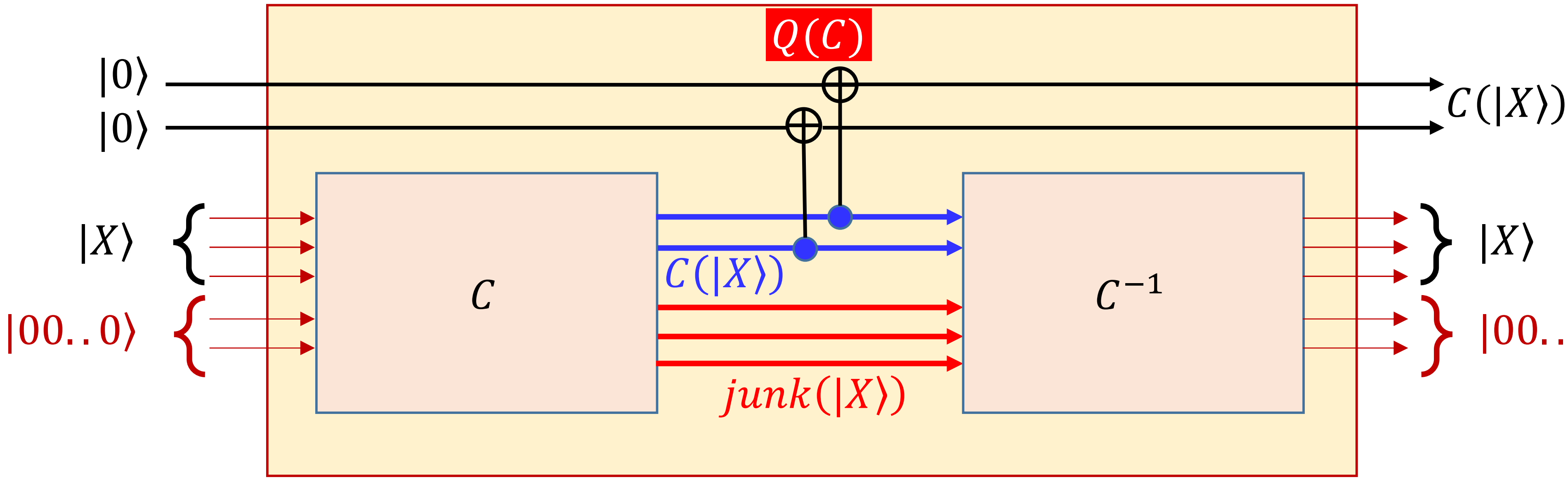
- If you connect the inverse of the circuit to the circuit, you "disentangle" the junk bits
  - Which will return to the value $|00\ldots0\rangle$
- But now, we've lost the target output $C(|X\rangle)$

Retaining the output



- Have a second set of output qubits which are CNOTted with $C(|X\rangle)$
  - The output qubits are initialized to $|0\rangle$
  - $|0\rangle$ CNOT $C(X) = C(X)$
- The output is captured
  - The input is retained
  - The Junk bits are disentangled

The full circuit



- Input comprises
  - $|X\rangle$
  - output bits initialized to $|0\rangle$
  - and a bunch of auxiliary $|0\rangle$s needed for computation

- Output is
  - $C(|X\rangle)$,
  - $|X\rangle$,
  - and a bunch of $|0\rangle$s,
- With junk disentangled

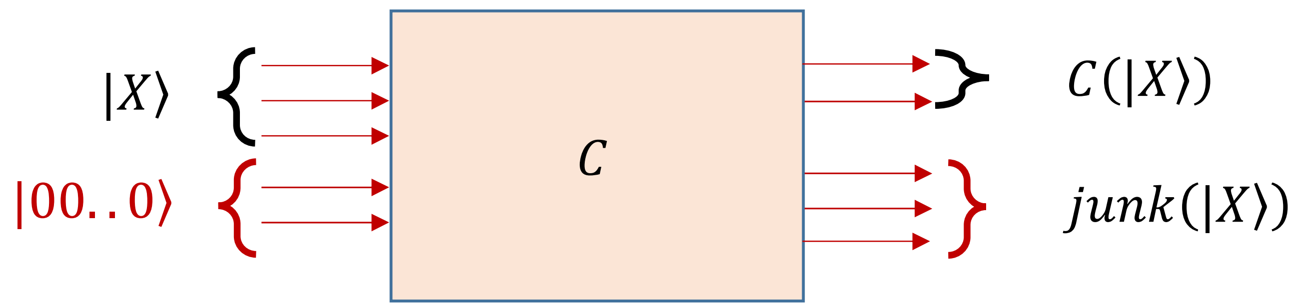
$|X\rangle$ remains entangled with $C(|X\rangle)$, as it must be

