Quantum information

Now we're ready to move on to quantum information, where we make a different choice for the type of vector that represents a state — in this case a *quantum state* — of the system being considered. Like in the previous discussion of classical information, we'll be concerned with systems having finite and nonempty sets of classical states, and we'll make use of much of the same notation.

Quantum state vectors

A *quantum state* of a system is represented by a column vector, similar to a probabilistic state. As before, the indices of the vector label the classical states of the system. Vectors representing quantum states are characterized by these two properties:

1. The entries of a quantum state vector are *complex numbers*.

2. The sum of the *absolute values squared* of the entries of a quantum state vector is $1.$

Thus, in contrast to probabilistic states, vectors representing quantum states need not have nonnegative real number entries, and it is the sum of the absolute values squared of the entries (as opposed to the sum of the entries) that must equal $1.$ Simple as these changes are, they give rise to the differences between quantum and classical information; any speedup from a quantum computer, or improvement from a quantum communication protocol, is ultimately derived from these simple mathematical changes.

The *Euclidean norm* of a column vector

$$v = \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix}$$

is denoted and defined as follows:

$$\|v\| = \sqrt{\sum_{k=1}^{n} |\alpha_k|^2}.$$

The condition that the sum of the absolute values squared of a quantum state vector equals 1 is therefore equivalent to that vector having Euclidean norm equal to 1. That is, quantum state vectors are *unit vectors* with respect to the Euclidean norm.

Examples of qubit states

The term *qubit* refers to a quantum system whose classical state set is $\{0, 1\}$. That is, a qubit is really just a bit — but by using this name we explicitly recognize that this bit can be in a quantum state.

These are examples of quantum states of a qubit:

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

$$\begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} = \frac{1}{\sqrt{2}} |0\rangle + \frac{1}{\sqrt{2}} |1\rangle, \tag{1}$$

and

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

The first two examples, $|0\rangle$ and $|1\rangle$, illustrate that standard basis elements are valid quantum state vectors: their entries are complex numbers, where the imaginary part of these numbers all happen to be 0, and computing the sum of the absolute values squared of the entries yields

$$|1|^2 + |0|^2 = 1 \quad \text{and} \quad |0|^2 + |1|^2 = 1,$$

as required. Similar to the classical setting, we associate the quantum state vectors $|0\rangle$ and $|1\rangle$ with a qubit being in the classical state 0 and 1, respectively.

For the other two examples, we again have complex number entries, and computing the sum of the absolute value squared of the entries yields

$$\left| \frac{1}{\sqrt{2}} \right|^2 + \left| \frac{1}{\sqrt{2}} \right|^2 = \frac{1}{2} + \frac{1}{2} = 1$$

and

$$\left|\frac{1+2i}{3}\right|^2 + \left|-\frac{2}{3}\right|^2 = \frac{5}{9} + \frac{4}{9} = 1.$$

These are therefore valid quantum state vectors. Note that they are linear combinations of the standard basis states $|0\rangle$ and $|1\rangle$, and for this reason we often say that they're *superpositions* of the states 0 and 1. Within the context of quantum states, *superposition* and *linear combination* are essentially synonymous.

The example (1) of a qubit state vector above is very commonly encountered — it is called the *plus state* and is denoted as follows:

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

We also use the notation

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

to refer to a related quantum state vector where the second entry is negative rather than positive, and we call this state the *minus state*.

This sort of notation, where some symbol other than one referring to a classical state appears inside of a ket, is common — we can use whatever name we wish inside of a ket to name a vector. It is quite common to use the notation $|\psi\rangle$, or a different name in place of ψ, to refer to an arbitrary vector that may not necessarily be a standard basis vector.

Notice that, if we have a vector $|\psi\rangle$ whose indices correspond to some classical state set Σ, and if $a \in \Sigma$ is an element of this classical state set, then the matrix product $\langle a||\psi\rangle$ is equal to the entry of the vector $|\psi\rangle$ whose index corresponds to a. As we did when $|\psi\rangle$ was a standard basis vector, we write $\langle a|\psi\rangle$ rather than $\langle a||\psi\rangle$ for the sake of readability.

