# ※ Foundations 2b: Single Qubit Systems

*"Truth is simple yet purposely complex."*

- Wald Wassermann

A quantum algorithm comprises of three main components.

1. Storing quantum information (statevector)
2. Manipulating the stored quantum information (unitary transformations), and
3. Extracting a result (quantum measurement).

## 5.1 Storing Quantum Information

The smallest quantum system we can define is a single qubit.

**Definition 5.1** (Qubit)**.** A **qubit** is an object whose state can be represented by a unit vector $|\psi\rangle \in \mathbb{C}^2$.

As elements of a Hilbert space, any qubit should be expressible as a linear combination of some basis vectors. The first basis we will use is the standard basis.

**Example 5.2.** The **standard basis** of a single qubit is the set

$$\left\{ \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix} \right\}. \tag{23}$$

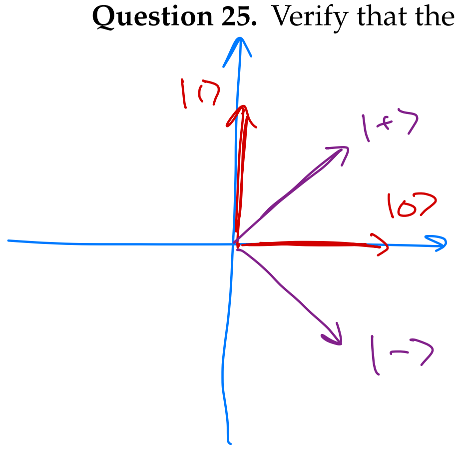
In braket notation, we will describe these vectors as $|0\rangle := \begin{bmatrix} 1 \\ 0 \end{bmatrix}$ and $|1\rangle := \begin{bmatrix} 0 \\ 1 \end{bmatrix}$.

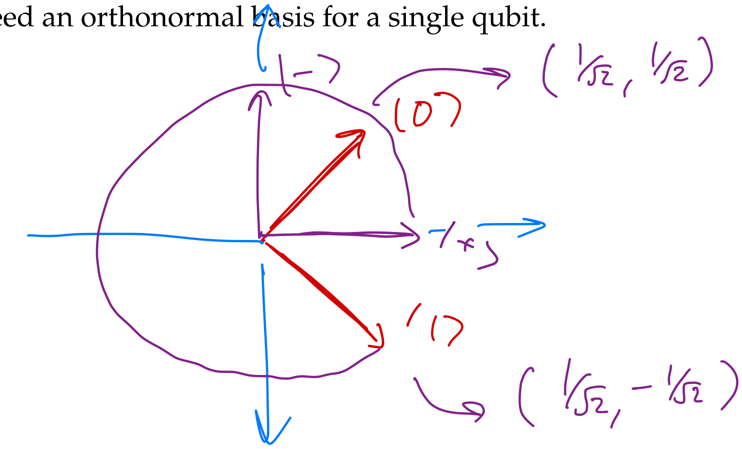
**Example 5.3.** The **Hadamard basis** is the set containing the following two vectors:

$$|+\rangle := \frac{1}{\sqrt{2}} |0\rangle + \frac{1}{\sqrt{2}} |1\rangle \,, \tag{24}$$

$$|-\rangle := \frac{1}{\sqrt{2}} |0\rangle - \frac{1}{\sqrt{2}} |1\rangle \,. \tag{25}$$

**Question 25.** Verify that the Hadamard basis is indeed an orthonormal basis for a single qubit.



Any state can be written in the Hadamard basis as well. This is equivalent to saying that there exist unique scalars $\alpha'$ and $\beta'$ such that

$$|\psi\rangle := \alpha\,|0\rangle + \beta\,|1\rangle = \alpha'\,|+\rangle + \beta'\,|-\rangle\,. \tag{26}$$

**Question 26.** Let $|\phi\rangle := \frac{1}{2}\,|0\rangle + \frac{\sqrt{3}}{2}\,|1\rangle$. Express $|\phi\rangle$ in the Hadamard basis.

