Understanding quantum information and computation

By John Watrous

Lesson 3

Quantum circuits

Circuits

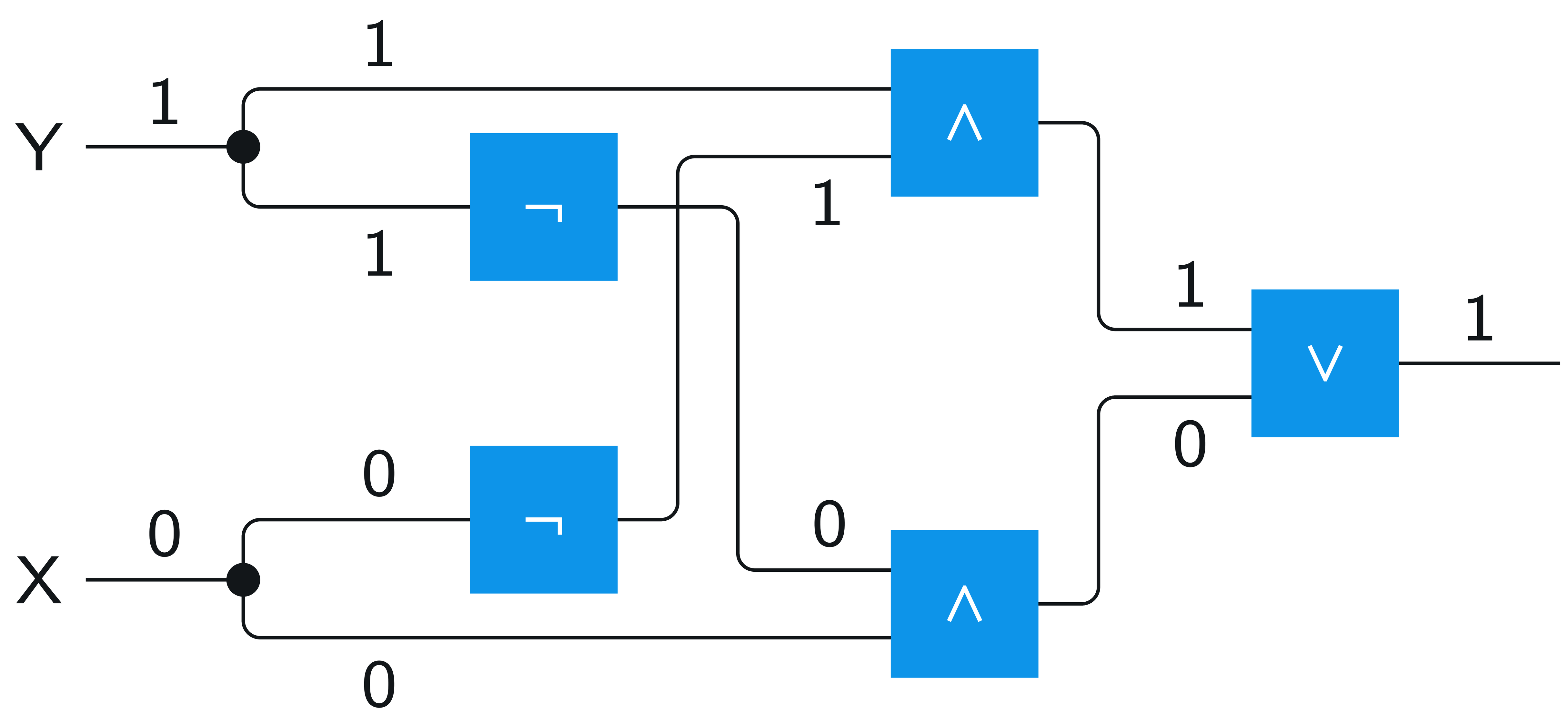
Circuits are models of computation:

- Wires carry information
- Gates represent operations

In this series, circuits are always *acyclic* — information flows from left to right.

Example: Boolean circuits

Wires store binary values, gates represent Boolean logic operations, such as AND ($\wedge$), OR ($\vee$), NOT ($\neg$), and FANOUT ($\bullet$).



Circuits

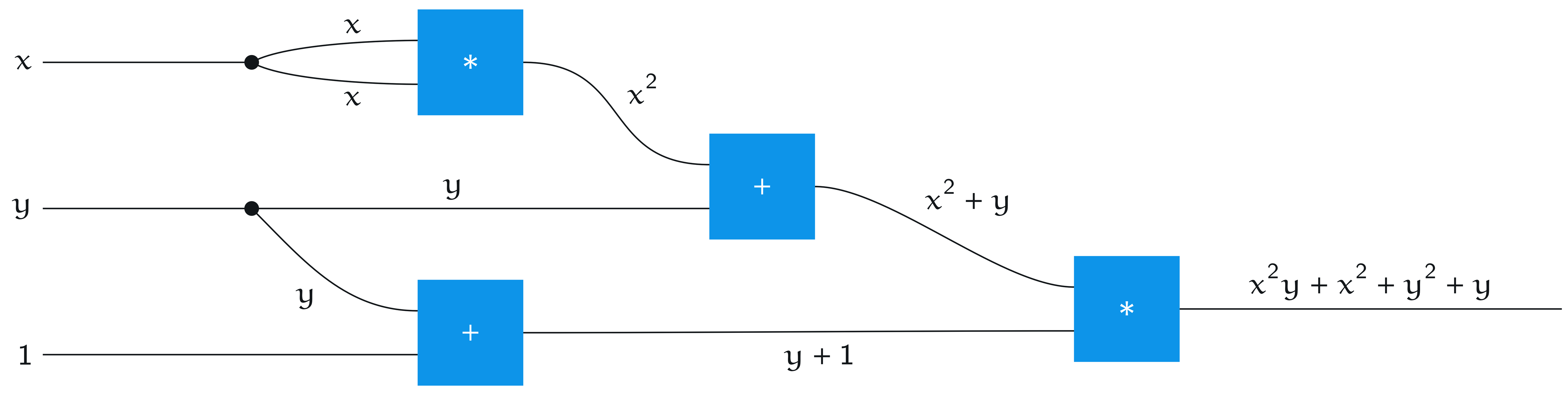
Circuits are models of computation:

- Wires carry information
- Gates represent operations

In this series, circuits are always *acyclic* — information flows from left to right.

Example: arithmetic circuits

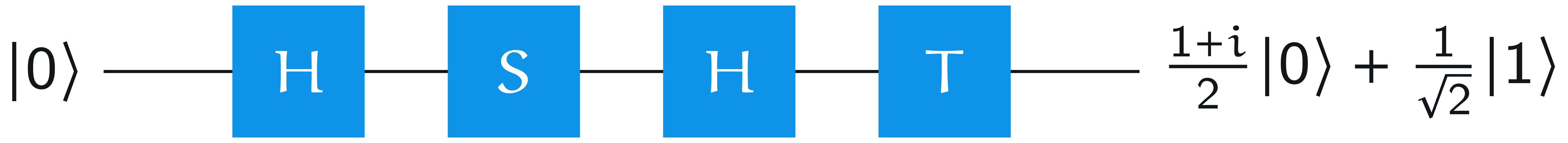
Wires store numbers and gates represent arithmetic operations, such as addition ($+$) and multiplication ($*$).



Quantum circuits

In the *quantum circuit* model, the wires represent qubits and the gates represent both unitary operations and measurements.

Example

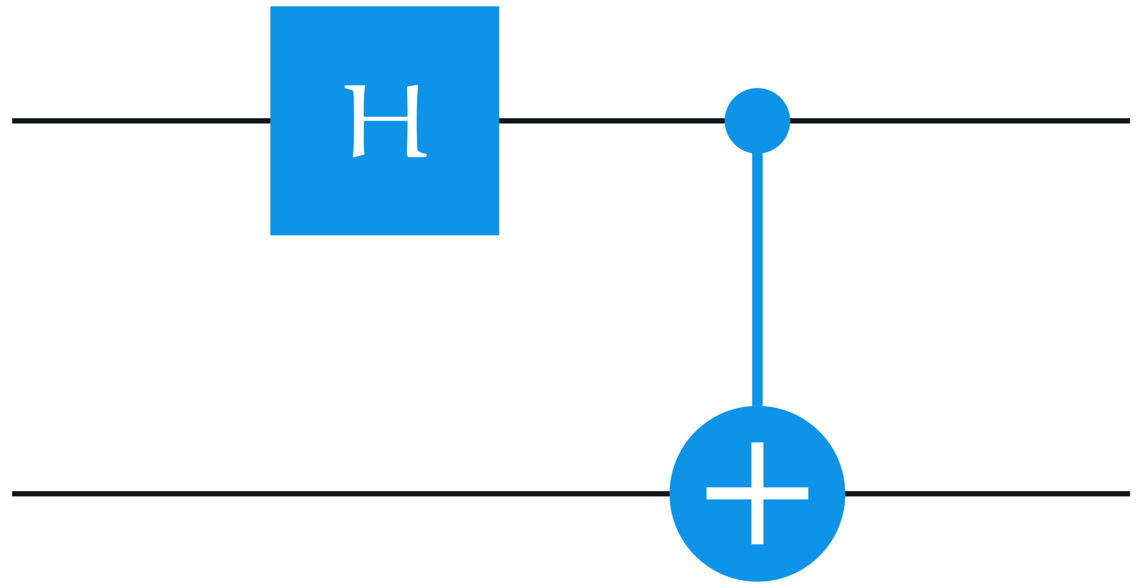


$$H = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix} \qquad S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \qquad T = \begin{pmatrix} 1 & 0 \\ 0 & \frac{1+i}{\sqrt{2}} \end{pmatrix}$$