For example, if $\Sigma = \{0, 1\}$ and

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

then

$$\langle 0|\psi\rangle = \frac{1+2i}{3} \quad \text{and} \quad \langle 1|\psi\rangle = -\frac{2}{3}.$$

In general, when using the Dirac notation for arbitrary vectors, the notation $\langle\psi|$ refers to the row vector obtained by taking the *conjugate-transpose* of the column vector $|\psi\rangle$, where the vector is transposed from a column vector to a row vector and each entry is replaced by its complex conjugate. For example, if $|\psi\rangle$ is the vector defined in (2), then

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

The reason we take the complex conjugate, in addition to the transpose, will be made more clear later on we discuss inner products.

Quantum states of other systems

We can consider quantum states of systems having arbitrary classical state sets. For example, here is a quantum state vector for an electrical fan switch:

$$\begin{pmatrix} \frac{1}{2} \\ 0 \\ -\frac{i}{2} \\ \frac{1}{\sqrt{2}} \end{pmatrix} = \frac{1}{2}|\text{high}\rangle - \frac{i}{2}|\text{low}\rangle + \frac{1}{\sqrt{2}}|\text{off}\rangle.$$

The assumption in place here is that the classical states are ordered as *high, medium, low, off*. There may be no particular reason why one would want to consider a quantum state of an electrical fan switch, but it is possible in principle.

Here's another example, this time of a quantum decimal digit whose classical states are $0, 1, \ldots, 9$:

$$\frac{1}{\sqrt{385}}\begin{pmatrix} 1 \\ 2 \\ 3 \\ 4 \\ 5 \\ 6 \\ 7 \\ 8 \\ 9 \\ 10 \end{pmatrix} = \frac{1}{\sqrt{385}}\sum_{k=0}^{9}(k+1)|k\rangle.$$

This example illustrates the convenience of writing state vectors using the Dirac notation. For this particular example, the column vector representation is merely cumbersome — but if there were significantly

more classical states it would become unusable. The Dirac notation, in contrast, supports precise descriptions of large and complicated vectors in a compact form.

The Dirac notation also allows for the expression of vectors where different aspects of the vectors are *indeterminate,* meaning that they are unknown or not yet established. For example, for an arbitrary classical state set Σ, we can consider the quantum state vector

$$\frac{1}{\sqrt{|\Sigma|}} \sum_{a \in \Sigma} |a\rangle,$$

where the notation $|\Sigma|$ refers to the number of elements in Σ. In words, this is a *uniform superposition* over the classical states in Σ.

We'll encounter much more complicated expressions of quantum state vectors in later lessons, where the use of column vectors would be impractical or impossible. In fact, we'll mostly abandon the column vector representation of state vectors, except for vectors having a small number of entries (often in the context of examples), where it may be helpful to display and examine the entries explicitly.

Here's one more reason why expressing state vectors using the Dirac notation is convenient: it alleviates the need to explicitly specify an ordering of the classical states (or, equivalently, the correspondence between classical states and vector indices).

For example, a quantum state vector for a system having classical state set $\{\clubsuit, \diamondsuit, \heartsuit, \spadesuit\}$, such as

$$\frac{1}{2}|\clubsuit\rangle + \frac{i}{2}|\diamondsuit\rangle - \frac{1}{2}|\heartsuit\rangle - \frac{i}{2}|\spadesuit\rangle,$$

is unambiguously described by this expression, and there's really no need to choose or specify an ordering of this classical state set to make sense of the expression. In this case, it's not difficult to specify an ordering of the standard card suits — for instance, we might choose to order them like this: $\clubsuit, \diamondsuit, \heartsuit, \spadesuit$. If we choose this particular ordering, the quantum state vector above would be represented by the column vector

$$\begin{pmatrix} \frac{1}{2} \\ \frac{i}{2} \\ -\frac{1}{2} \\ -\frac{i}{2} \end{pmatrix}.$$

In general, however, it is convenient to be able to simply ignore the issue of how classical state sets are ordered.

Measuring quantum states

Next let us consider what happens when a quantum state is *measured*, focusing on a simple type of measurement known as a *standard basis measurement*. (There are more general notions of measurement that we'll discuss later on.)

Similar to the probabilistic setting, when a system in a quantum state is measured, the hypothetical observer performing the measurement won't see a quantum state vector, but rather will see some classical state. In this sense, measurements act as an interface between quantum and classical information, through which classical information is extracted from quantum states.