$|0\rangle = \frac{1}{\sqrt{2}}|+\rangle + \frac{1}{\sqrt{2}}|-\rangle$ $\quad |1\rangle = \frac{1}{\sqrt{2}}|+\rangle - \frac{1}{\sqrt{2}}|-\rangle$

$\frac{1}{\sqrt{2}}\begin{bmatrix} 1/\sqrt{2} \\ 1/\sqrt{2} \end{bmatrix} + \frac{1}{\sqrt{2}}\begin{bmatrix} 1/\sqrt{2} \\ -1/\sqrt{2} \end{bmatrix} = \begin{bmatrix} \frac{1}{2}+\frac{1}{2} \\ \frac{1}{2}-\frac{1}{2} \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$ $\quad \frac{1+\sqrt{3}}{2\sqrt{2}} \quad \frac{1-\sqrt{3}}{2\sqrt{2}}$

$|\phi\rangle = \frac{1}{2}\left(\frac{1}{\sqrt{2}}|+\rangle + \frac{1}{\sqrt{2}}|-\rangle\right) + \frac{\sqrt{3}}{2}\left(\frac{1}{\sqrt{2}}|+\rangle - \frac{1}{\sqrt{2}}|-\rangle\right)$

Goal: $|\phi\rangle = \_\,|+\rangle + \_\,|-\rangle$

In the case of having more than one qubit, we can think of having a system that can be represented by a unit vector in $(\mathbb{C}^2)^{\otimes n}$, where the tensor power notation is shorthand for

$$(\mathbb{C}^2)^{\otimes n} := \mathbb{C}^2 \otimes \overset{n}{\cdots} \otimes \mathbb{C}^2 = \mathbb{C}^{2^n}\,. \tag{27}$$

**Example 5.4** (3 qubit system)**.** The **standard basis** for 3 qubits is the set of all combinations of the tensor product over single qubit standard basis states. For example, one such state is

$$|000\rangle := |0\rangle \otimes |0\rangle \otimes |0\rangle = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}. \tag{28}$$

$\underline{0}$ index is 1.

We like to abbreviate $\otimes$ when using braket notation if it isn't too confusing. Using this shorthand, the full set of standard basis states for 3 qubits is

$$\{|000\rangle\,, |001\rangle\,, |010\rangle\,, |011\rangle\,, |100\rangle\,, |101\rangle\,, |110\rangle\,, |111\rangle\}. \tag{29}$$

We will also often write these states as

$$\{|0\rangle\,, |1\rangle\,, |2\rangle\,, |3\rangle\,, |4\rangle\,, |5\rangle\,, |6\rangle\,, |7\rangle\}. \tag{30}$$

## 5.2 Transforming Quantum Systems

A quantum state should only be transformed into another quantum state. By our definition, this means that the transformation should preserve the L2-norm, and it should also be linear. An operation that satisfies these properties is called **unitary**, and every unitary transformation can be represented by a **unitary matrix**. This is the family of "quantum gates" we will be using throughout this course.

**Question 27.** Suppose we have a qubit in the following state:

$$\hookrightarrow \quad |\psi\rangle = \begin{bmatrix} 1/\sqrt{2} \\ i/\sqrt{2} \end{bmatrix} \tag{31}$$

and we have a unitary whose action is represented by the matrix

$$\hookrightarrow \quad A = \begin{bmatrix} \frac{1}{2} & \frac{i\sqrt{3}}{2} \\ -\frac{\sqrt{3}}{2} & \frac{i}{2} \end{bmatrix} \tag{32}$$

What is the state of our system after $A$ is applied to $|\psi\rangle$?

$$A|\psi\rangle = \begin{bmatrix} 1/2 & i\sqrt{3}/2 \\ -\sqrt{3}/2 & i/2 \end{bmatrix}\begin{bmatrix} 1/\sqrt{2} \\ i/\sqrt{2} \end{bmatrix} = \begin{bmatrix} \frac{1}{2\sqrt{2}} - \frac{\sqrt{3}}{2\sqrt{2}} \\ -\frac{\sqrt{3}}{2\sqrt{2}} - \frac{1}{2\sqrt{2}} \end{bmatrix} = \begin{bmatrix} \frac{1-\sqrt{3}}{2\sqrt{2}} \\ \frac{-1-\sqrt{3}}{2\sqrt{2}} \end{bmatrix}$$

**Definition 5.5** (Adjoint)**.** The **adjoint** $A^\dagger$ (read "A dagger") of a matrix $A$ is the matrix you get after transposing $A$ and taking the complex conjugate of each element. This process is also referred to as taking the **conjugate transpose** of a matrix.