The full process: Step 1

- Step 1a: Using truth tables
  - Compose a truth table for the function
    - Will require new output bits
  - Compose the transform for the table
    - As a (minimal) tensor product of universal set of quantum gates
    - Will generally require new junk bits

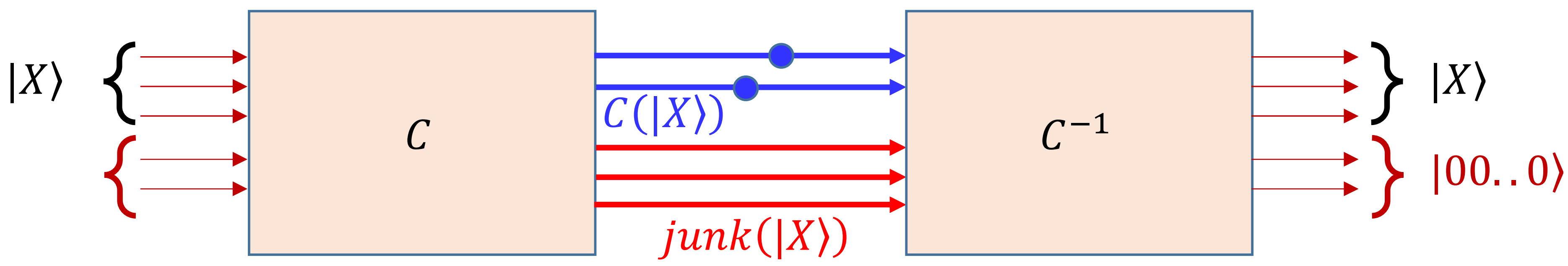
- Step 1alternative: Compose the circuit using quantum variants of Boolean gates
  - Construct quantum circuit using the gates
  - Will require output and junk bits

The output of step 1



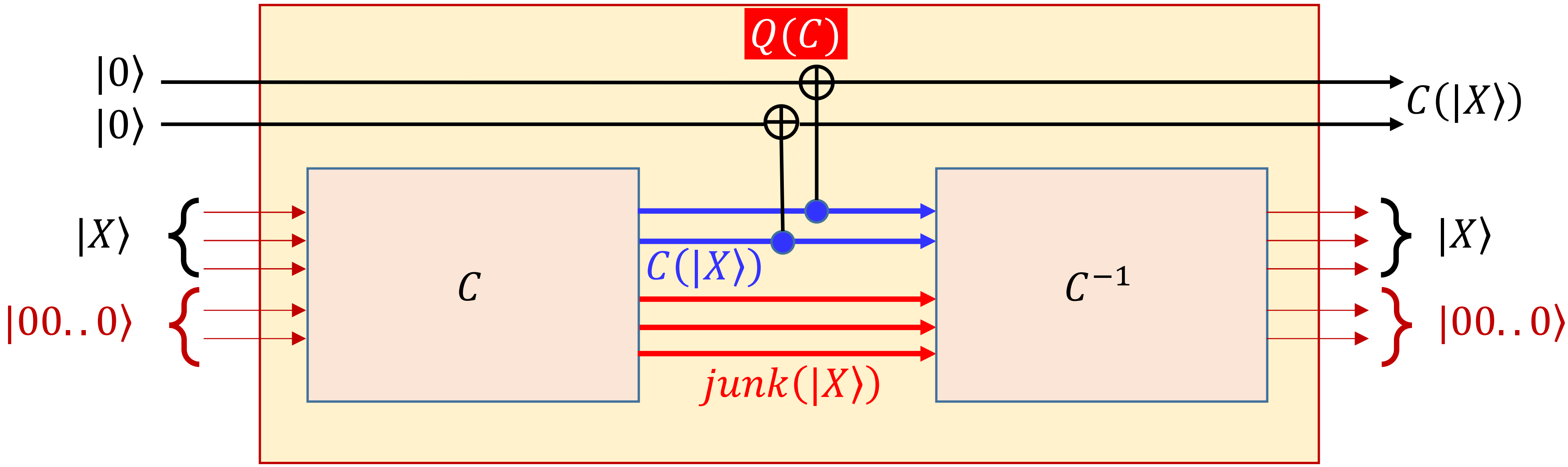
- A circuit that takes in input bits, output bits and junk bits
- And outputs the target output, plus a number of potentially entangled junk bits

Step 2:



