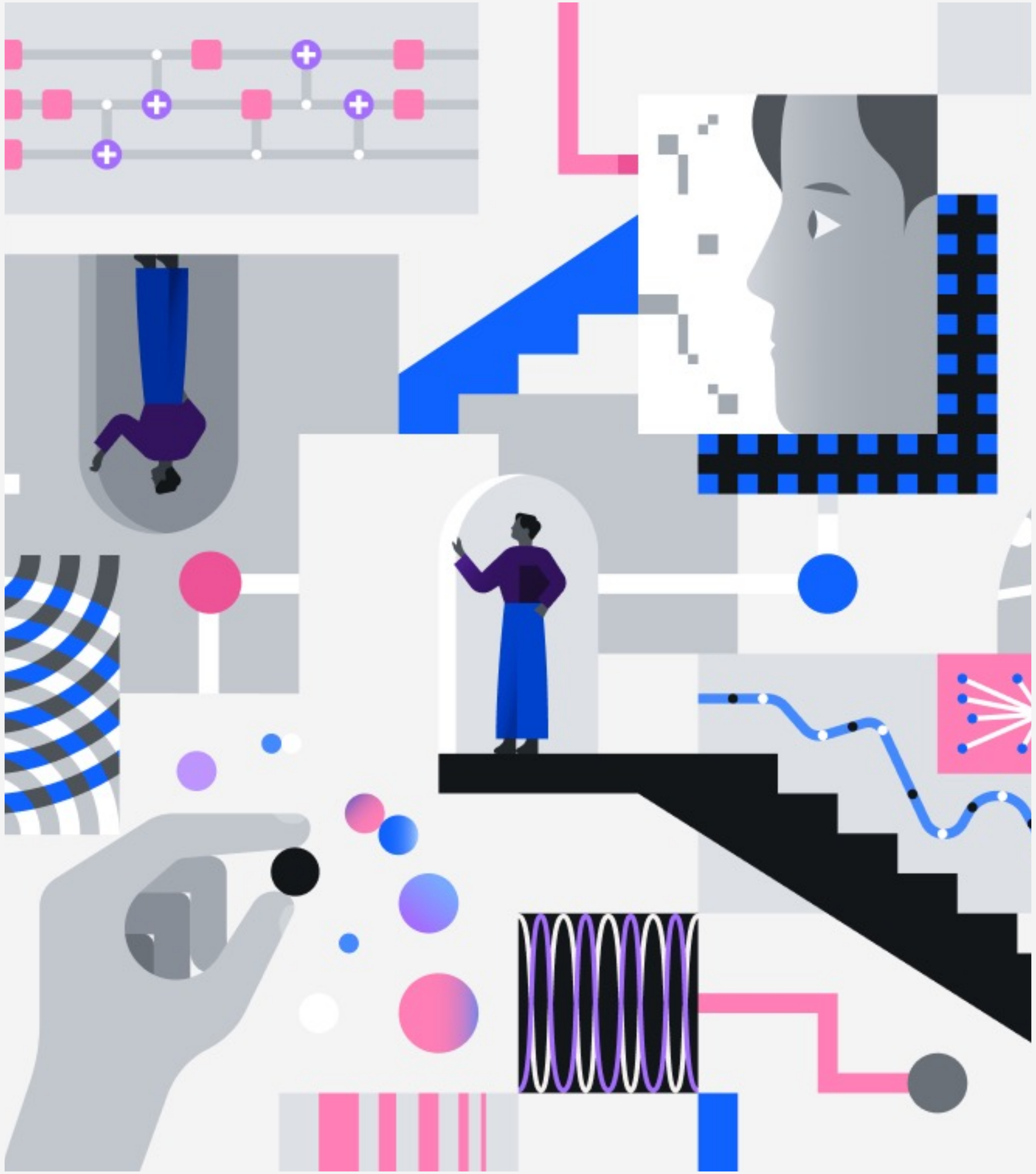
Understanding quantum information and computation

By John Watrous

Lesson 1

Single systems



Descriptions of quantum information

Simplified description (this unit)

- Simpler and typically learned first
- Quantum states represented by *vectors;* operations are represented by *unitary matrices*
- Sufficient for an understanding of most quantum algorithms

General description (covered in a later unit)

- More general and more broadly applicable
- Quantum states represented by *density matrices;* allows for a more general class of measurements and operations
- Includes both the simplified description and classical information (including probabilistic states) as special cases

Classical information

Consider a physical system that stores information: let us call it X.