**Question 28.** What is the adjoint of $A$? Calculate $\boxed{\langle \overset{\psi}{\cancel{\phi}}| A^\dagger}$ and $\boxed{\langle \overset{\psi}{\cancel{\phi}}|A^\dagger A|\overset{\psi}{\cancel{\phi}}\rangle}$.

$$\langle\psi|A^\dagger = \begin{bmatrix} 1/\sqrt{2} & -i/\sqrt{2} \end{bmatrix}\begin{bmatrix} 1/2 & -\sqrt{3}/2 \\ -\frac{i\sqrt{3}}{2} & -i/2 \end{bmatrix} = \begin{bmatrix} \frac{1}{2\sqrt{2}} - \frac{\sqrt{3}}{2\sqrt{2}} & -\frac{\sqrt{3}}{2\sqrt{2}} - \frac{1}{2\sqrt{2}} \end{bmatrix}$$

$$(\langle\psi|A^\dagger)(A|\psi\rangle) = 1$$

One of the most basic unitary matrices that will show up is the **identity matrix**. This is the matrix with ones on its diagonals and zeros everywhere else. We will use $I_n$ to denote the $n \times n$ identity matrix.

Let's see a consequence of requiring an operator $U$ to be norm-preserving when applied to a quantum state. We can write this condition mathematically as

$$\| |\psi\rangle \|_2 = 1 \to \|U |\psi\rangle \|_2 = 1, \tag{33}$$

which we know can alternatively be written as

gate2 start state.

$$\langle\psi|\psi\rangle = 1 \to \langle\psi\boxed{|U^\dagger U|\psi\rangle} = 1. \tag{34}$$

$= |\psi\rangle$

gate

An important consequence of this fact is that all quantum operations are **reversible**. For any starting state $|\psi\rangle$ and norm preserving operation $U$, we can find the inverse operator $U^\dagger$ which is simply the adjoint of $U$.

**Question 29.** Are classical operations reversible? If not, describe an operation that is not reversible.

$f(x) = 0$ No

**Definition 5.6.** A matrix $U$ is a **unitary matrix** if any of the following equivalent definitions are true.

- $U$ is norm-preserving.
- $U$ preserves inner products (inner product of $|\psi\rangle$ and $|\phi\rangle$ is equal to the inner product of $U|\psi\rangle$ and $U|\phi\rangle$.
- $U^\dagger U = UU^\dagger = I$.
- Rows of $U$ form an orthonormal basis.
- Columns of $U$ form an orthonormal basis.

**Question 30.** Prove that all of the above definitions for a unitary matrix are equivalent.

## 5.3 Single Qubit Operations

Here we will look at examples of important single qubit operators.

**Question 31.** Determine the action of the following single qubit operators on the standard basis states. What about their action on a state in superposition, $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$? Hadamard basis

$$\rightarrow \quad 1)\ I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad 2) \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad 3) \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \quad 4) \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \quad 5)\ H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \tag{35}$$

1) Nothing! Identity.

2) S.B.: Bit flip/negation. NOT $\rightarrow$ X

3) S.B.: Negate value of amp. $\beta$. / H.B. "bit flip"

4) Does (2) and (3) then multiplies by $i$

5) $|0\rangle \xrightarrow{H} |+\rangle$
$|1\rangle \xrightarrow{H} |-\rangle$

$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$

$|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

$|+\rangle \Leftrightarrow |-\rangle$

The final operator we looked at in the previous question is called the **Hadamard gate** $H$. It serves the important function of transitioning between the standard and Hadamard basis. It also is a good gate for us to see our first example of **negative interference**.

**Question 32.** What is the adjoint of the Hadamard gate? Verify this by computing $H^\dagger H|0\rangle$.

$$H^\dagger = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = H$$

Let's use the previous question to see how we draw quantum circuits.

$$|0\rangle - \boxed{H} - \boxed{H^\dagger} -$$

$H^\dagger H|0\rangle$

$$|1\rangle - - \boxed{X} -$$

The starting state of each qubit is written on the left, and the sequence of gates we apply goes from left to right.

**Definition 5.7** (Important Single Qubit Gates)**.** The following gates will appear frequently throughout this course and are standard in the literature.