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

Quantum circuits

Example



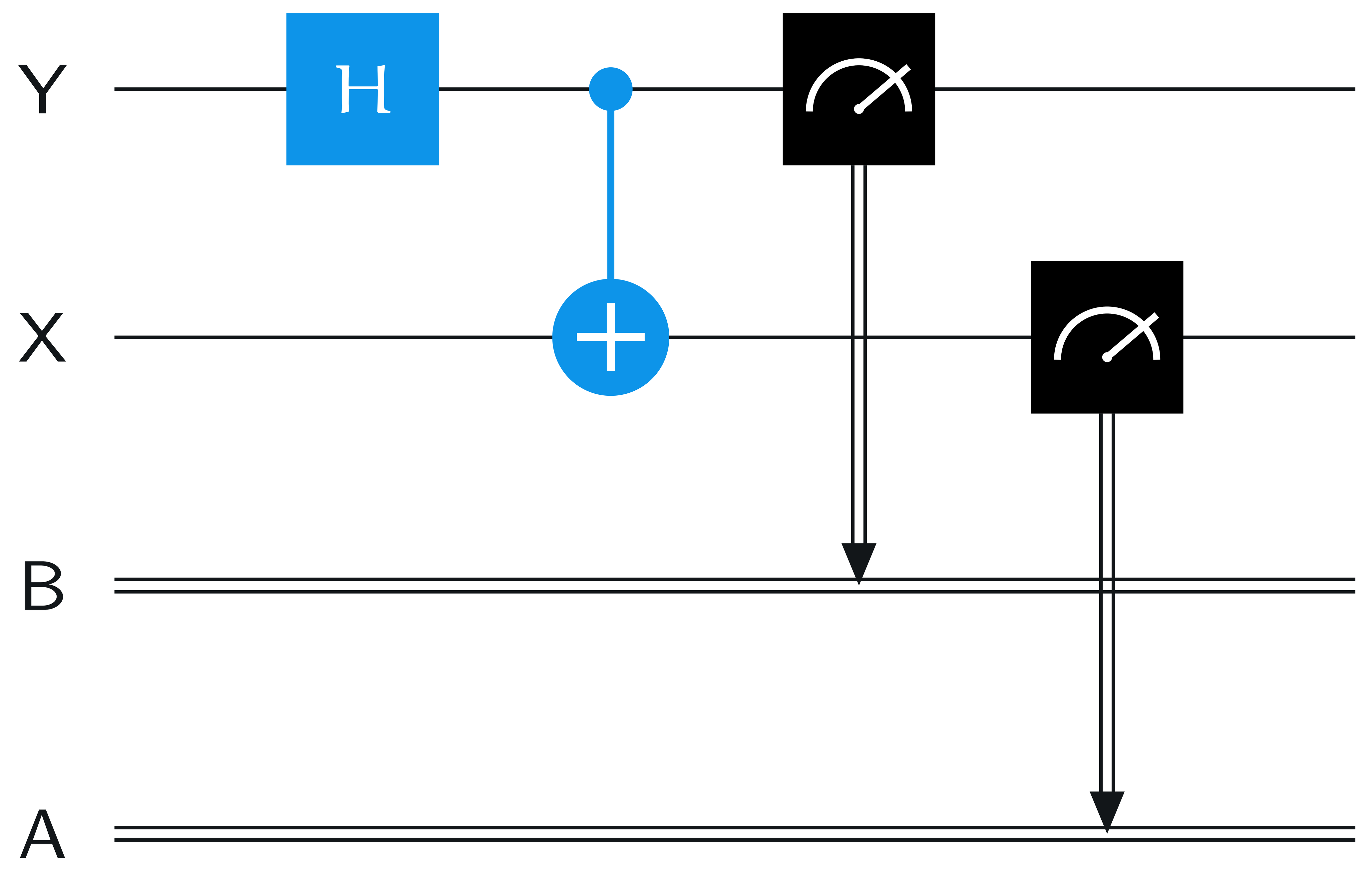
$$\begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 & 0 \\ 0 & 0 & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \\ 0 & 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} & 0 & 0 \end{pmatrix}$$

Convention

In this series (and in Qiskit), ordering qubits from *bottom-to-top* is equivalent to ordering them *left-to-right.*