Assume X can be in one of a finite number of *classical states* at each moment. Denote this classical state set by Σ.

Examples

- If X is a bit, then its classical state set is $\Sigma = \{0, 1\}$.
- If X is a six-sided die, then $\Sigma = \{1, 2, 3, 4, 5, 6\}$.
- If X is a switch on a standard electric fan, then perhaps $\Sigma = \{\text{high}, \text{medium}, \text{low}, \text{off}\}$.

There there may be *uncertainty* about the classical state of a system, where each classical state has some *probability* associated with it.

Classical information

For example, if X is a bit, then perhaps it is in the classical state 0 with probability 3/4 and in the classical state 1 with probability 1/4. This is a *probabilistic state* of X.

$$\Pr(X = 0) = \frac{3}{4} \quad \text{and} \quad \Pr(X = 1) = \frac{1}{4}$$

A succinct way to represent this probabilistic state is by a *column vector:*

$$\begin{pmatrix} \frac{3}{4} \\ \frac{1}{4} \end{pmatrix} \begin{array}{l} \longleftarrow \text{entry corresponding to 0} \\ \longleftarrow \text{entry corresponding to 1} \end{array}$$

This vector is a *probability vector:*

- All entries are nonnegative real numbers.
- The sum of the entries is 1.

Dirac notation (first part)

Let Σ be any classical state set, and assume the elements of Σ have been placed in correspondence with the integers $1, \ldots, |\Sigma|$.

We denote by $|a\rangle$ the *column vector* having a 1 in the entry corresponding to $a \in \Sigma$, with 0 for all other entries.

Example 1

If $\Sigma = \{0, 1\}$, then

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad \text{and} \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

Dirac notation (first part)

Let Σ be any classical state set, and assume the elements of Σ have been placed in correspondence with the integers $1, \ldots, |\Sigma|$.

We denote by $|a\rangle$ the *column vector* having a 1 in the entry corresponding to $a \in \Sigma$, with 0 for all other entries.

Example 2

If $\Sigma = \{\clubsuit, \diamondsuit, \heartsuit, \spadesuit\}$, then we might choose to order these states like this: $\clubsuit, \diamondsuit, \heartsuit, \spadesuit$. This yields

$$|\clubsuit\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \qquad |\diamondsuit\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \qquad |\heartsuit\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \qquad |\spadesuit\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

Dirac notation (first part)

Let Σ be any classical state set, and assume the elements of Σ have been placed in correspondence with the integers $1, \ldots, |\Sigma|$.

We denote by $|a\rangle$ the *column vector* having a 1 in the entry corresponding to $a \in \Sigma$, with 0 for all other entries.

Vectors of this form are called *standard basis vectors.* Every vector can be expressed uniquely as a linear combination of standard basis vectors.

Example

$$\begin{pmatrix} \frac{3}{4} \\ \frac{1}{4} \end{pmatrix} = \frac{3}{4}\,|0\rangle + \frac{1}{4}\,|1\rangle$$

Measuring probabilistic states

What happens if we *measure* a system X while it is in some probabilistic state?

We see a *classical state,* chosen at random according to the probabilities.

Suppose we see the classical state $a \in \Sigma$.

This changes the probabilistic state of X (from our viewpoint): having recognized that X is in the classical state a, we now have

$$\Pr(\mathsf{X} = a) = 1$$

This probabilistic state is represented by the vector $|a\rangle$.

Measuring probabilistic states

Example

Consider the probabilistic state of a bit X where

$$\Pr(X = 0) = \frac{3}{4} \quad \text{and} \quad \Pr(X = 1) = \frac{1}{4}$$

Measuring X selects (or reveals) a transition, chosen at random:

$$\begin{tikzcd}
& \frac{3}{4}\,|0\rangle + \frac{1}{4}\,|1\rangle \arrow[dl, "\text{probability } \frac{3}{4}"'] \arrow[dr, "\text{probability } \frac{1}{4}"] & \\
|0\rangle & & |1\rangle
\end{tikzcd}$$

Deterministic operations

Every function $f : \Sigma \to \Sigma$ describes a *deterministic operation* that transforms the classical state a into $f(a)$, for each $a \in \Sigma$.