- Hadamard gate: $H := \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$.
- Pauli gates:

$$X := \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad Y := \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \quad Z := \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \tag{36}$$

**Question 33.** What is the state of the qubit at the end of this circuit?

$$|0\rangle \text{—} \boxed{H} \text{—} \boxed{Y} \text{—}$$

Remember that since a qubit is a unit vector, if we know it has real amplitudes, it is a vector on the unit circle of the plane. This motivates the following standard gate we will be using as well.

**Definition 5.8** (Rotation gate)**.** The rotation gate $R_\theta$ is a parameterized gate defined as

$$R_\theta := \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}. \tag{37}$$

**Question 34.** Verify that the rotation gate is indeed unitary.

$$R_\theta^\dagger R_\theta = \begin{bmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{bmatrix} \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} = \begin{bmatrix} c^2\theta + s^2\theta & \cancel{-cs+cs} \\ \cancel{-cs} + cs & s^2+c^2 \end{bmatrix}$$

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

**Question 35.** Compute the following:

- $R_{\pi/4}\,|0\rangle$
- $R_{\pi/4}\,|+\rangle$
- $R_{\pi/4}\,|1\rangle$
- $R_{\pi/4}\,|-\rangle$

You may need the fact that, $\cos(\pi/4) = \sin(\pi/4) = \frac{1}{\sqrt{2}}$.

Let's now look at the full family of single qubit states where we allow complex amplitudes. In your homework, you observed that multiplying a state by a **global phase** does not change the probability of observing an outcome. That is, multiplying both amplitudes by the same complex number $e^{i\theta}$ didn't change the measurement probabilities.

Things get more interesting when we consider **relative phases**. These are phases that are applied separately to each amplitude, through transformations that might look like

$$\alpha |0\rangle + \beta |1\rangle \to \alpha |0\rangle + \beta e^{i\theta} |1\rangle . \tag{38}$$

**Question 36.** The Hadamard basis states can be written as two states that differ by a relative phase:

$$|+\rangle = \frac{1}{\sqrt{2}} |0\rangle + \frac{1}{\sqrt{2}} |1\rangle \tag{39}$$

$$|-\rangle = \frac{1}{\sqrt{2}} |0\rangle + e^{i\pi} \frac{1}{\sqrt{2}} |1\rangle . \tag{40}$$

What is the probability of measuring $|0\rangle$ and $|1\rangle$ for each of these states? What if we apply the $H$ gate first to each state and then measure?

The above question highlights that relative phase is different from global phase, and can actually be detected. It seems then, that the most general way to express the state of a qubit is something like the following, where $m_0, m_1, \phi_0, \phi_1 \in \mathbb{R}$:

$$|\psi\rangle := m_0 e^{i\pi\phi_0} |0\rangle + m_1 e^{i\pi\phi_1} |1\rangle . \tag{41}$$

Thus we have found a four variable parameterization of a qubit. However, we only have two real constraints for a qubit state:

1. The $L_2$-norm is 1.

2. The global phase does not matter.

**Question 37.** Use the constraint of the $L2$ norm to express $m_0$ and $m_1$ using a single parameter.

**Question 38.** Use the constraint on the global phase factor to express $\phi_0$ and $\phi_1$ using a single parameter.

**Lemma 5.9** (Parameterization of a qubit)**.**

We can sum up the important properties of quantum operations as follows:

1. **Reversible.** By unitarity, any operation $U$ has a reverse operation $U^\dagger$.
2. **Deterministic.** The action of a unitary $U$ is well defined.
3. **Continuous.** Any unitary $U$ can be performed "half-way".

$\sqrt[1072]{Z}$

**Question 39.** Find the "half-way" unitary operator of $Z$. That is, find the unitary $U$ such that $U \cdot U = Z$.

$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \qquad D = \begin{bmatrix} d_0 & 0 \\ 0 & d_1 \end{bmatrix}$$

$$U = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} \qquad D^2 = \begin{bmatrix} d_0 & 0 \\ 0 & d_1 \end{bmatrix}\begin{bmatrix} d_0 & 0 \\ 0 & d_1 \end{bmatrix}$$

$$= \begin{bmatrix} d_0^2 & 0 \\ 0 & d_1^2 \end{bmatrix}$$

## 5.4 Single Qubit Measurements

The final piece of quantum algorithms we need to formalize are quantum measurements. In contrast to the properties that transformations had, quantum measurements have the exact opposite properties.

1. **Irreversible**. Once a measurement is performed, there is no way to recover the state before without rerunning the entire algorithm.
2. **Probabilistic**. The probability of observing an outcome is the squared norm of the amplitude corresponding to that outcome.
3. **Discrete**. Measurement results are inherently discrete.