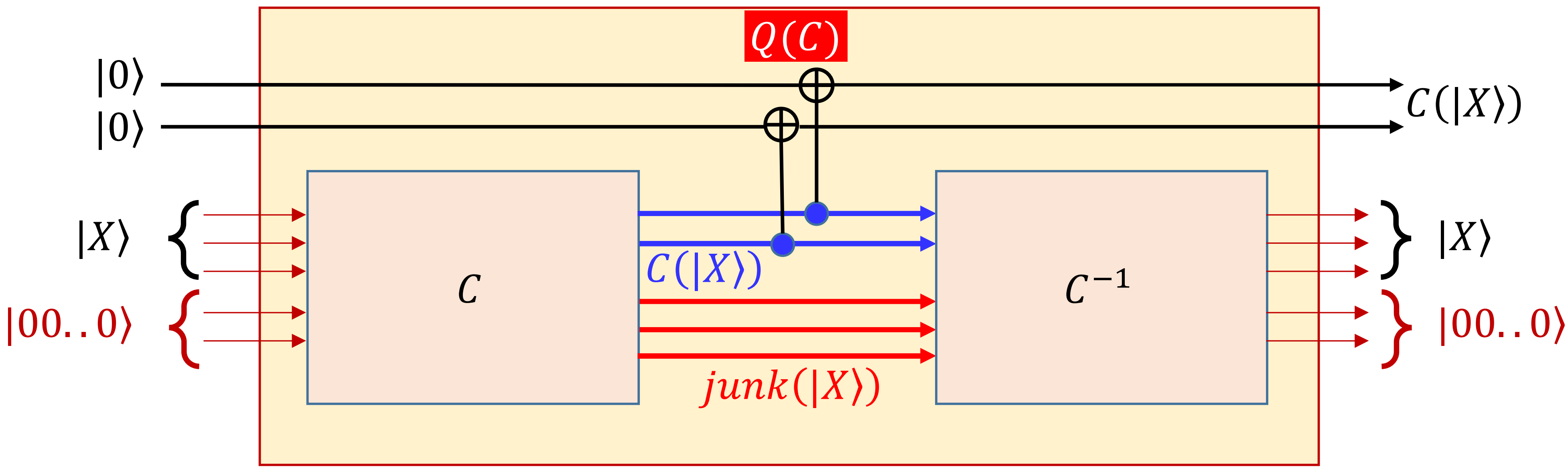
- Couple the output of Step 1 with its own inverse

Step 3:



- Add the actual output qubits, which are CNOTted with the $C(|X\rangle)$ computed by the inner circuit

The full circuit

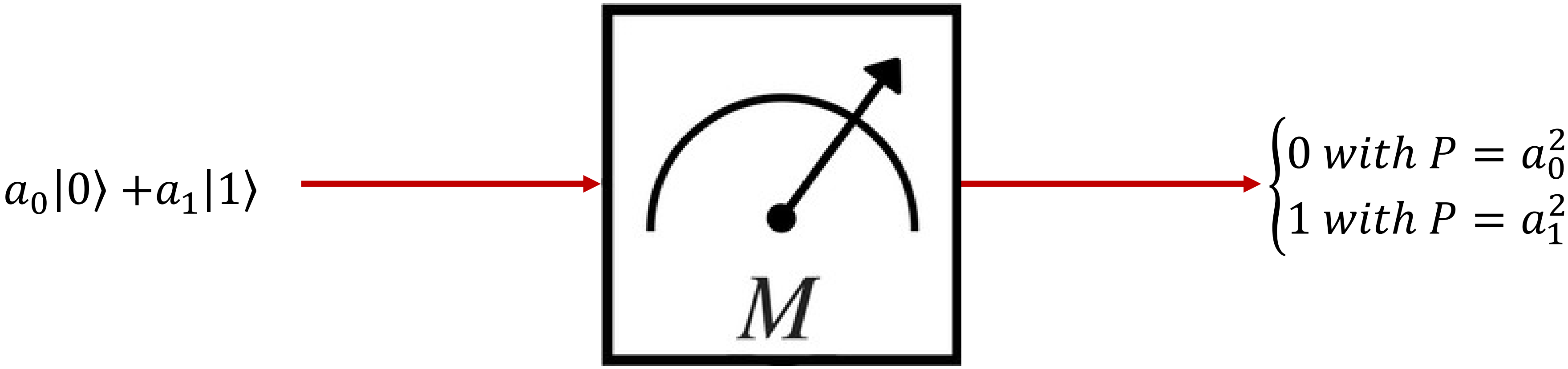


What are the universal quantum set of gates?

- Universal quantum set of gates:
  - CNOT
  - X
  - H
  - Z
  - $\frac{\pi}{8}$ rotation

- Any function can be computed using just these gates

A note on measurement…

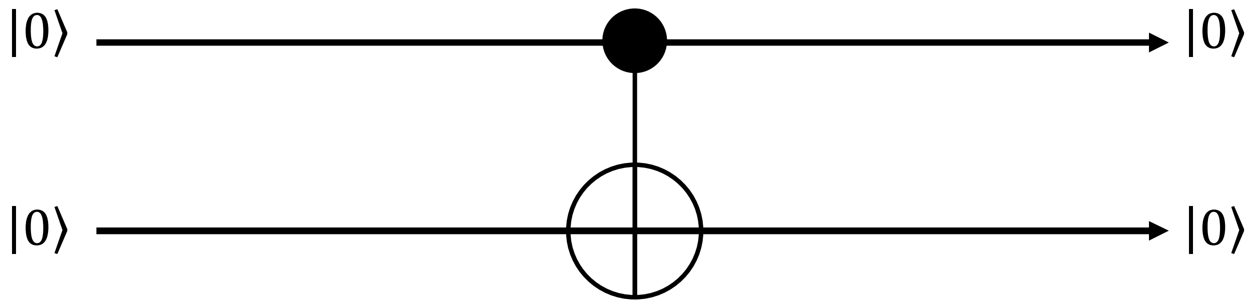


- What is this crazy thing called measurement?