Given any function $f : \Sigma \to \Sigma$, there is a (unique) matrix M satisfying

$$M|a\rangle = |f(a)\rangle \qquad \text{(for every } a \in \Sigma\text{)}$$

This matrix has exactly one 1 in each column, and 0 for all other entries:

$$M(b, a) = \begin{cases} 1 & b = f(a) \\ 0 & b \neq f(a) \end{cases}$$

The action of this operation is described by *matrix-vector multiplication:*

$$v \longmapsto Mv$$

Deterministic operations

Example

For $\Sigma = \{0, 1\}$, there are four functions of the form $f : \Sigma \to \Sigma$:

a	$f_1(a)$
0	0
1	0

a	$f_2(a)$
0	0
1	1

a	$f_3(a)$
0	1
1	0

a	$f_4(a)$
0	1
1	1

Here are the matrices corresponding to these functions:

$$M_1 = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \quad M_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad M_3 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad M_4 = \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}$$

$$M(b, a) = \begin{cases} 1 & b = f(a) \\ 0 & b \neq f(a) \end{cases}$$

$$M\,|a\rangle = |f(a)\rangle$$

Dirac notation (second part)

Let Σ be any classical state set, and assume the elements of Σ have been placed in correspondence with the integers $1, \ldots, |\Sigma|$.

We denote by $\langle a |$ the *row vector* having a 1 in the entry corresponding to $a \in \Sigma$, with 0 for all other entries.

Example

If $\Sigma = \{0, 1\}$, then

$$\langle 0| = \begin{pmatrix} 1 & 0 \end{pmatrix} \quad \text{and} \quad \langle 1| = \begin{pmatrix} 0 & 1 \end{pmatrix}$$

Dirac notation (second part)

Let Σ be any classical state set, and assume the elements of Σ have been placed in correspondence with the integers $1, \ldots, |\Sigma|$.

We denote by $\langle a|$ the *row vector* having a 1 in the entry corresponding to $a \in \Sigma$, with 0 for all other entries.

Multiplying a row vector to a column vector yields a scalar:

$$\begin{pmatrix} * & * & * & \cdots & * \end{pmatrix} \begin{pmatrix} * \\ * \\ * \\ \vdots \\ * \end{pmatrix} = \begin{pmatrix} * \end{pmatrix}$$

$$\langle a|b\rangle = \langle a||b\rangle = \begin{cases} 1 & a = b \\ 0 & a \neq b \end{cases}$$

Dirac notation (second part)

Let Σ be any classical state set, and assume the elements of Σ have been placed in correspondence with the integers $1, \ldots, |\Sigma|$.

We denote by $\langle a|$ the *row vector* having a 1 in the entry corresponding to $a \in \Sigma$, with 0 for all other entries.

Multiplying a row vector to a column vector yields a scalar:

$$\begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \end{pmatrix}$$

$$\langle a|b\rangle = \langle a||b\rangle = \begin{cases} 1 & a = b \\ 0 & a \neq b \end{cases}$$

Dirac notation (second part)

Let Σ be any classical state set, and assume the elements of Σ have been placed in correspondence with the integers $1, \ldots, |\Sigma|$.

We denote by $\langle a|$ the *row vector* having a 1 in the entry corresponding to $a \in \Sigma$, with 0 for all other entries.

Multiplying a row vector to a column vector yields a scalar:

$$\begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \end{pmatrix}$$

$$\langle a|b\rangle = \langle a||b\rangle = \begin{cases} 1 & a = b \\ 0 & a \neq b \end{cases}$$

Dirac notation (second part)

Let Σ be any classical state set, and assume the elements of Σ have been placed in correspondence with the integers $1, \ldots, |\Sigma|$.

We denote by $\langle a|$ the *row vector* having a 1 in the entry corresponding to $a \in \Sigma$, with 0 for all other entries.

Multiplying a column vector to a row vector yields a matrix:

$$\begin{pmatrix} * \\ * \\ * \\ \vdots \\ * \end{pmatrix} \begin{pmatrix} * & * & * & \cdots & * \end{pmatrix} = \begin{pmatrix} * & * & * & \cdots & * \\ * & * & * & \cdots & * \\ * & * & * & \cdots & * \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ * & * & * & \cdots & * \end{pmatrix}$$

Dirac notation (second part)

Multiplying a column vector to a row vector yields a matrix:

$$\begin{pmatrix} * \\ * \\ * \\ \vdots \\ * \end{pmatrix} \begin{pmatrix} * & * & * & \cdots & * \end{pmatrix} = \begin{pmatrix} * & * & * & \cdots & * \\ * & * & * & \cdots & * \\ * & * & * & \cdots & * \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ * & * & * & \cdots & * \end{pmatrix}$$