Up until know, all measurements I described were performed in the **standard basis**. However, it turns out that we can measure in any basis we like! If you fix a basis, every qubit has a unique representation in that basis.

**Example 5.10.** Consider the Hadamard basis $|+\rangle, |-\rangle$. Suppose we have a state $|\psi\rangle := \alpha|0\rangle + \beta|1\rangle$. We can express this state in the Hadamard basis with another pair of amplitudes $\alpha'$ and $\beta'$ as

$$|\psi\rangle = \alpha'|+\rangle + \beta'|-\rangle. \tag{42}$$

Measuring in a different basis affects the measurement outcomes. If we measure in the standard basis, $\{|0\rangle, |1\rangle\}$:

1. $|0\rangle$ with probability $|\langle 0|\psi\rangle|^2 = |\alpha|^2$, and
2. $|1\rangle$ with probability $|\langle 1|\psi\rangle|^2 = |\beta|^2$.

$$\langle 0|\psi\rangle = \langle 0|(\alpha|0\rangle + \beta|1\rangle)$$
$$= \langle 0|\alpha|0\rangle + \langle 0|\beta|1\rangle$$
$$= \alpha\langle 0|0\rangle + \beta\langle 0|1\rangle = \alpha.$$

If we measure in the Hadamard basis, $\{|+\rangle, |-\rangle\}$:

1. $|+\rangle$ with probability $|\langle +|\psi\rangle|^2 = |\alpha'|^2$, and
2. $|-\rangle$ with probability $|\langle -|\psi\rangle|^2 = |\beta'|^2$.

$$\langle -|\psi\rangle = \langle -|(\alpha'|+\rangle + \beta'|-\rangle)$$
$$= \alpha'\langle -|+\rangle + \beta'\langle -|-\rangle$$
$$= \beta'$$

**Question 40.** What are the outcomes and corresponding probabilities if we measure $|1\rangle$ in the standard basis? What about in the Hadamard basis?

Bra "picks out" the coefficient in that basis.

The standard basis and Hadamard basis are a pair of **complementary bases.** This means that if you are certain that the state is in $|+\rangle$ or $|-\rangle$, you will be maximally *uncertain* of the state in the standard basis, and vice versa. Another way to think of unitary matrices is that they are a transformation between two orthonormal bases. For example, the Hadamard basis is a transformation between the standard and Hadamard bases.

$$|+\rangle \overset{H}{\leftrightarrow} |0\rangle \tag{43}$$

$$|-\rangle \overset{H}{\leftrightarrow} |1\rangle \tag{44}$$

A useful consequence of this is that if we want to simulate a measurement in the Hadamard basis, we can apply the Hadamard gate and then measure in the standard basis. Let's now define measurements formally.

**Definition 5.11** (Measurements)**.** Let $|\psi\rangle \in \mathbb{C}^N$ be a quantum state on $n$ qubits and $\{|v_1\rangle, \ldots, |v_N\rangle\}$ be an orthonormal basis. If we measure in this basis, we will see outcome $|v_i\rangle$ with probability $|\langle v_i|\psi\rangle|^2$, and the state collapses to $|v_i\rangle$.

$|+\rangle = H|0\rangle$

$\langle +| = \langle 0|H^\dagger = \langle 0|H$

$\langle +|\psi\rangle$

$\hookrightarrow (\langle 0|H)|\psi\rangle$

$= \langle 0|(H|\psi\rangle)$ → What's the prob. of seeing $\langle 0|$ given state $H|\psi\rangle$

## 5.5 Distinguishing non-orthogonal states

Sometimes, we are interested in distinguishing outcomes of an experiment where the possible results are not necessarily orthogonal. This arises frequently in quantum computing with our limited capabilities of combating noise.

Consider the following experiment. We are running a simulation on a quantum device, which in theory should measure $|0\rangle$ with probability 1. However, there is some external noise affecting our system such that $1/2$ of the time the experiment will end in the state $|+\rangle$ instead. In this case, we will say the experiment "failed". Can we effectively distinguish a failed experiment from a successful experiment?

**Question 41.** What are the probabilities and outcomes when we measure a successful vs. failed experiment in the standard basis?