- We have a qubit $|x\rangle = a_0|0\rangle + a_1|1\rangle$
- We want to run some physical operation on it such that the outcome is 0 with P = a_0^2 and 1 with P = a_1^2

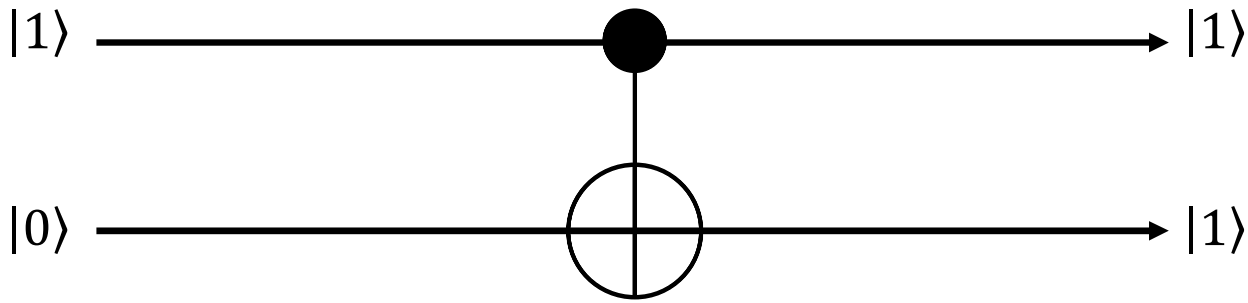
- What might such a process look like?

The CNOT with $|0\rangle$ creates a Bell State



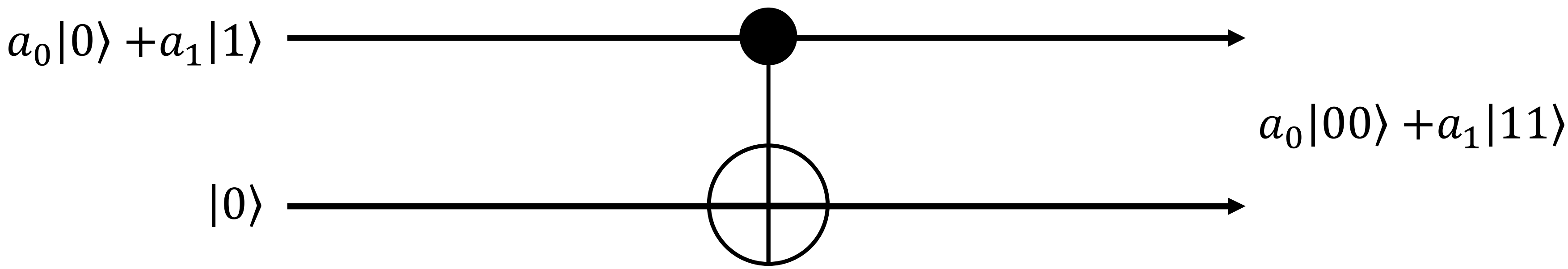
- The target input is $|x\rangle = a_0|0\rangle + a_1|1\rangle$
- The output is $|y\rangle = a_0|00\rangle + a_1|11\rangle$