Example

$$|0\rangle\langle 0| = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

Dirac notation (second part)

Multiplying a column vector to a row vector yields a matrix:

$$\begin{pmatrix} * \\ * \\ * \\ \vdots \\ * \end{pmatrix} \begin{pmatrix} * & * & * & \cdots & * \end{pmatrix} = \begin{pmatrix} * & * & * & \cdots & * \\ * & * & * & \cdots & * \\ * & * & * & \cdots & * \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ * & * & * & \cdots & * \end{pmatrix}$$

Example

$$|0\rangle\langle 1| = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

Dirac notation (second part)

Multiplying a column vector to a row vector yields a matrix:

$$\begin{pmatrix} * \\ * \\ * \\ \vdots \\ * \end{pmatrix} \begin{pmatrix} * & * & * & \cdots & * \end{pmatrix} = \begin{pmatrix} * & * & * & \cdots & * \\ * & * & * & \cdots & * \\ * & * & * & \cdots & * \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ * & * & * & \cdots & * \end{pmatrix}$$

Example

$$|1\rangle\langle 0| = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$$

Dirac notation (second part)

Multiplying a column vector to a row vector yields a matrix:

$$\begin{pmatrix} * \\ * \\ * \\ \vdots \\ * \end{pmatrix} \begin{pmatrix} * & * & * & \cdots & * \end{pmatrix} = \begin{pmatrix} * & * & * & \cdots & * \\ * & * & * & \cdots & * \\ * & * & * & \cdots & * \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ * & * & * & \cdots & * \end{pmatrix}$$

Example

$$|1\rangle\langle 1| = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

Dirac notation (second part)

Multiplying a column vector to a row vector yields a matrix:

$$\begin{pmatrix} * \\ * \\ * \\ \vdots \\ * \end{pmatrix} \begin{pmatrix} * & * & * & \cdots & * \end{pmatrix} = \begin{pmatrix} * & * & * & \cdots & * \\ * & * & * & \cdots & * \\ * & * & * & \cdots & * \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ * & * & * & \cdots & * \end{pmatrix}$$

In general, the matrix

$$|a\rangle\langle b|$$

has a 1 in the (a, b)-entry and 0 for all other entries.

Deterministic operations

Every function $f : \Sigma \rightarrow \Sigma$ describes a *deterministic operation* that transforms the classical state a into $f(a)$, for each $a \in \Sigma$.

Given any function $f : \Sigma \rightarrow \Sigma$, there is a (unique) matrix M satisfying

$$M\,|a\rangle = |f(a)\rangle \qquad \text{(for every } a \in \Sigma)$$

This matrix may be expressed as

$$M = \sum_{b \in \Sigma} |f(b)\rangle\langle b|$$

Its action on standard basis vectors works as required:

$$M|a\rangle = \left(\sum_{b \in \Sigma} |f(b)\rangle\langle b|\right)|a\rangle = \sum_{b \in \Sigma} |f(b)\rangle\langle b|a\rangle = |f(a)\rangle$$

Probabilistic operations

Probabilistic operations are classical operations that may introduce randomness or uncertainty.

Example

Here is a probabilistic operation on a bit:

If the classical state is 0, then do nothing.

If the classical state is 1, then flip the bit with probability $1/2$.

$$\begin{pmatrix} 1 & \frac{1}{2} \\ 0 & \frac{1}{2} \end{pmatrix}$$

Probabilistic operations are described by *stochastic matrices:*

- All entries are nonnegative real numbers
- The entries in every column sum to 1

Probabilistic operations

Probabilistic operations are classical operations that may introduce randomness or uncertainty.

Example

Here is a probabilistic operation on a bit:

If the classical state is 0, then do nothing.

If the classical state is 1, then flip the bit with probability $1/2$.

$$\begin{pmatrix} 1 & \frac{1}{2} \\ 0 & \frac{1}{2} \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} + \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Probabilistic operations are described by *stochastic matrices:*

- All entries are nonnegative real numbers
- The entries in every column sum to 1

Composing operations

Suppose X is a system and $M_1, \ldots, M_n$ are stochastic matrices representing probabilistic operations on X.