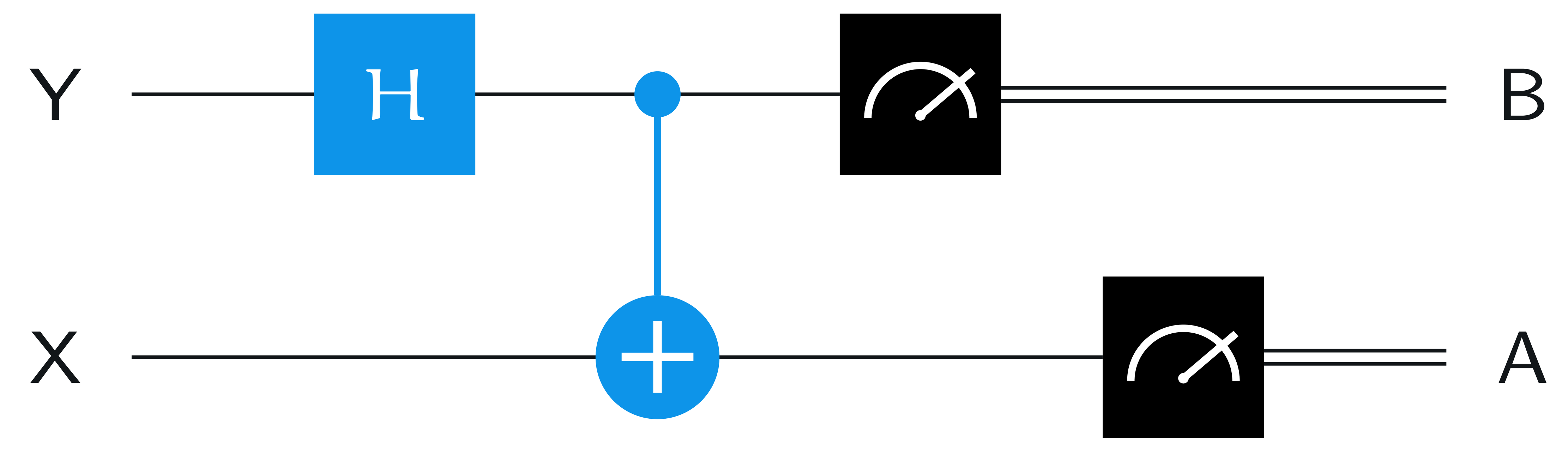
Quantum circuits

Example

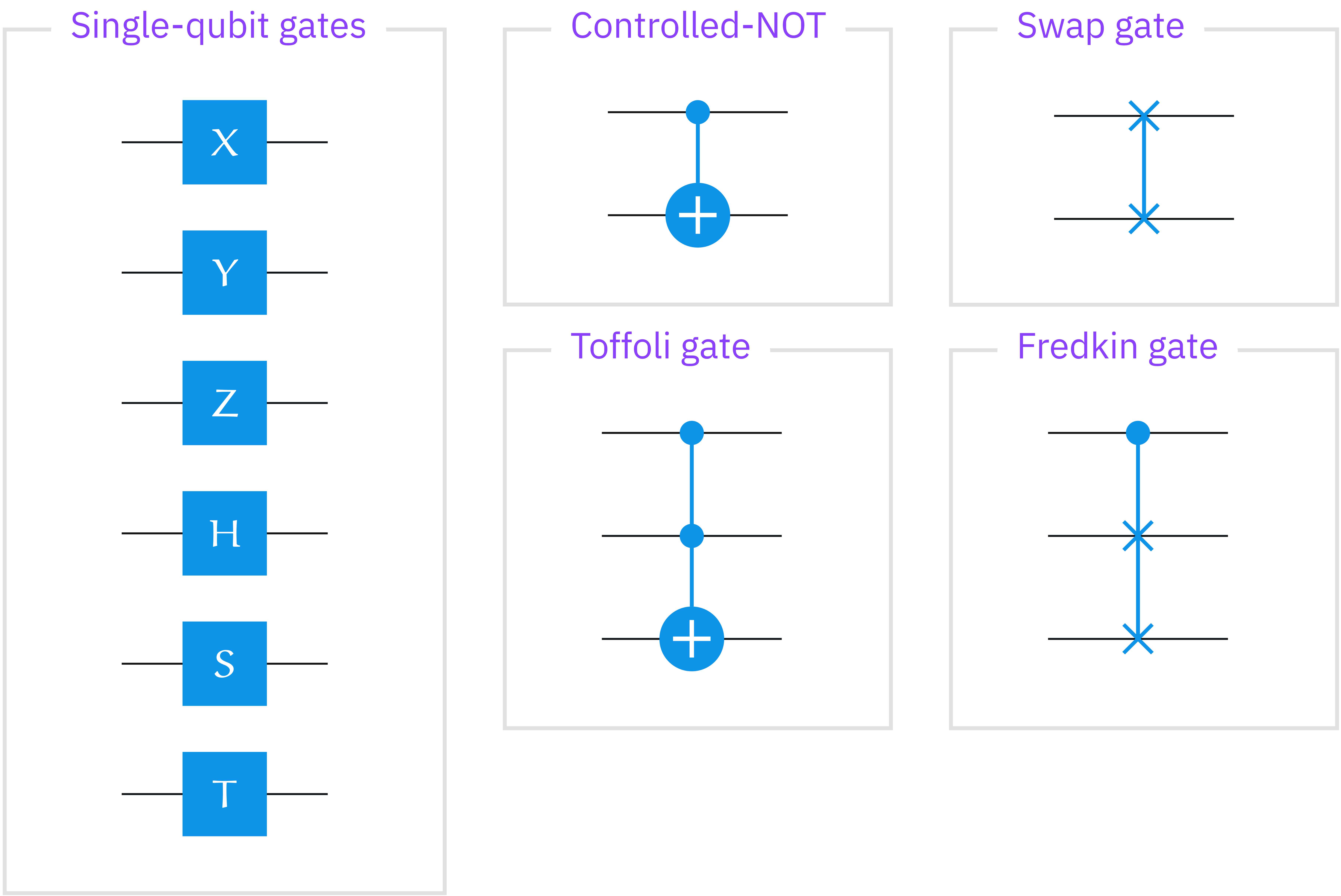


Quantum circuits

Example



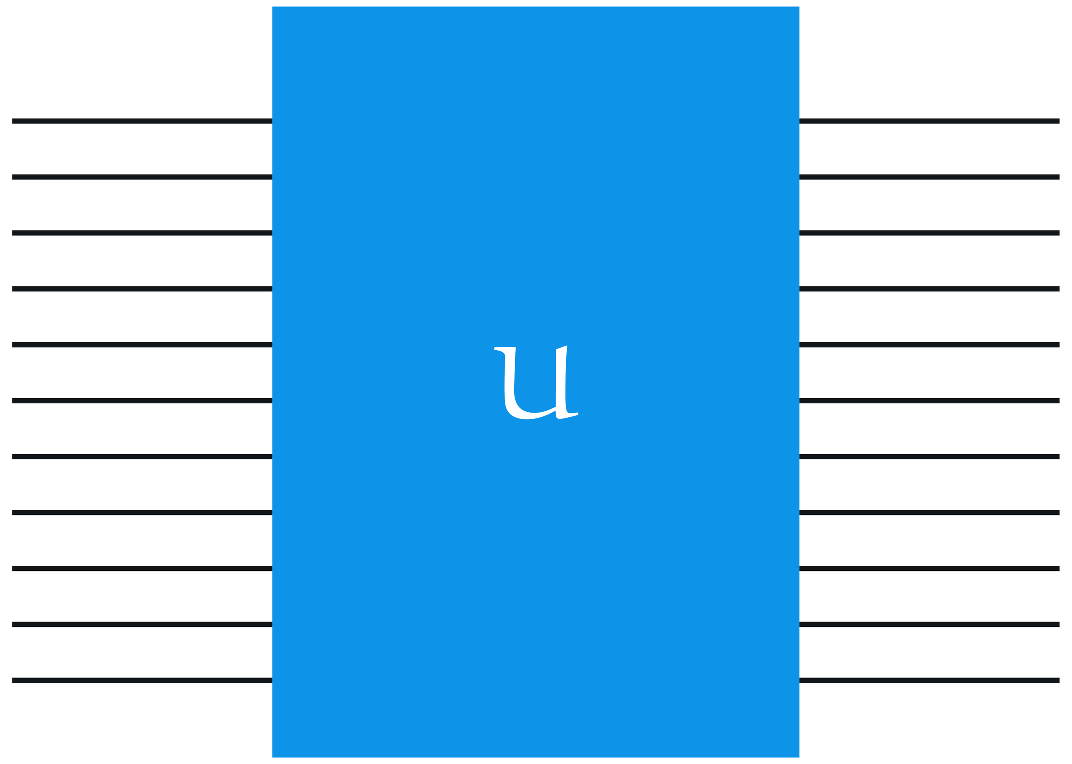
Quantum circuits



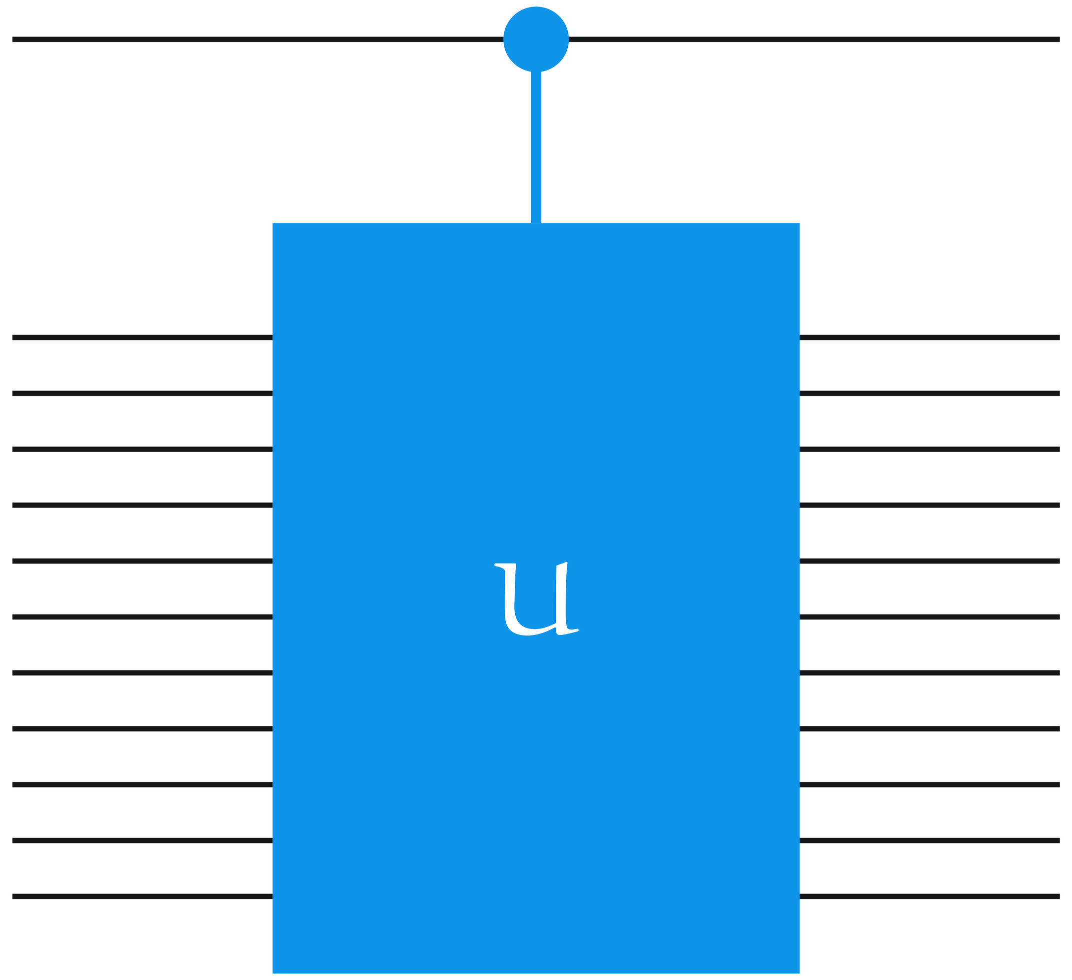
Quantum circuits

It is also sometimes convenient to view *arbitrary unitary operations* as gates.

Unitary operation



Controlled-unitary operation



Inner products

When we use the Dirac notation, a ket is a column vector, and its corresponding bra is a row vector:

$$|\psi\rangle = \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} \qquad \langle\psi| = \begin{pmatrix} \overline{\alpha_1} & \cdots & \overline{\alpha_n} \end{pmatrix}$$

Suppose that we have two kets:

$$|\psi\rangle = \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} \quad \text{and} \quad |\phi\rangle = \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix}$$

Inner products

Suppose that we have two kets:

$$|\psi\rangle = \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} \qquad \text{and} \qquad |\phi\rangle = \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix}$$

We then have

$$\langle\psi|\phi\rangle = \begin{pmatrix} \overline{\alpha_1} & \cdots & \overline{\alpha_n} \end{pmatrix} \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix} = \overline{\alpha_1}\beta_1 + \cdots + \overline{\alpha_n}\beta_n$$

This is the *inner product* of $|\psi\rangle$ and $|\phi\rangle$.