The rule is simple: if a quantum state is measured, each classical state of the system appears with probability equal to the *absolute value squared* of the entry in the quantum state vector corresponding to that classical state. This is known as the *Born rule* in quantum mechanics. Notice that this rule is consistent with the requirement that the absolute values squared of the entries in a quantum state vector sum to 1, as it implies that the probabilities of different classical state measurement outcomes sum to 1.

For example, measuring the plus state

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

results in the two possible outcomes, 0 and 1, with probabilities as follows.

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

$$\mathrm{Pr}(\text{outcome is } 1) = \left|\langle 1|+\rangle\right|^2 = \left|\frac{1}{\sqrt{2}}\right|^2 = \frac{1}{2}$$

Interestingly, measuring the minus state

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

results in exactly the same probabilities for the two outcomes.

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

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

This suggests that, as far as standard basis measurements are concerned, the plus and minus states are no different. Why, then, would we care to make a distinction between them? The answer is that these two states behave differently when operations are performed on them, as we will discuss in the next subsection below.

Of course, measuring the quantum state $|0\rangle$ results in the classical state 0 with certainty, and likewise measuring the quantum state $|1\rangle$ results in the classical state 1 with certainty. This is consistent with the identification of these quantum states with the system *being* in the corresponding classical state, as was suggested previously.

As a final example, measuring the state

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

causes the two possible outcomes to appear with probabilities as follows:

$$\Pr(\text{outcome is } 0) = \big|\langle 0|\psi\rangle\big|^2 = \left|\frac{1+2i}{3}\right|^2 = \frac{5}{9},$$

and

$$\Pr(\text{outcome is } 1) = \big|\langle 1|\psi\rangle\big|^2 = \left|-\frac{2}{3}\right|^2 = \frac{4}{9}.$$

Unitary operations

Thus far, it may not be evident why quantum information is fundamentally different from classical information. That is, when a quantum state is measured, the probability to obtain each classical state is given by the absolute value squared of the corresponding vector entry — so why not simply record these probabilities in a probability vector?

The answer, at least in part, is that the set of allowable *operations* that can be performed on a quantum state is different than it is for classical information. Similar to the probabilistic setting, operations on quantum states are linear mappings — but rather than being represented by stochastic matrices, like in the classical case, operations on quantum state vectors are represented by *unitary* matrices.

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

$$UU^\dagger = \mathbb{I}$$
$$U^\dagger U = \mathbb{I}. \tag{3}$$

Here, $\mathbb{I}$ is the identity matrix, and $U^\dagger$ is the *conjugate transpose* of U, meaning the matrix obtained by transposing U and taking the complex conjugate of each entry.

$$U^\dagger = \overline{U^T}$$

If either of the two equalities numbered (3) above is true, then the other must also be true. Both equalities are equivalent to $U^\dagger$ being the inverse of U :

$$U^{-1} = U^\dagger.$$

(Warning: if M is not a square matrix, then it could be that $M^\dagger M = \mathbb{I}$ and $MM^\dagger \neq \mathbb{I}$, for instance. The equivalence of the two equalities in the first equation above is only true for square matrices.)

The condition that U is unitary is equivalent to the condition that multiplication by U does not change the Euclidean norm of any vector. That is, an $n \times n$ matrix U is unitary if and only if $\|U|\psi\rangle\| = \||\psi\rangle\|$ for every n-dimensional column vector $|\psi\rangle$ with complex number entries. Thus, because the set of all quantum state vectors is the same as the set of vectors having Euclidean norm equal to 1, multiplying a unitary matrix to a quantum state vector results in another quantum state vector.

Indeed, unitary matrices are exactly the set of linear mappings that always transform quantum state vectors to other quantum state vectors. Notice here a resemblance to the classical probabilistic case where operations are associated with stochastic matrices, which are the ones that always transform probability vectors into probability vectors.

Examples of unitary operations on qubits

The following list describes some commonly encountered unitary operations on qubits.

1. *Pauli operations.* The four Pauli matrices are as follows:

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

A common alternative notation is $X = \sigma_x$, $Y = \sigma_y$, and $Z = \sigma_z$ (but be aware that the letters X, Y, and Z are also commonly used for other purposes). The X operation is also called a *bit flip* or a *NOT operation* because it induces this action on bits:

$$X|0\rangle = |1\rangle \quad \text{and} \quad X|1\rangle = |0\rangle.$$

The Z operation is also called a *phase flip,* and it has this action:

$$Z|0\rangle = |0\rangle \quad \text{and} \quad Z|1\rangle = -|1\rangle.$$

2. *Hadamard operation.* The Hadamard operation is described by this matrix:

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

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

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

are particularly important examples. Other examples include $\mathbb{I} = P_0$ and $Z = P_\pi$.