Applying the first probabilistic operation to the probability vector v, then applying the second probabilistic operation to the result yields this vector:

$$M_2(M_1 v) = (M_2 M_1) v$$

The probabilistic operation obtained by *composing* the first and second probabilistic operations is represented by the *matrix product* $M_2 M_1$.

Composing the probabilistic operations represented by the matrices $M_1, \ldots, M_n$ (in that order) is represented by this matrix product:

$$M_n \cdots M_1$$

Composing operations

Suppose X is a system and $M_1, \ldots, M_n$ are stochastic matrices representing probabilistic operations on X.

Composing the probabilistic operations represented by the matrices $M_1, \ldots, M_n$ (in that order) is represented by this matrix product:

$$M_n \cdots M_1$$

The order is important: matrix multiplication is *not commutative!*

$$M_1 = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \qquad M_2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$M_2 M_1 = \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix} \qquad M_1 M_2 = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$$

Quantum information

A *quantum state* of a system is represented by a *column vector* whose indices are placed in correspondence with the classical states of that system:

- The entries are complex numbers.
- The sum of the absolute values squared of the entries must equal 1.

Definition

The *Euclidean norm* for vectors with complex number entries is defined like this:

$$v = \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} \implies \|v\| = \sqrt{\sum_{k=1}^{n} |\alpha_k|^2}$$

Quantum state vectors are therefore *unit vectors* with respect to this norm.

Quantum information

A *quantum state* of a system is represented by a *column vector* whose indices are placed in correspondence with the classical states of that system:

- The entries are complex numbers.
- The sum of the absolute values squared of the entries must equal 1.

Examples of qubit states

- Standard basis states: $|0\rangle$ and $|1\rangle$
- Plus/minus states:

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

- A state without a special name:

$$\frac{1+2i}{3}|0\rangle - \frac{2}{3}|1\rangle$$

Quantum information

A *quantum state* of a system is represented by a *column vector* whose indices are placed in correspondence with the classical states of that system:

- The entries are complex numbers.
- The sum of the absolute values squared of the entries must equal 1.

Example

A quantum state of a system with classical states ♣, ♦, ♥, and ♠:

$$\frac{1}{2}|\clubsuit\rangle - \frac{i}{2}|\diamondsuit\rangle + \frac{1}{\sqrt{2}}|\spadesuit\rangle = \begin{pmatrix} \frac{1}{2} \\ -\frac{i}{2} \\ 0 \\ \frac{1}{\sqrt{2}} \end{pmatrix}$$

Dirac notation (third part)

The Dirac notation can be used for arbitrary vectors: any name can be used in place of a classical state. Kets are column vectors, bras are row vectors.

Example

The notation $|\psi\rangle$ is commonly used to refer to an arbitrary vector:

$$|\psi\rangle = \frac{1+2i}{3}|0\rangle - \frac{2}{3}|1\rangle$$

For any column vector $|\psi\rangle$, the row vector $\langle\psi|$ is the *conjugate transpose* of $|\psi\rangle$:

$$\langle\psi| = |\psi\rangle^{\dagger}$$

Dirac notation (third part)

The Dirac notation can be used for arbitrary vectors: any name can be used in place of a classical state. Kets are column vectors, bras are row vectors.

Example

The notation $|\psi\rangle$ is commonly used to refer to an arbitrary vector:

$$|\psi\rangle = \frac{1+2i}{3}\,|0\rangle - \frac{2}{3}\,|1\rangle$$

$$\langle\psi| = \frac{1-2i}{3}\,\langle 0| - \frac{2}{3}\,\langle 1|$$

For any column vector $|\psi\rangle$, the row vector $\langle\psi|$ is the *conjugate transpose* of $|\psi\rangle$:

$$\langle\psi| = |\psi\rangle^{\dagger}$$

Dirac notation (third part)

The Dirac notation can be used for arbitrary vectors: any name can be used in place of a classical state. Kets are column vectors, bras are row vectors.

Example

The notation $|\psi\rangle$ is commonly used to refer to an arbitrary vector:

$$|\psi\rangle = \frac{1+2i}{3}|0\rangle - \frac{2}{3}|1\rangle = \begin{pmatrix} \frac{1+2i}{3} \\ -\frac{2}{3} \end{pmatrix}$$

$$\langle\psi| = \frac{1-2i}{3}\langle 0| - \frac{2}{3}\langle 1| = \begin{pmatrix} \frac{1-2i}{3} & -\frac{2}{3} \end{pmatrix}$$

Measuring quantum states

For this lesson will restrict our attention to *standard basis measurements:*

- The possible *outcomes* are the *classical states.*
- The probability for each classical state to be the outcome is the *absolute value squared* of the corresponding quantum state vector entry.