Inner products

Alternatively, suppose that we have two column vectors expressed like this:

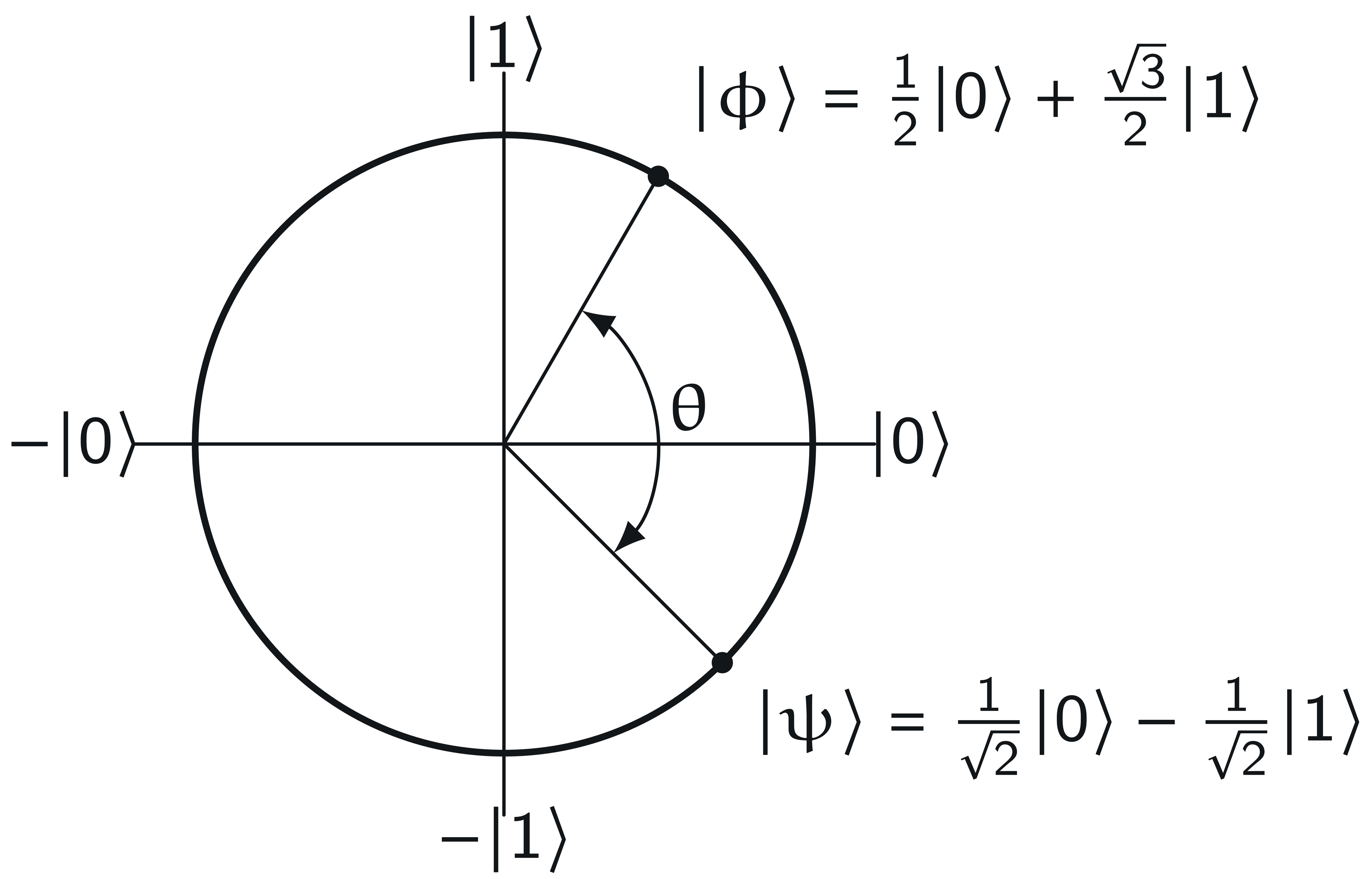
$$|\psi\rangle = \sum_{a\in\Sigma} \alpha_a |a\rangle \quad \text{and} \quad |\phi\rangle = \sum_{b\in\Sigma} \beta_b |b\rangle$$

Then the inner product of these vectors is as follows:

$$\begin{aligned}
\langle\psi|\phi\rangle &= \left(\sum_{a\in\Sigma} \overline{\alpha_a} \langle a|\right)\left(\sum_{b\in\Sigma} \beta_b |b\rangle\right) \\
&= \sum_{a\in\Sigma} \sum_{b\in\Sigma} \overline{\alpha_a} \beta_b \langle a|b\rangle \\
&= \sum_{a\in\Sigma} \overline{\alpha_a} \beta_a
\end{aligned}$$