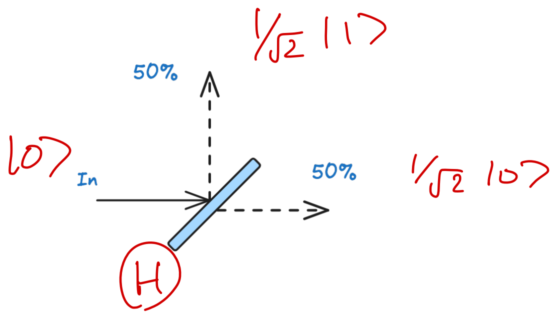
**Question 42.** What are the probabilities and outcomes when we measure a successful vs. failed experiment in the Hadamard basis?

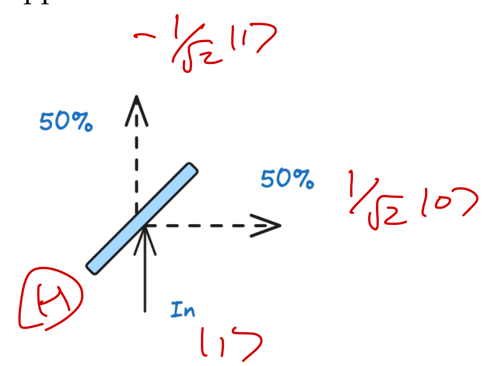
**Question 43.** There is no measurement that can be performed which can distinguish these outcomes perfectly. Is there a basis we can measure in that will do better than the previous two bases?

## 5.6 Beam Splitters

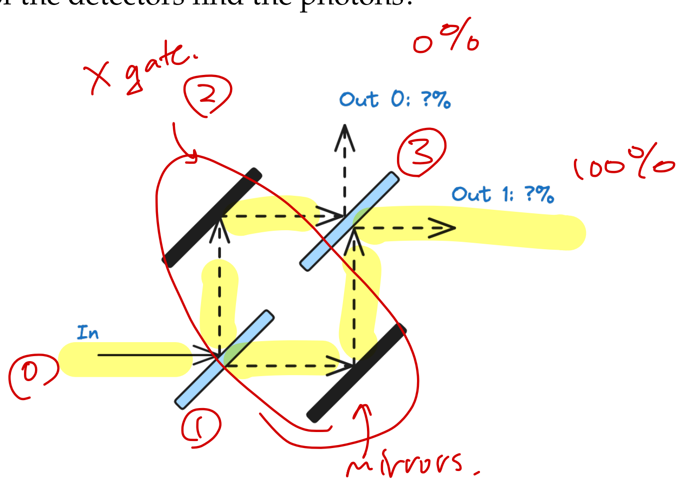
$\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

A **beam splitter** is a device which is used to split of beam of light into two. This works even if a single photon is fired, and the measurement statistics will be correctly reproduced! If we place a photon detector at the two possible directions the photon goes after it is split, we will detect the photon with probability 1/2 at each location. The same thing happens if we fire it from the perpendicular direction!




**Question 44.** What would you expect the outcome of the following setup to be? That is, with what probabilities will each of the detectors find the photons?




(0) $|0\rangle$

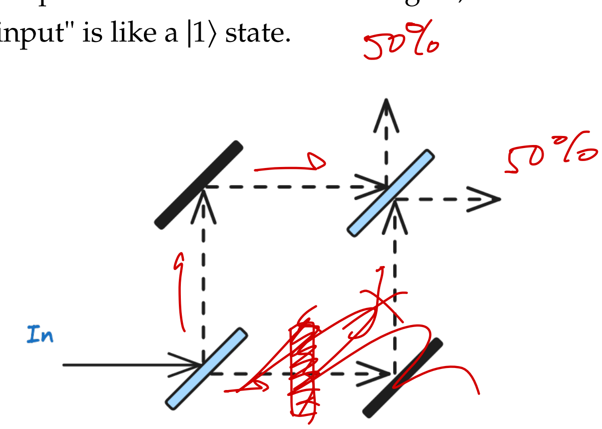
(1) $\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$

(2) $\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$

(3) $H\left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right)$

$= H|+\rangle = |0\rangle$

It turns out that the beam splitter acts like a Hadamard gate, and the horizontal "input" is like a $|0\rangle$ state, and the vertical "input" is like a $|1\rangle$ state.