The CNOT with $|0\rangle$ creates a Bell State



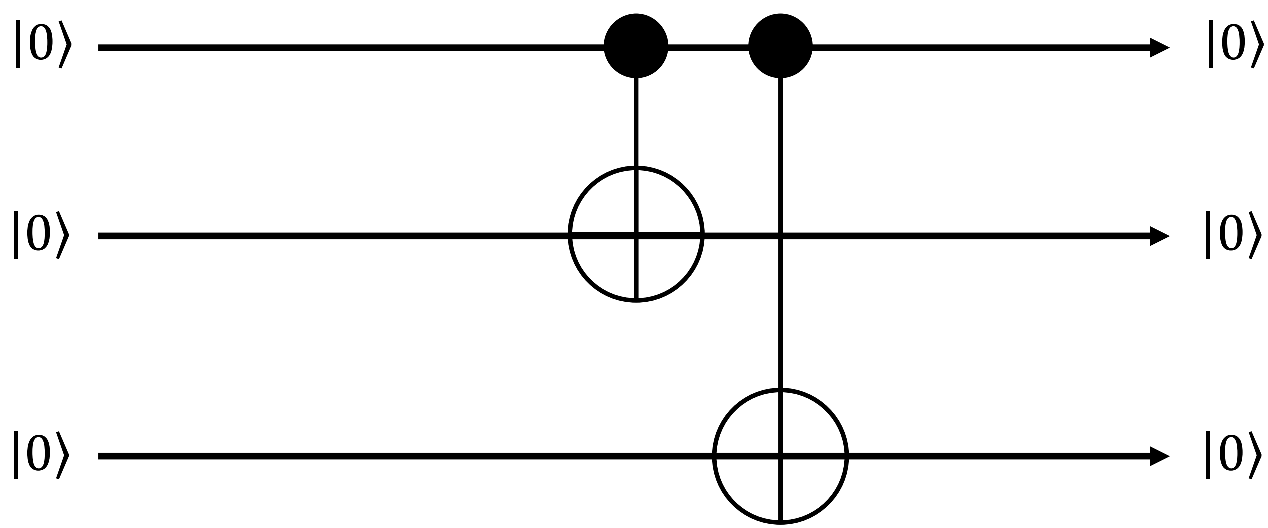
- The target input is $|x\rangle = a_0|0\rangle + a_1|1\rangle$
- The output is $|y\rangle = a_0|00\rangle + a_1|11\rangle$

The CNOT with $|0\rangle$ creates a Bell State



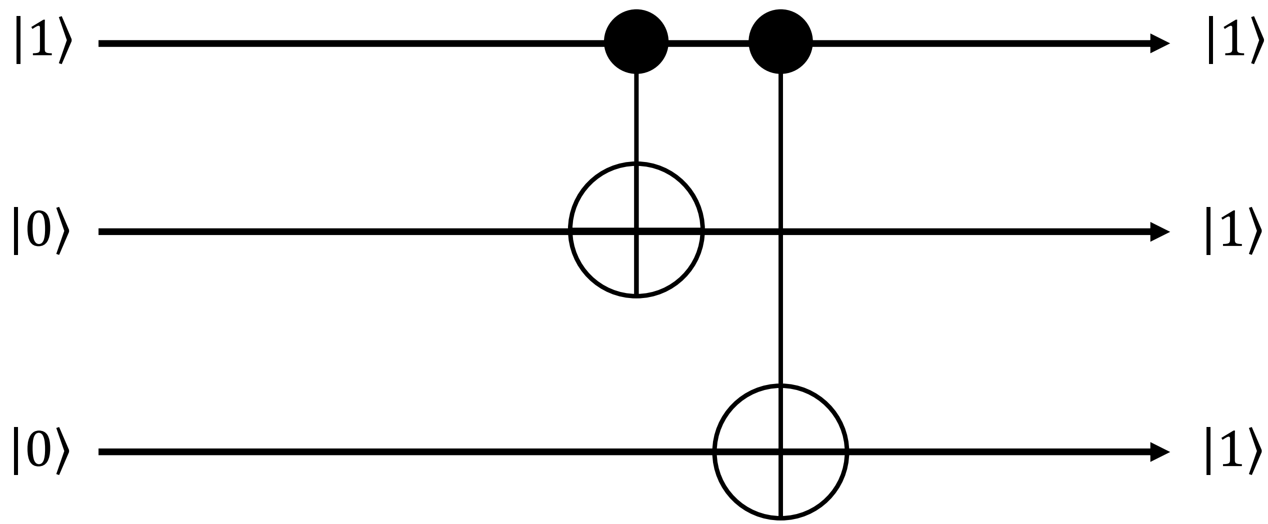
- The target input is $|x\rangle = a_0|0\rangle + a_1|1\rangle$
- The output is $|y\rangle = a_0|00\rangle + a_1|11\rangle$