Inner products

Example

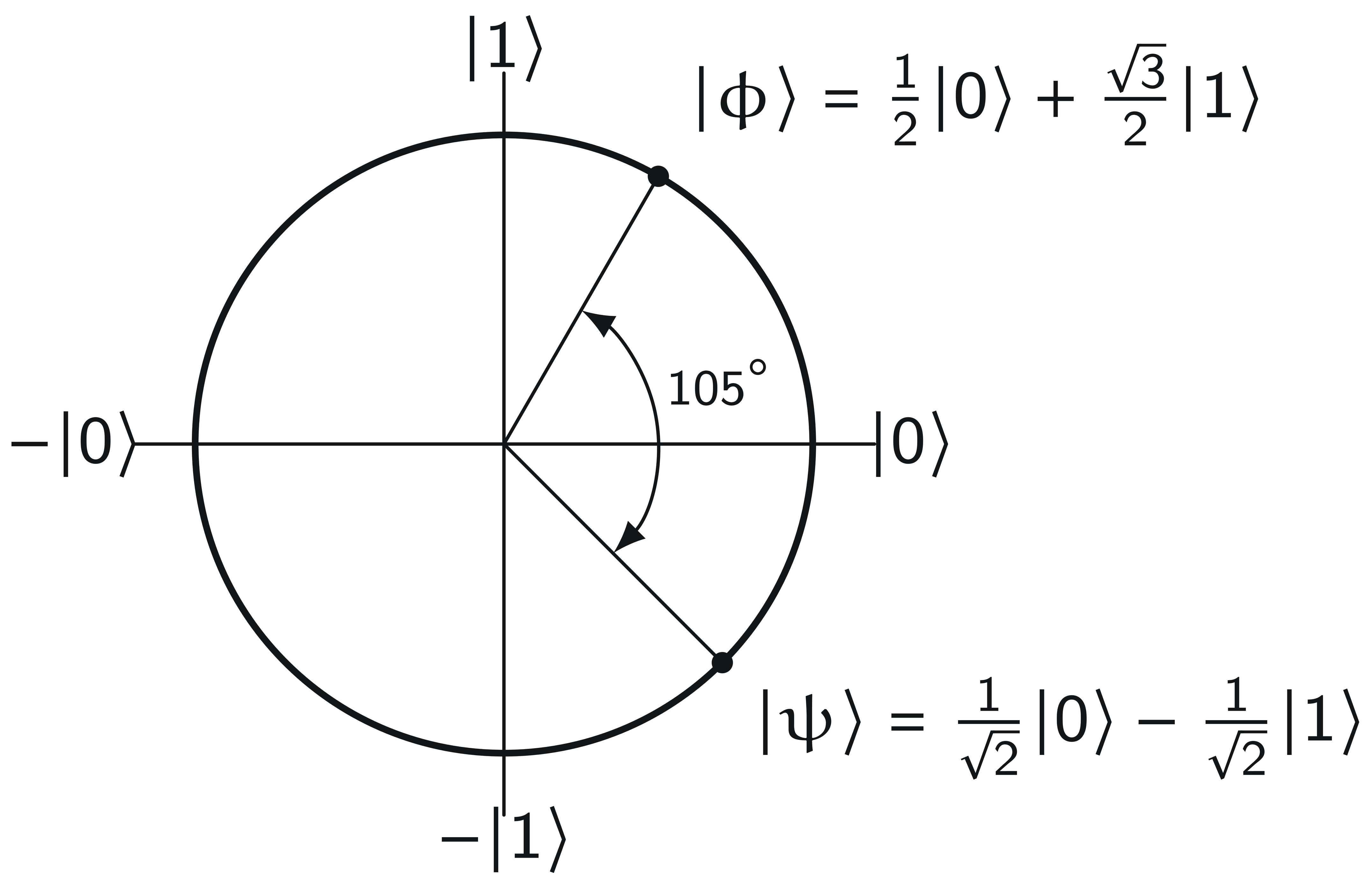


The inner product of these two vectors is

$$\langle\psi|\phi\rangle = \frac{1-\sqrt{3}}{2\sqrt{2}} \approx -0.2588$$

Inner products

Example

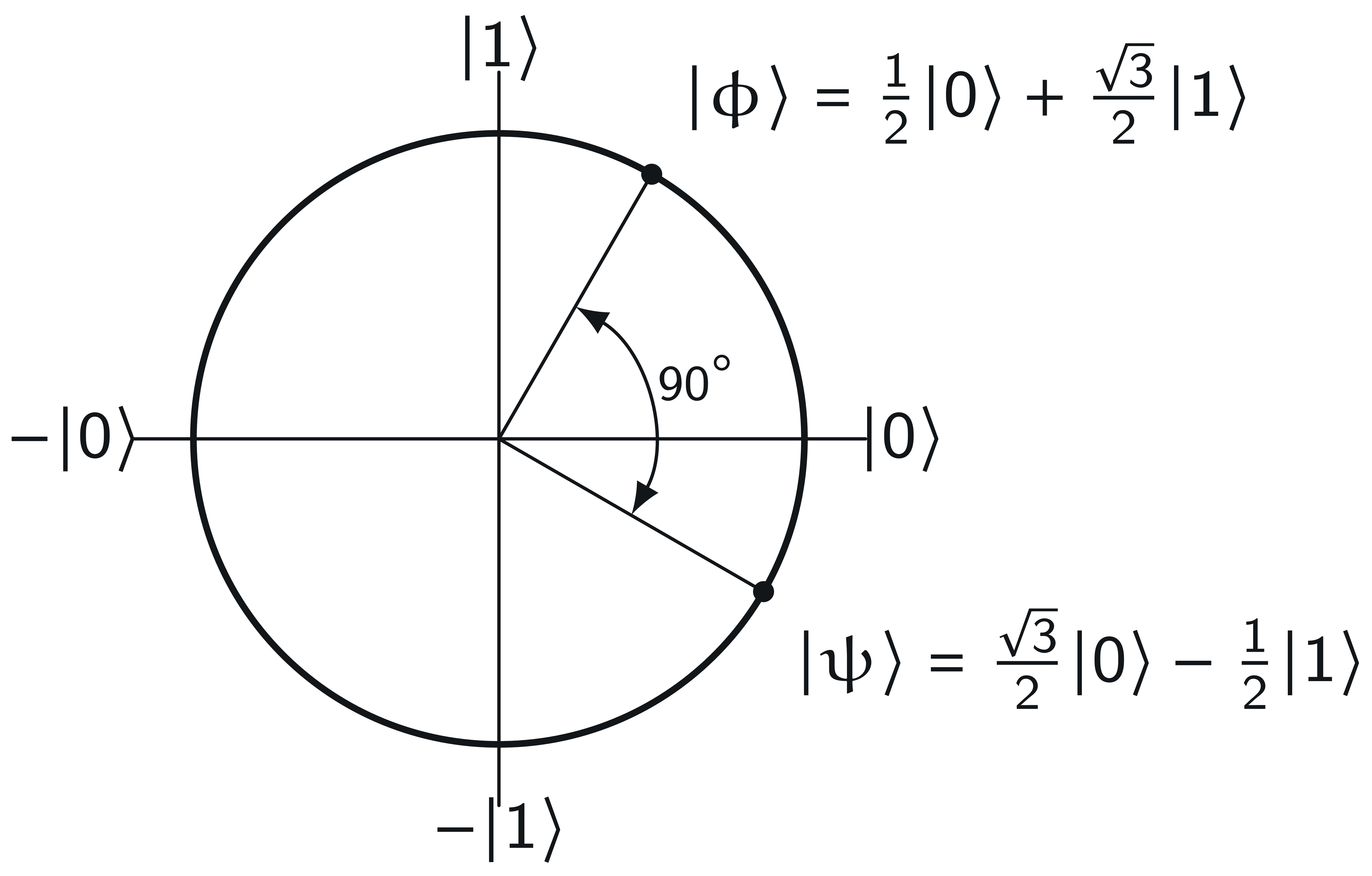


The inner product of these two vectors is

$$\langle\psi|\phi\rangle = \frac{1-\sqrt{3}}{2\sqrt{2}} = \cos(105^\circ) \approx -0.2588$$

Inner products

Example



The inner product of these two vectors is

$$\langle\psi|\phi\rangle = 0 = \cos(90^\circ)$$

Inner products

Relationship to the Euclidean norm

The inner product of any vector

$$|\psi\rangle = \sum_{a\in\Sigma} \alpha_a |a\rangle$$

with itself is

$$\langle\psi|\psi\rangle = \sum_{a\in\Sigma} \overline{\alpha_a}\alpha_a = \sum_{a\in\Sigma} |\alpha_a|^2 = \big\| |\psi\rangle \big\|^2$$

That is, the Euclidean norm of a vector $|\psi\rangle$ is given by

$$\big\| |\psi\rangle \big\| = \sqrt{\langle\psi|\psi\rangle}$$

Inner products

Conjugate symmetry

For any two vectors

$$|\psi\rangle = \sum_{a\in\Sigma} \alpha_a |a\rangle \quad \text{and} \quad |\phi\rangle = \sum_{b\in\Sigma} \beta_b |b\rangle$$

we have

$$\langle\psi|\phi\rangle = \sum_{a\in\Sigma} \overline{\alpha_a}\beta_a \quad \text{and} \quad \langle\phi|\psi\rangle = \sum_{a\in\Sigma} \overline{\beta_a}\alpha_a$$

and therefore

$$\overline{\langle\psi|\phi\rangle} = \langle\phi|\psi\rangle$$

Inner products

Linearity in the second argument

Suppose that $|\psi\rangle$, $|\phi_1\rangle$, and $|\phi_2\rangle$ are vectors and α_1 and α_2 are complex numbers. If we define a new vector

$$|\phi\rangle = \alpha_1|\phi_1\rangle + \alpha_2|\phi_2\rangle$$

then

$$\langle\psi|\phi\rangle = \langle\psi|\Big(\alpha_1|\phi_1\rangle + \alpha_2|\phi_2\rangle\Big) = \alpha_1\langle\psi|\phi_1\rangle + \alpha_2\langle\psi|\phi_2\rangle$$

Inner products

Conjugate linearity in the first argument

Suppose that $|\psi_1\rangle$, $|\psi_2\rangle$, and $|\phi\rangle$ are vectors and β_1 and β_2 are complex numbers. If we define a new vector

$$|\psi\rangle = \beta_1|\psi_1\rangle + \beta_2|\psi_2\rangle$$

then

$$\langle\psi|\phi\rangle = \Bigl(\overline{\beta_1}\langle\psi_1| + \overline{\beta_2}\langle\psi_2|\Bigr)|\phi\rangle = \overline{\beta_1}\langle\psi_1|\phi\rangle + \overline{\beta_2}\langle\psi_2|\phi\rangle$$

Inner products

The Cauchy–Schwarz inequality

For every choice of vectors $|\psi\rangle$ and $|\phi\rangle$ we have

$$\big|\langle\psi|\phi\rangle\big| \leq \big\||\psi\rangle\big\| \, \big\||\phi\rangle\big\|$$

(Equality holds if and only if $|\psi\rangle$ and $|\phi\rangle$ are linearly dependent.)

Orthogonality and orthonormality

Two vectors $|\psi\rangle$ and $|\phi\rangle$ are *orthogonal* if their inner product is zero:

$$\langle\psi|\phi\rangle = 0$$

An *orthogonal set* $\{|\psi_1\rangle, \ldots, |\psi_m\rangle\}$ is one where all pairs pairs are orthogonal:

$$\langle\psi_j|\psi_k\rangle = 0 \qquad \text{(for all } j \neq k\text{)}$$

An *orthonormal set* $\{|\psi_1\rangle, \ldots, |\psi_m\rangle\}$ is an orthogonal set of unit vectors:

$$\langle\psi_j|\psi_k\rangle = \begin{cases} 1 & j = k \\ 0 & j \neq k \end{cases} \qquad \text{(for all } j \neq k\text{)}$$

An *orthonormal basis* $\{|\psi_1\rangle, \ldots, |\psi_m\rangle\}$ is an orthonormal set that forms a basis (of a given space).

Orthogonality and orthonormality

Example

For any classical state set Σ, the set of all standard basis vectors

$$\{|a\rangle : a \in \Sigma\}$$

is an orthonormal basis.

Example

The set $\{|+\rangle, |-\rangle\}$ is an orthonormal basis for the 2-dimensional space corresponding to a single qubit.

Example

The Bell basis $\{|\phi^+\rangle, |\phi^-\rangle, |\psi^+\rangle, |\psi^-\rangle\}$ is an orthonormal basis for the 4-dimensional space corresponding to two qubits.