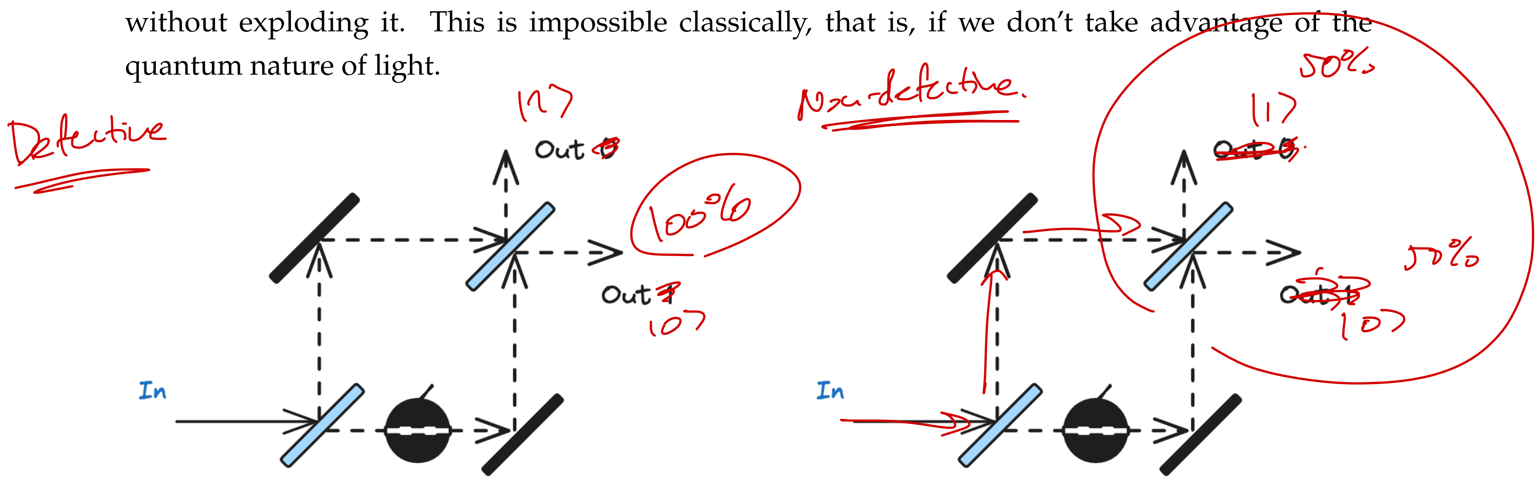


## 5.7 Elitzur-Vaidman Bombs

Consider the following thought experiment. Suppose that we had a bomb that we can fire a photon through which has the following properties:

- If the bomb is not defective, the photon gets detected, and the bomb explodes.
- If the bomb is defective, the photon passes undetected, and the bomb does not explode.

Suppose we have many of these bombs and would like to find one which is not defective without exploding it. This is impossible classically, that is, if we don't take advantage of the quantum nature of light.




50%, bomb explodes, photon is gone

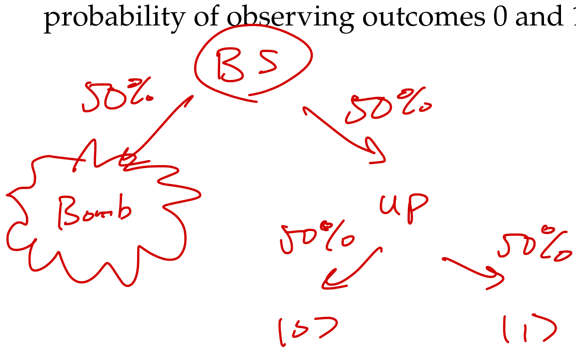
**Question 45.** What is the probability of observing each outcome if the bomb is defective?

Basically B.S. experiment w/ no block.

→ |0⟩ → 100%

|1⟩ → 0%

**Question 46.** What is the probability the bomb explodes if the bomb is not defective? What is the probability of observing outcomes 0 and 1 if the bomb is not defective and it doesn't explode?




50% → explode

25% → |0⟩

25% → |1⟩

We can also describe this scenario using a quantum circuit, and creating a special gate to represent the bomb. We will define the gate $B$ as follows:

- If the bomb is defective, it is just an identity gate $I$.
- If the bomb is not defective, measure in the standard basis. If $|0\rangle$ is observed, keep going. If $|1\rangle$ is observed, the bomb explodes.