Example 1

Measuring the quantum state

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

yields an outcome as follows:

$$\Pr(\text{outcome is } 0) = \left|\frac{1}{\sqrt{2}}\right|^2 = \frac{1}{2} \qquad \Pr(\text{outcome is } 1) = \left|\frac{1}{\sqrt{2}}\right|^2 = \frac{1}{2}$$

Measuring quantum states

For this lesson will restrict our attention to *standard basis measurements:*

- The possible *outcomes* are the *classical states.*
- The probability for each classical state to be the outcome is the *absolute value squared* of the corresponding quantum state vector entry.

Example 2

Measuring the quantum state

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

yields an outcome as follows:

$$\Pr(\text{outcome is } 0) = \left|\frac{1}{\sqrt{2}}\right|^2 = \frac{1}{2} \qquad \Pr(\text{outcome is } 1) = \left|-\frac{1}{\sqrt{2}}\right|^2 = \frac{1}{2}$$

Measuring quantum states

For this lesson will restrict our attention to *standard basis measurements:*

- The possible *outcomes* are the *classical states.*
- The probability for each classical state to be the outcome is the *absolute value squared* of the corresponding quantum state vector entry.

Example 3

Measuring the quantum state

$$\frac{1+2i}{3}\,|0\rangle - \frac{2}{3}\,|1\rangle$$

yields an outcome as follows:

$$\Pr(\text{outcome is } 0) = \left|\frac{1+2i}{3}\right|^2 = \frac{5}{9} \qquad \Pr(\text{outcome is } 1) = \left|-\frac{2}{3}\right|^2 = \frac{4}{9}$$

Measuring quantum states

For this lesson will restrict our attention to *standard basis measurements:*

- The possible *outcomes* are the *classical states.*
- The probability for each classical state to be the outcome is the *absolute value squared* of the corresponding quantum state vector entry.

Example 4

Measuring the quantum state $|0\rangle$ gives the outcome 0 with certainty, and measuring the quantum state $|1\rangle$ gives the outcome 1 with certainty.

Measuring quantum states

For this lesson will restrict our attention to *standard basis measurements:*

- The possible *outcomes* are the *classical states.*
- The probability for each classical state to be the outcome is the *absolute value squared* of the corresponding quantum state vector entry.

Measuring a system changes its quantum state: if we obtain the classical state a, the new quantum state becomes $|a\rangle$.

$$\begin{tikzcd} & \frac{1+2i}{3}|0\rangle - \frac{2}{3}|1\rangle \arrow[dl, "\text{probability } \frac{5}{9}"'] \arrow[dr, "\text{probability } \frac{4}{9}"] & \\ |0\rangle & & |1\rangle \end{tikzcd}$$

Unitary operations

The set of allowable *operations* that can be performed on a quantum state is different than it is for classical information.

Operations on quantum state vectors are represented by *unitary matrices.*

Definition

A square matrix U having complex number entries is *unitary* if it satisfies the equalities

$$U^\dagger U = \mathbb{1} = U U^\dagger$$

where $U^\dagger$ is the conjugate transpose of U and $\mathbb{1}$ is the identity matrix.

Both equalities are equivalent to $U^{-1} = U^\dagger$.

Unitary operations

Definition

A square matrix U having complex number entries is *unitary* if it satisfies the equalities

$$U^\dagger U = \mathbb{1} = U U^\dagger$$

where $U^\dagger$ is the conjugate transpose of U and $\mathbb{1}$ is the identity matrix.

The condition that an $n \times n$ matrix U is unitary is equivalent to

$$\|Uv\| = \|v\|$$

for every n-dimensional column vector v with complex number entries.

If v is a quantum state vector, then Uv is also a quantum state vector.

Qubit unitary operations

1. Pauli operations

Pauli operations are ones represented by the Pauli matrices:

$$\mathbb{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Common alternative notations: $X = \sigma_x$, $Y = \sigma_y$, and $Z = \sigma_z$.