Orthogonality and orthonormality

Example

The set $\{|+\rangle, |-\rangle\}$ is an orthonormal basis for the 2-dimensional space corresponding to a single qubit.

Example

The Bell basis $\{|\phi^+\rangle, |\phi^-\rangle, |\psi^+\rangle, |\psi^-\rangle\}$ is an orthonormal basis for the 4-dimensional space corresponding to two qubits.

Example

The set $\{|0\rangle, |+\rangle\}$ is not an orthogonal set because

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

Orthogonality and orthonormality

Fact

Suppose that

$$\{|\psi_1\rangle, \ldots, |\psi_m\rangle\}$$

is an *orthonormal set* of vectors in an n-dimensional space.

(Orthonormal sets are always linearly independent, so these vectors span a subspace of dimension $m \leq n$.)

If $m < n$, then there must exist vectors

$$|\psi_{m+1}\rangle, \ldots, |\psi_n\rangle$$

so that $\{|\psi_1\rangle, \ldots, |\psi_n\rangle\}$ forms an orthonormal basis.

(The *Gram–Schmidt* orthogonalization process can be used to construct these vectors.)

Orthogonality and orthonormality

Orthonormal bases are closely connected with unitary matrices.

These conditions on a square matrix U are equivalent:

1. The matrix U is unitary (i.e., $U^\dagger U = \mathbb{1} = UU^\dagger$).
2. The rows of U form an orthonormal basis.
3. The columns of U form an orthonormal basis.

For example, consider a 3×3 matrix U:

$$U^\dagger = \begin{pmatrix} \overline{\alpha_{1,1}} & \overline{\alpha_{2,1}} & \overline{\alpha_{3,1}} \\ \overline{\alpha_{1,2}} & \overline{\alpha_{2,2}} & \overline{\alpha_{3,2}} \\ \overline{\alpha_{1,3}} & \overline{\alpha_{2,3}} & \overline{\alpha_{3,3}} \end{pmatrix} \qquad U = \begin{pmatrix} \alpha_{1,1} & \alpha_{1,2} & \alpha_{1,3} \\ \alpha_{2,1} & \alpha_{2,2} & \alpha_{2,3} \\ \alpha_{3,1} & \alpha_{3,2} & \alpha_{3,3} \end{pmatrix}$$

Orthogonality and orthonormality

For example, consider a 3×3 matrix U:

$$U^\dagger = \begin{pmatrix} \overline{\alpha_{1,1}} & \overline{\alpha_{2,1}} & \overline{\alpha_{3,1}} \\ \overline{\alpha_{1,2}} & \overline{\alpha_{2,2}} & \overline{\alpha_{3,2}} \\ \overline{\alpha_{1,3}} & \overline{\alpha_{2,3}} & \overline{\alpha_{3,3}} \end{pmatrix} \qquad U = \begin{pmatrix} \alpha_{1,1} & \alpha_{1,2} & \alpha_{1,3} \\ \alpha_{2,1} & \alpha_{2,2} & \alpha_{2,3} \\ \alpha_{3,1} & \alpha_{3,2} & \alpha_{3,3} \end{pmatrix}$$

Forming vectors from the columns of U, we can express $U^\dagger U$ like this:

$$|\psi_1\rangle = \begin{pmatrix} \alpha_{1,1} \\ \alpha_{2,1} \\ \alpha_{3,1} \end{pmatrix} \qquad |\psi_2\rangle = \begin{pmatrix} \alpha_{1,2} \\ \alpha_{2,2} \\ \alpha_{3,2} \end{pmatrix} \qquad |\psi_3\rangle = \begin{pmatrix} \alpha_{1,3} \\ \alpha_{2,3} \\ \alpha_{3,3} \end{pmatrix}$$

$$U^\dagger U = \begin{pmatrix} \langle\psi_1|\psi_1\rangle & \langle\psi_1|\psi_2\rangle & \langle\psi_1|\psi_3\rangle \\ \langle\psi_2|\psi_1\rangle & \langle\psi_2|\psi_2\rangle & \langle\psi_2|\psi_3\rangle \\ \langle\psi_3|\psi_1\rangle & \langle\psi_3|\psi_2\rangle & \langle\psi_3|\psi_3\rangle \end{pmatrix}$$

Orthogonality and orthonormality

These conditions on a square matrix U are equivalent:

1. The matrix U is unitary (i.e., $U^\dagger U = \mathbb{1} = UU^\dagger$).
2. The rows of U form an orthonormal basis.
3. The columns of U form an orthonormal basis.

Fact

Given any orthonormal set of n-dimensional vectors

$$\{|\psi_1\rangle, \ldots, |\psi_m\rangle\}$$

there is a unitary matrix U whose first m columns are these vectors:

$$U = \begin{pmatrix} \vdots & \vdots & & \vdots & \vdots & & \vdots \\ |\psi_1\rangle & |\psi_2\rangle & \cdots & |\psi_m\rangle & |\psi_{m+1}\rangle & \cdots & |\psi_n\rangle \\ \vdots & \vdots & & \vdots & \vdots & & \vdots \end{pmatrix}$$

Projections

A square matrix Π is called a *projection* if it satisfies two properties:

1. $\Pi = \Pi^\dagger$
2. $\Pi^2 = \Pi$

Example

If $|\psi\rangle$ is a unit vector, then this matrix is a projection:

$$\Pi = |\psi\rangle\langle\psi|$$

$$\Pi^\dagger = (|\psi\rangle\langle\psi|)^\dagger = (\langle\psi|)^\dagger(|\psi\rangle)^\dagger = |\psi\rangle\langle\psi| = \Pi$$

$$(AB)^\dagger = B^\dagger A^\dagger$$

Projections

A square matrix Π is called a *projection* if it satisfies two properties:

1. $\Pi = \Pi^\dagger$
2. $\Pi^2 = \Pi$

Example

If $|\psi\rangle$ is a unit vector, then this matrix is a projection:

$$\Pi = |\psi\rangle\langle\psi|$$

$$\Pi^\dagger = \big(|\psi\rangle\langle\psi|\big)^\dagger = \big(\langle\psi|\big)^\dagger\big(|\psi\rangle\big)^\dagger = |\psi\rangle\langle\psi| = \Pi$$

$$\Pi^2 = \big(|\psi\rangle\langle\psi|\big)^2 = |\psi\rangle\langle\psi|\psi\rangle\langle\psi| = |\psi\rangle\langle\psi| = \Pi$$

Projections

A square matrix Π is called a *projection* if it satisfies two properties:

1. $\Pi = \Pi^\dagger$
2. $\Pi^2 = \Pi$

Example

If $\{|\psi_1\rangle, \ldots, |\psi_m\rangle\}$ is an orthonormal set, then this is a projection:

$$\Pi = \sum_{k=1}^{m} |\psi_k\rangle\langle\psi_k|$$

$$\Pi^\dagger = \left(\sum_{k=1}^{m} |\psi_k\rangle\langle\psi_k|\right)^\dagger = \sum_{k=1}^{m} \big(|\psi_k\rangle\langle\psi_k|\big)^\dagger = \sum_{k=1}^{m} |\psi_k\rangle\langle\psi_k| = \Pi$$

$$\Pi^2 = \sum_{j=1}^{m}\sum_{k=1}^{m} |\psi_j\rangle\langle\psi_j|\psi_k\rangle\langle\psi_k| = \sum_{k=1}^{m} |\psi_k\rangle\langle\psi_k| = \Pi$$

Projections

A square matrix Π is called a *projection* if it satisfies two properties:

1. $\Pi = \Pi^\dagger$
2. $\Pi^2 = \Pi$

Fact

Every projection matrix Π takes the form

$$\Pi = \sum_{k=1}^{m} |\psi_k\rangle\langle\psi_k|$$

for some orthonormal set $\{|\psi_1\rangle, \ldots, |\psi_m\rangle\}$.

(This includes the case $\Pi = 0$.)

Projective measurements

A collection of projections $\{\Pi_1, \ldots, \Pi_m\}$ that satisfies

$$\Pi_1 + \cdots + \Pi_m = \mathbb{1}$$

describes a *projective measurement.*

When such a measurement is performed on a system in the state $|\psi\rangle$, two things happen:

1. The outcome $k \in \{1, \ldots, m\}$ of the measurement is chosen randomly:

$$\Pr(\text{outcome is } k) = \big\| \Pi_k |\psi\rangle \big\|^2 = \langle\psi|\Pi_k|\psi\rangle$$

2. The state of the system becomes

$$\frac{\Pi_k |\psi\rangle}{\big\| \Pi_k |\psi\rangle \big\|}$$

Projective measurements

We can also choose different names for the measurement outcomes. Any collection of projections $\{\Pi_a : a \in \Gamma\}$ that satisfies the condition

$$\sum_{a \in \Gamma} \Pi_a = \mathbb{1}$$

describes a projective measurement having outcomes in the set Γ. The rules are the same as before:

1. The outcome $a \in \Gamma$ of the measurement is chosen randomly:

$$\Pr(\text{outcome is } a) = \big\| \Pi_a |\psi\rangle \big\|^2$$

2. The state of the system becomes

$$\frac{\Pi_a |\psi\rangle}{\big\| \Pi_a |\psi\rangle \big\|}$$

Projective measurements

Example

Standard basis measurements are projective measurements:

- The outcomes are the classical states of the system being measured.
- The measurement is described by the set $\{|a\rangle\langle a| : a \in \Sigma\}$.