Adding another CNOT



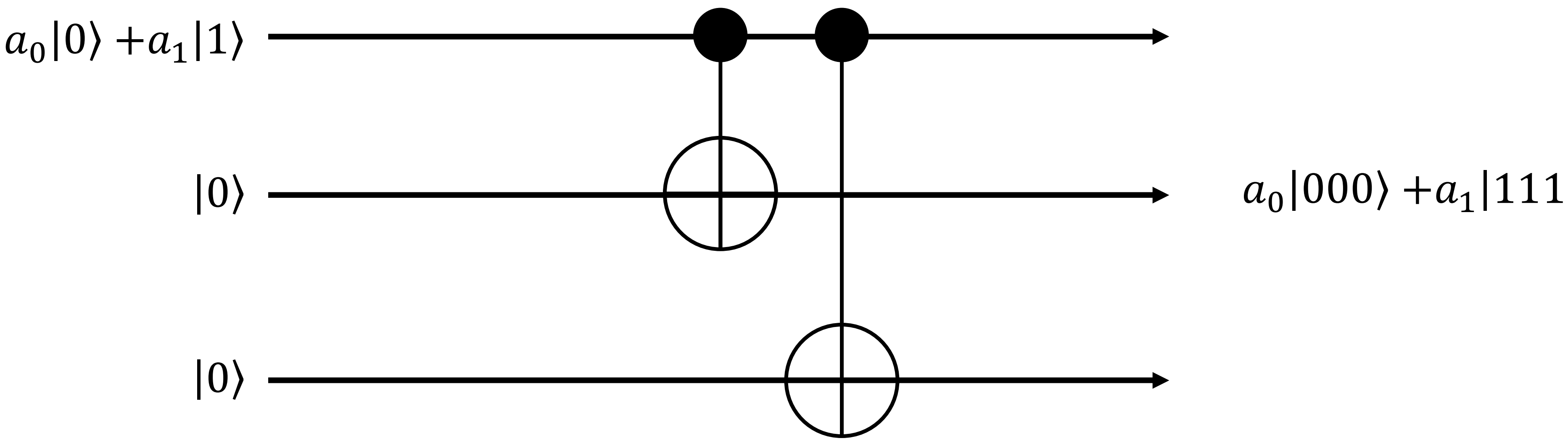
- The target input is $|y\rangle = a_0|00\rangle + a_1|11\rangle$
- The output is $|z\rangle = a_0|000\rangle + a_1|111\rangle$

Adding another CNOT



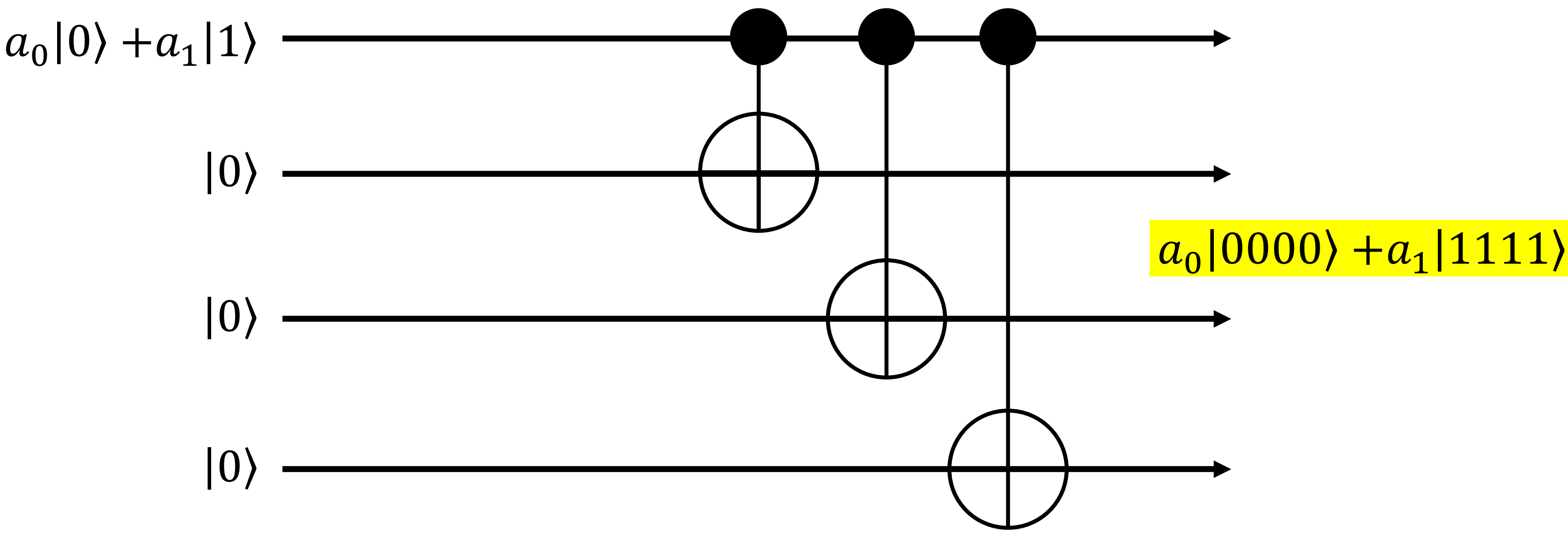
- The target input is $|y\rangle = a_0|00\rangle + a_1|11\rangle$
- The output is $|z\rangle = a_0|000\rangle + a_1|111\rangle$