The operation σ_x is also called a *bit flip* (or a NOT operation) and the σ_z operation is called a *phase flip:*

$$\sigma_x|0\rangle = |1\rangle \qquad \sigma_z|0\rangle = |0\rangle$$
$$\sigma_x|1\rangle = |0\rangle \qquad \sigma_z|1\rangle = -|1\rangle$$

Qubit unitary operations

2. Hadamard operation

The Hadamard operation is represented by this matrix:

$$\mathrm{H} = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix}$$

Checking that H is unitary is a straightforward calculation:

$$\begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix}^{\dagger} \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix} = \begin{pmatrix} \frac{1}{2} + \frac{1}{2} & \frac{1}{2} - \frac{1}{2} \\ \frac{1}{2} - \frac{1}{2} & \frac{1}{2} + \frac{1}{2} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Qubit unitary operations

3. Phase operations

A phase operation is one described by the matrix

$$P_\theta = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix}$$

for any choice of a real number θ.

The operations

$$S = P_{\pi/2} = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \qquad \text{and} \qquad T = P_{\pi/4} = \begin{pmatrix} 1 & 0 \\ 0 & \frac{1+i}{\sqrt{2}} \end{pmatrix}$$

are important examples.

Qubit unitary operations

Example 1

$$H|0\rangle = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} = |+\rangle$$

$$H|1\rangle = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{pmatrix} = |-\rangle$$

$$H|+\rangle = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle$$

$$H|-\rangle = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1\rangle$$

Qubit unitary operations

Example 1

$$H|0\rangle = |+\rangle \qquad H|+\rangle = |0\rangle$$
$$H|1\rangle = |-\rangle \qquad H|-\rangle = |1\rangle$$

$$H\left(\frac{1+2i}{3}|0\rangle - \frac{2}{3}|1\rangle\right) = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix}\begin{pmatrix} \frac{1+2i}{3} \\ -\frac{2}{3} \end{pmatrix} = \begin{pmatrix} \frac{-1+2i}{3\sqrt{2}} \\ \frac{3+2i}{3\sqrt{2}} \end{pmatrix}$$

$$= \frac{-1+2i}{3\sqrt{2}}|0\rangle + \frac{3+2i}{3\sqrt{2}}|1\rangle$$

Qubit unitary operations

Example 2

$$T|0\rangle = |0\rangle \qquad \text{and} \qquad T|1\rangle = \frac{1+i}{\sqrt{2}}|1\rangle$$

$$\begin{aligned} T\,|+\rangle &= T\left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right) \\ &= \frac{1}{\sqrt{2}}T\,|0\rangle + \frac{1}{\sqrt{2}}T\,|1\rangle \\ &= \frac{1}{\sqrt{2}}|0\rangle + \frac{1+i}{2}|1\rangle \end{aligned}$$

$$T = \begin{pmatrix} 1 & 0 \\ 0 & \frac{1+i}{\sqrt{2}} \end{pmatrix}$$

Qubit unitary operations

Example 2

$$T|+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1+i}{2}|1\rangle$$

$$\begin{aligned}
HT|+\rangle &= H\left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1+i}{2}|1\rangle\right)\\
&= \frac{1}{\sqrt{2}}H|0\rangle + \frac{1+i}{2}H|1\rangle\\
&= \frac{1}{\sqrt{2}}|+\rangle + \frac{1+i}{2}|-\rangle\\
&= \left(\frac{1}{2}|0\rangle + \frac{1}{2}|1\rangle\right) + \left(\frac{1+i}{2\sqrt{2}}|0\rangle - \frac{1+i}{2\sqrt{2}}|1\rangle\right)\\
&= \left(\frac{1}{2} + \frac{1+i}{2\sqrt{2}}\right)|0\rangle + \left(\frac{1}{2} - \frac{1+i}{2\sqrt{2}}\right)|1\rangle
\end{aligned}$$

$$H|0\rangle = |+\rangle$$
$$H|1\rangle = |-\rangle$$

Composing unitary operations

Compositions of unitary operations are represented by *matrix multiplication* (similar to the probabilistic setting).

Example: square root of NOT

Applying a Hadamard operation, followed by the phase operation S, followed by another Hadamard operation yields this operation:

$$\mathrm{HSH} = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix} = \begin{pmatrix} \frac{1+i}{2} & \frac{1-i}{2} \\ \frac{1-i}{2} & \frac{1+i}{2} \end{pmatrix}$$

Applying this unitary operation twice yields a NOT operation:

$$(\mathrm{HSH})^2 = \begin{pmatrix} \frac{1+i}{2} & \frac{1-i}{2} \\ \frac{1-i}{2} & \frac{1+i}{2} \end{pmatrix}^2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$