All of the matrices just defined are unitary, and therefore represent quantum operations on a single qubit. For example, here is a calculation that verifies that H is unitary:

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

And here's the action of the Hadamard operation on a few commonly encountered qubit state vectors.

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

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

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

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

More succinctly, we obtain these four equations.

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

It's worth pausing to consider the fact that $H|+\rangle = |0\rangle$ and $H|-\rangle = |1\rangle$, in light of the question suggested in the previous section concerning the distinction between the states $|+\rangle$ and $|-\rangle$.

Imagine a situation in which a qubit is prepared in one of the two quantum states $|+\rangle$ and $|-\rangle$, but where it is not known to us which one it is. Measuring either state produces the same output distribution as the other, as we already observed: 0 and 1 both appear with equal probability $1/2$, which provides no information whatsoever about which of the two states was prepared.

However, if we first apply a Hadamard operation and then measure, we obtain the outcome 0 with certainty if the original state was $|+\rangle$, and we obtain the outcome 1, again with certainty, if the original state was $|-\rangle$. The quantum states $|+\rangle$ and $|-\rangle$ can therefore be discriminated perfectly. This reveals that sign changes, or more generally changes to the *phases* (which are also traditionally called *arguments*) of the complex number entries of a quantum state vector, can significantly change that state.

Here's another example, showing how a Hadamard operation acts on a state vector that was mentioned previously.

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

Next, let's consider the action of a T operation on a plus state.

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

Notice here that we did not bother to convert to the equivalent matrix/vector forms, and instead used the linearity of matrix multiplication together with the formulas

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

Along similar lines, we may compute the result of applying a Hadamard operation to the quantum state vector just obtained:

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

The two approaches — one where we explicitly convert to matrix representations and the other where we use linearity and plug in the actions of an operation on standard basis states — are equivalent. We can use whichever one is more convenient in the case at hand.

Compositions of qubit unitary operations

Compositions of unitary operations are represented by matrix multiplication, just like we had in the probabilistic setting.

For example, suppose we first apply a Hadamard operation, followed by an S operation, followed by another Hadamard operation. The resulting operation, which we shall name R for the sake of this example, is as follows:

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

This unitary operation R is an interesting example. By applying this operation twice, which is equivalent to squaring its matrix representation, we obtain a NOT operation:

$$R^2 = \begin{pmatrix} \frac{1+i}{2} & \frac{1-i}{2} \\ \frac{1-i}{2} & \frac{1+i}{2} \end{pmatrix}^2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

That is, R is a *square root of NOT* operation. Such a behavior, where the same operation is applied twice to yield a NOT operation, is not possible for a classical operation on a single bit.

Unitary operations on larger systems

In subsequent lessons, we will see many examples of unitary operations on systems having more than two classical states. An example of a unitary operation on a system having three classical states is given by the following matrix.

$$A = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

Assuming that the classical states of the system are 0, 1, and 2, we can describe this operation as addition modulo 3.

$$A|0\rangle = |1\rangle, \quad A|1\rangle = |2\rangle, \quad \text{and} \quad A|2\rangle = |0\rangle$$

The matrix A is an example of a *permutation matrix*, which is a matrix in which every row and column has exactly one 1. Such matrices merely rearrange, or permute, the entries of the vectors they act upon. The identity matrix is perhaps the simplest example of a permutation matrix, and another example is the NOT operation on a bit or qubit. Every permutation matrix, in any positive integer dimension, is unitary. These are the only examples of matrices that represent both classical and quantum operations: a matrix is both stochastic and unitary if and only if it is a permutation matrix.

Another example of a unitary matrix, this time being a 4×4 matrix, is this one:

$$U = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix}.$$

This matrix describes an operation known as the *quantum Fourier transform*, specifically in the 4×4 case. The quantum Fourier transform can be defined more generally, for any positive integer dimension n, and plays a key role in quantum algorithms.

Was this page helpful?

Yes　👍　　No　👎

Report a bug or request content on GitHub ↗.

Previous page　　　　Start the next lesson

© IBM Corp., 2017-2025