Suppose that we measure the state

$$|\psi\rangle = \sum_{a\in\Sigma} \alpha_a |a\rangle$$

Each outcome a appears with probability $\big\| |a\rangle\langle a|\psi\rangle \big\|^2 = |\alpha_a|^2$.

Conditioned on the outcome a, the state becomes

$$\frac{|a\rangle\langle a|\psi\rangle}{\big\| |a\rangle\langle a|\psi\rangle \big\|} = \frac{\alpha_a}{|\alpha_a|}|a\rangle$$

Projective measurements

Example

Standard basis measurements are projective measurements:

- The outcomes are the classical states of the system being measured.
- The measurement is described by the set $\{|a\rangle\langle a| : a \in \Sigma\}$.

Example

Performing a standard basis measurement on a system X and doing nothing to a system Y is equivalent to performing the projective measurement

$$\{|a\rangle\langle a| \otimes \mathbb{1}_{\mathsf{Y}} : a \in \Sigma\}$$

on the system (X, Y).

Projective measurements

Example

Performing a standard basis measurement on a system X and doing nothing to a system Y is equivalent to performing the projective measurement

$$\{|a\rangle\langle a| \otimes \mathbb{1}_{\mathsf{Y}} \,:\, a \in \Sigma\}$$

on the system (X, Y).

Each measurement outcome a appears with probability

$$\big\| (|a\rangle\langle a| \otimes \mathbb{1}) |\psi\rangle \big\|^2$$

The state of the system (X, Y) then becomes

$$\frac{(|a\rangle\langle a| \otimes \mathbb{1}) |\psi\rangle}{\big\| (|a\rangle\langle a| \otimes \mathbb{1}) |\psi\rangle \big\|}$$

Projective measurements

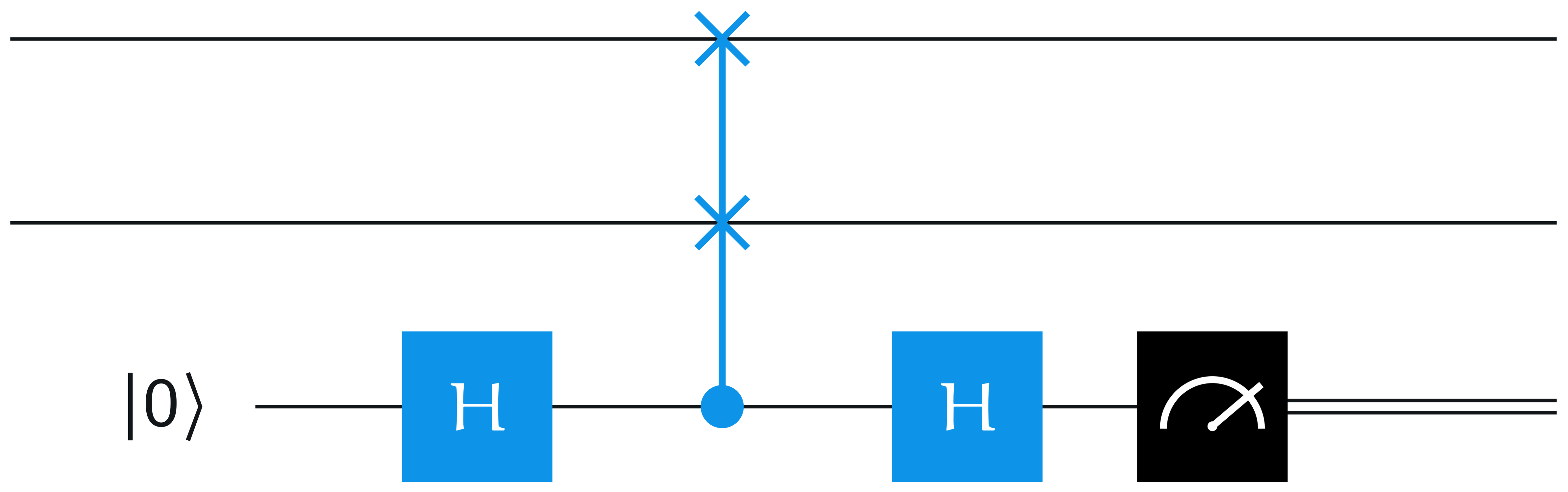
Example

Define two projections as follows:

$$\Pi_0 = |\phi\rangle\langle\phi^+| + |\phi^-\rangle\langle\phi^-| + |\psi^+\rangle\langle\psi^+|$$
$$\Pi_1 = |\psi^-\rangle\langle\psi^-|$$

The projective measurement $\{\Pi_0, \Pi_1\}$ is an interesting one...

Every projective measurements can be *implemented* using unitary operations and standard basis measurements.



Irrelevance of global phases

Definition

Suppose that $|\psi\rangle$ and $|\phi\rangle$ are quantum state vectors satisfying

$$|\phi\rangle = \alpha|\psi\rangle$$

The states $|\psi\rangle$ and $|\phi\rangle$ are then said to *differ by a global phase.*

(This requires $|\alpha| = 1$. Equivalently, $\alpha = e^{i\theta}$ for some real number θ.)

Imagine that two states that differ by a global phase are measured. If we start with the state $|\phi\rangle$, the probability to obtain any chosen outcome a is

$$|\langle a|\phi\rangle|^2 = |\alpha\langle a|\psi\rangle|^2 = |\alpha|^2|\langle a|\psi\rangle|^2 = |\langle a|\psi\rangle|^2$$

That's the same probability as if we started with the state $|\psi\rangle$.

Irrelevance of global phases

Definition

Suppose that $|\psi\rangle$ and $|\phi\rangle$ are quantum state vectors satisfying

$$|\phi\rangle = \alpha|\psi\rangle$$

The states $|\psi\rangle$ and $|\phi\rangle$ are then said to *differ by a global phase.*

(This requires $|\alpha| = 1$. Equivalently, $\alpha = e^{i\theta}$ for some real number θ.)

Imagine that two states that differ by a global phase are measured. If we start with the state $|\phi\rangle$, the probability to obtain any chosen outcome a is

$$\|\Pi_a|\phi\rangle\|^2 = \|\alpha\Pi_a|\psi\rangle\|^2 = |\alpha|^2\|\Pi_a|\psi\rangle\|^2 = \|\Pi_a|\psi\rangle\|^2$$

That's the same probability as if we started with the state $|\psi\rangle$.

Irrelevance of global phases

Definition

Suppose that $|\psi\rangle$ and $|\phi\rangle$ are quantum state vectors satisfying

$$|\phi\rangle = \alpha|\psi\rangle$$

The states $|\psi\rangle$ and $|\phi\rangle$ are then said to *differ by a global phase.*

(This requires $|\alpha| = 1$. Equivalently, $\alpha = e^{i\theta}$ for some real number θ.)

Suppose we apply a unitary operation to two states that differ by a global phase:

$$U|\phi\rangle = \alpha U|\psi\rangle = \alpha(U|\psi\rangle)$$

They still differ by a global phase...

Consequently, two quantum state vectors $|\psi\rangle$ and $|\phi\rangle$ that differ by a global phase are *completely indistinguishable* and are considered to be *equivalent.*

Irrelevance of global phases

Example

The quantum states

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

differ by a global phase.

Irrelevance of global phases

Example

The quantum states

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

do *not* differ by a global phase. (This is a *relative phase* difference.)