Adding another CNOT



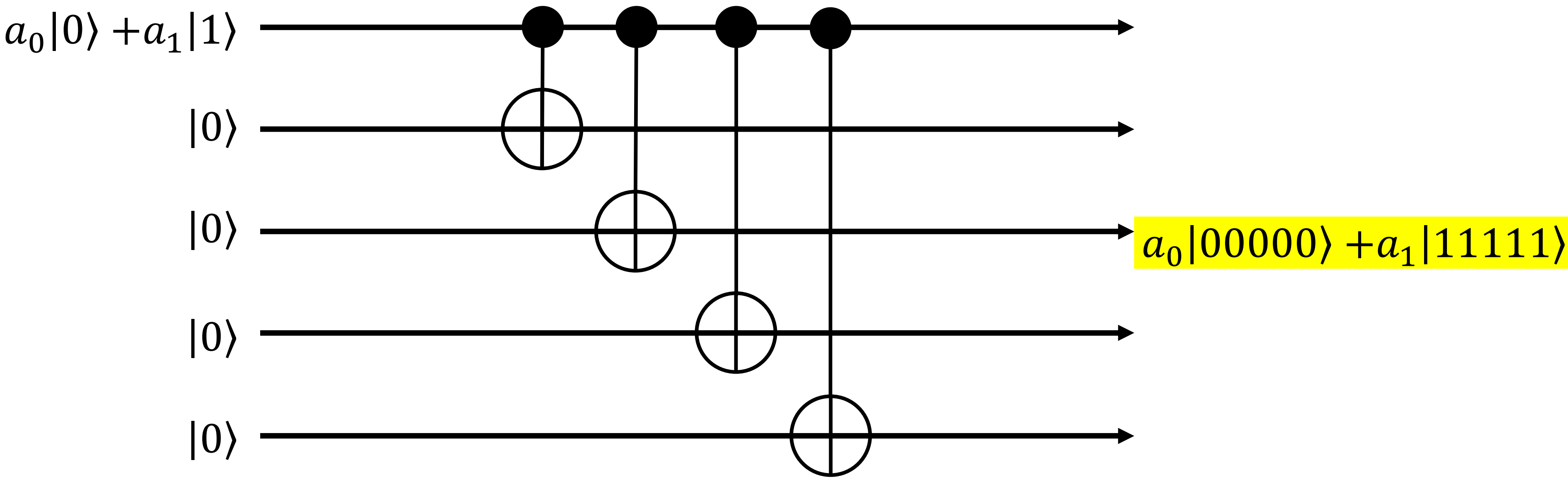
- The target input is $|y\rangle = a_0|00\rangle + a_1|11\rangle$
- The output is $|z\rangle = a_0|000\rangle + a_1|111\rangle$

Adding another CNOT



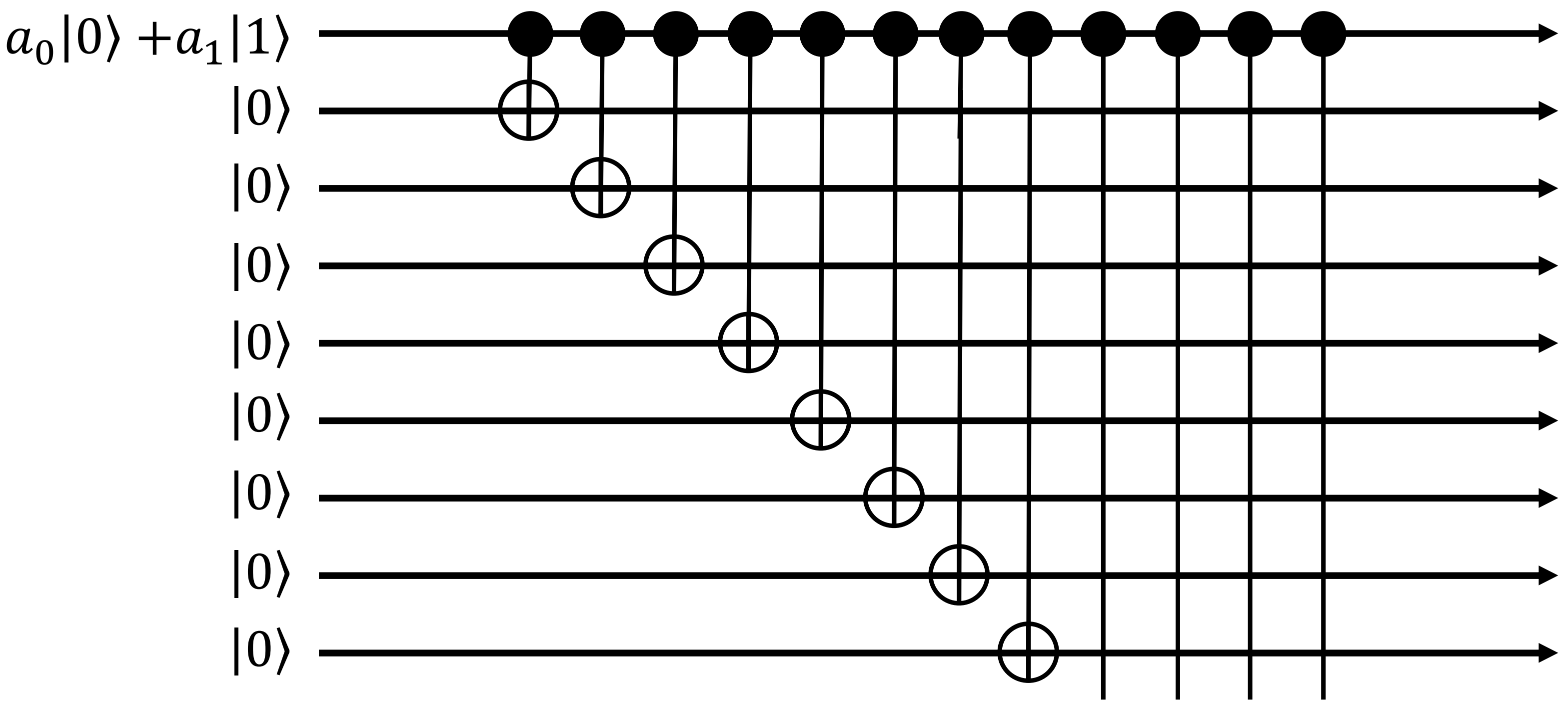
- The target input is $|z\rangle = a_0|000\rangle + a_1|111\rangle$
- The output is $|c\rangle = a_0|0000\rangle + a_1|1111\rangle$

Adding another CNOT



- The target input is $|c\rangle = a_0|0000\rangle + a_1|1111\rangle$
- The output is $|d\rangle = a_0|00000\rangle + a_1|11111\rangle$

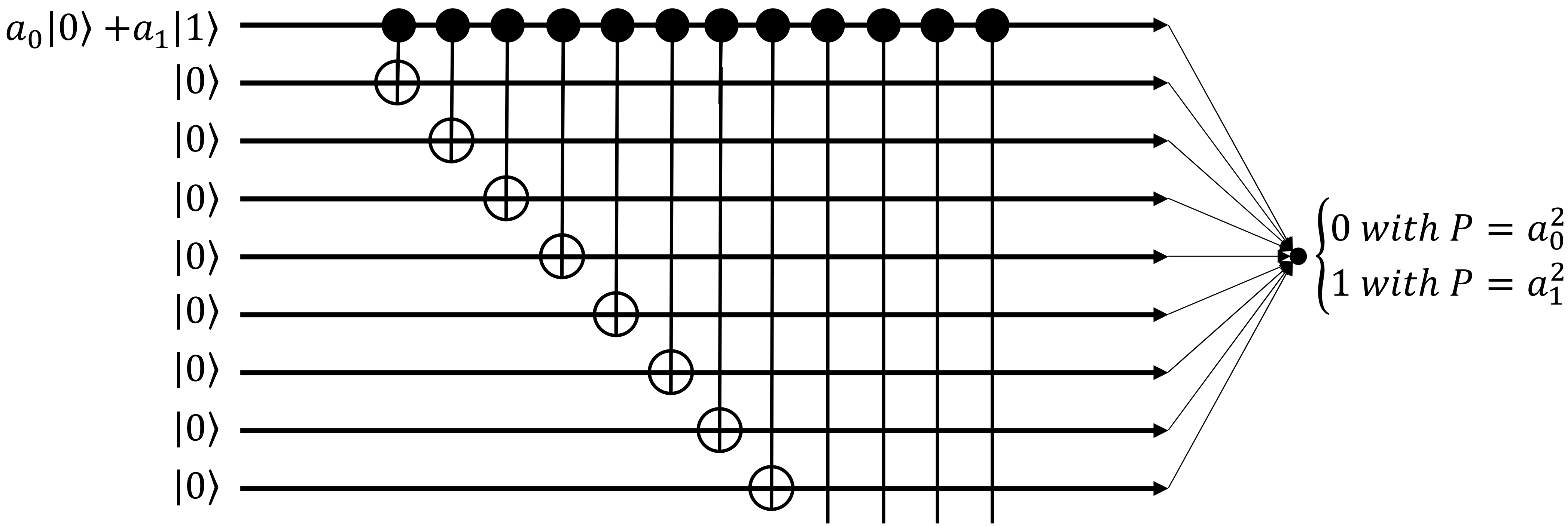
With sufficient addition we get…



- The output is

$$|o\rangle = a_0|000000 \dots 0\rangle + a_1|111111 \dots 1\rangle$$

With sufficient addition we get…



- The output is

$$|o\rangle = a_0|000000 \ldots 0\rangle + a_1|111111 \ldots 1\rangle$$

- Nature does not like quantum macroscopic objects
  - It will collapse this to either $|000000 \ldots 0\rangle$ with probability a_0^2 or $|111111 \ldots 1\rangle$ with probability a_1^2
- This gives us a measurement of 0 with P = a_0^2 and 1 with P = a_1^2

Measurement

- Previous example from Umesh Vazirani
- In general, measurement is more complex
  - But consists of composing macro quantum objects that will collapse
- More on this later
- Moving on...