This is consistent with the observation that these states can be discriminated perfectly:

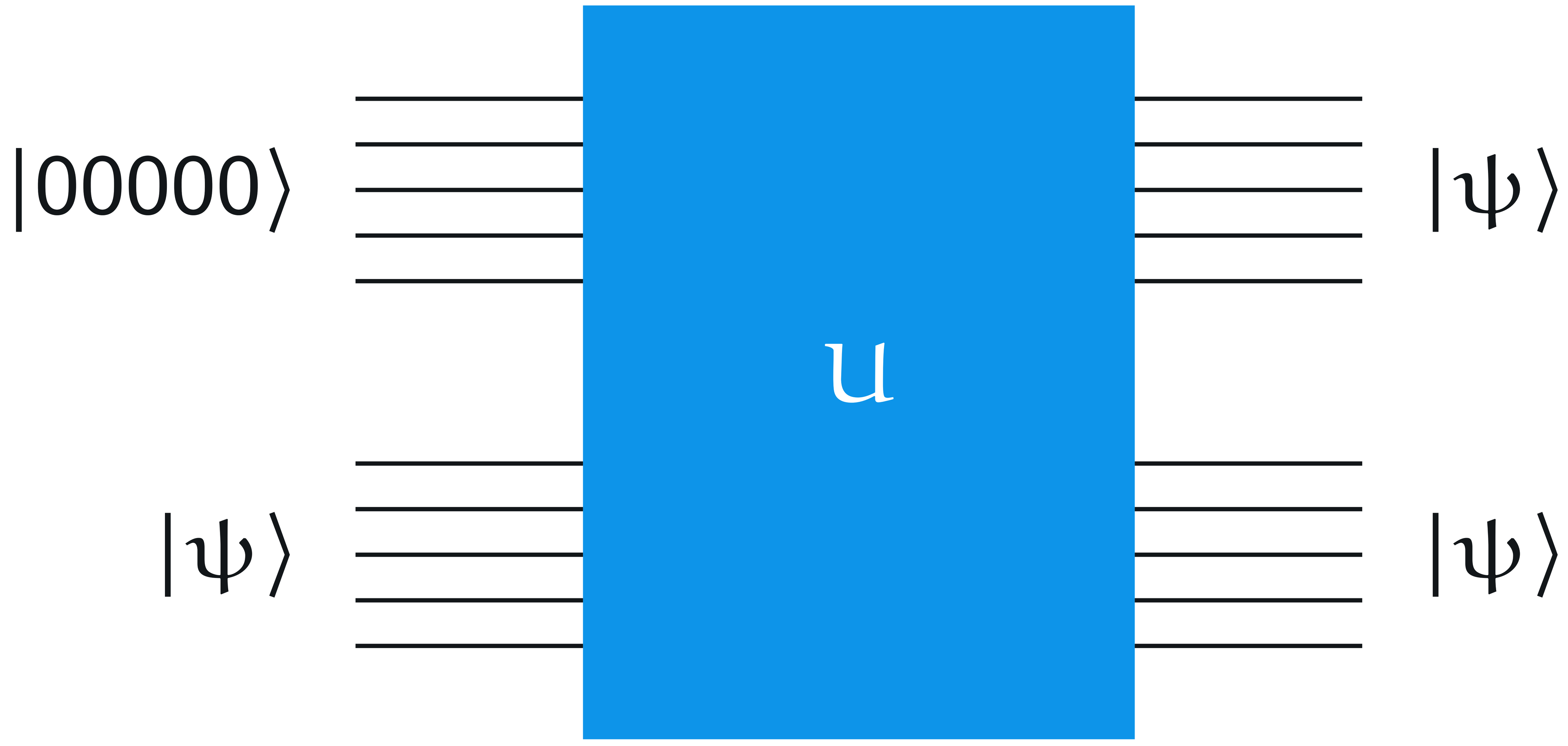
$$\begin{aligned} \left|\langle 0|\mathrm{H}|+\rangle\right|^2 &= 1 & \qquad \left|\langle 0|\mathrm{H}|-\rangle\right|^2 &= 0 \\ \left|\langle 1|\mathrm{H}|+\rangle\right|^2 &= 0 & \qquad \left|\langle 1|\mathrm{H}|-\rangle\right|^2 &= 1 \end{aligned}$$

No-cloning theorem

Theorem (No-cloning theorem)

Let X and Y both have the classical state set $\{0, \ldots, d-1\}$, where $d \geq 2$. There does not exist a unitary operation U on the pair (X, Y) such that

$$\forall |\psi\rangle : U(|\psi\rangle \otimes |0\rangle) = |\psi\rangle \otimes |\psi\rangle$$



No-cloning theorem

Theorem (No-cloning theorem)

Let X and Y both have the classical state set $\{0, \ldots, d-1\}$, where $d \geq 2$. There does not exist a unitary operation U on the pair (X, Y) such that

$$\forall |\psi\rangle : U(|\psi\rangle \otimes |0\rangle) = |\psi\rangle \otimes |\psi\rangle$$

The operation U must clone the standard basis states $|0\rangle$ and $|1\rangle$:

$$\begin{aligned} U(|0\rangle \otimes |0\rangle) &= |0\rangle \otimes |0\rangle \\ U(|1\rangle \otimes |0\rangle) &= |1\rangle \otimes |1\rangle \end{aligned}$$

Therefore, by linearity,

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

No-cloning theorem

Theorem (No-cloning theorem)

Let X and Y both have the classical state set $\{0, \ldots, d-1\}$, where $d \geq 2$. There does not exist a unitary operation U on the pair (X, Y) such that

$$\forall |\psi\rangle : U\big(|\psi\rangle \otimes |0\rangle\big) = |\psi\rangle \otimes |\psi\rangle$$

Therefore, by linearity,

$$U\bigg(\Big(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\Big) \otimes |0\rangle\bigg) = \frac{1}{\sqrt{2}}|0\rangle \otimes |0\rangle + \frac{1}{\sqrt{2}}|1\rangle \otimes |1\rangle$$

But this is not the correct behavior — we must have

$$\begin{aligned} &U\bigg(\Big(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\Big) \otimes |0\rangle\bigg) \\ &\qquad = \Big(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\Big) \otimes \Big(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\Big) \end{aligned}$$

No-cloning theorem

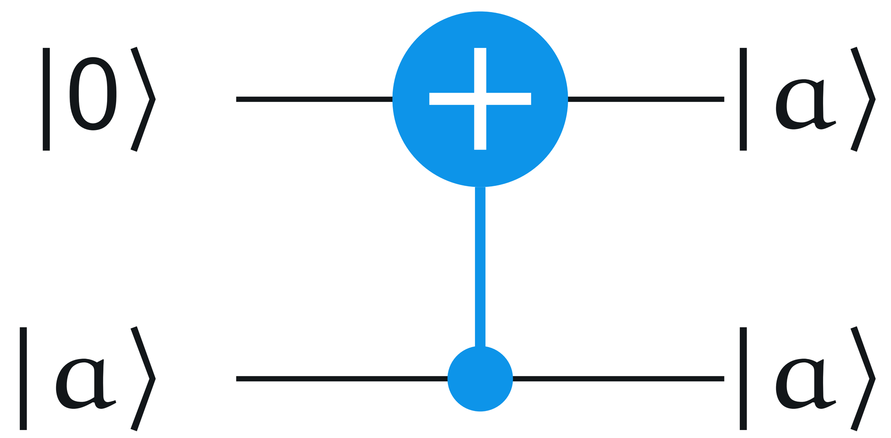
Theorem (No-cloning theorem)

Let X and Y both have the classical state set $\{0, \ldots, d-1\}$, where $d \geq 2$. There does not exist a unitary operation U on the pair (X, Y) such that

$$\forall |\psi\rangle : U\big(|\psi\rangle \otimes |0\rangle\big) = |\psi\rangle \otimes |\psi\rangle$$

Remarks:

- Approximate forms of the cloning theorem are known.
- Copying a standard basis state is possible — the no-cloning theorem does not contradict this.

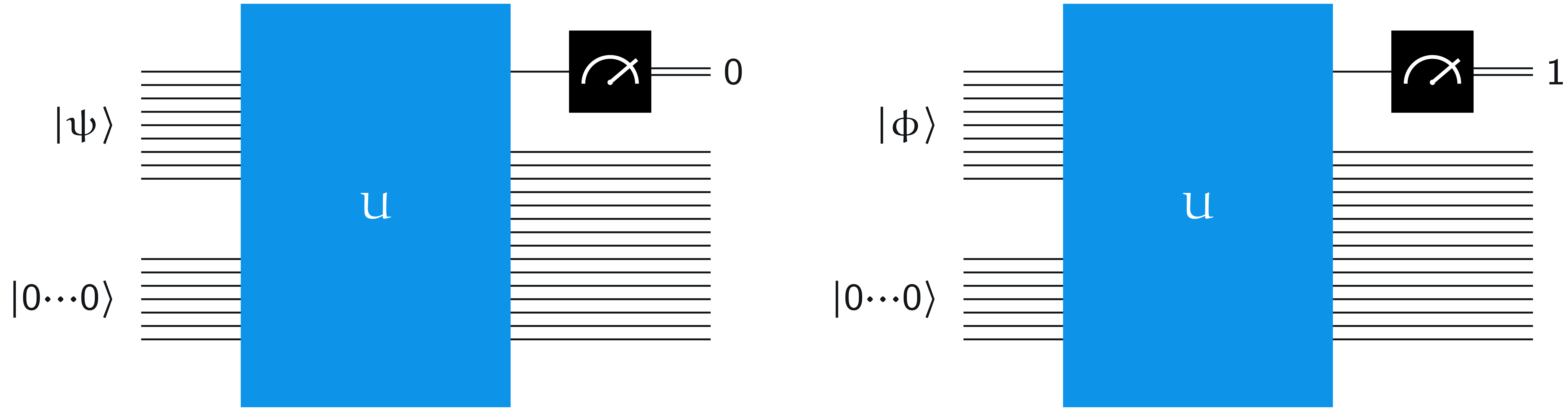


- Cloning a probabilistic state (classically) is also impossible.

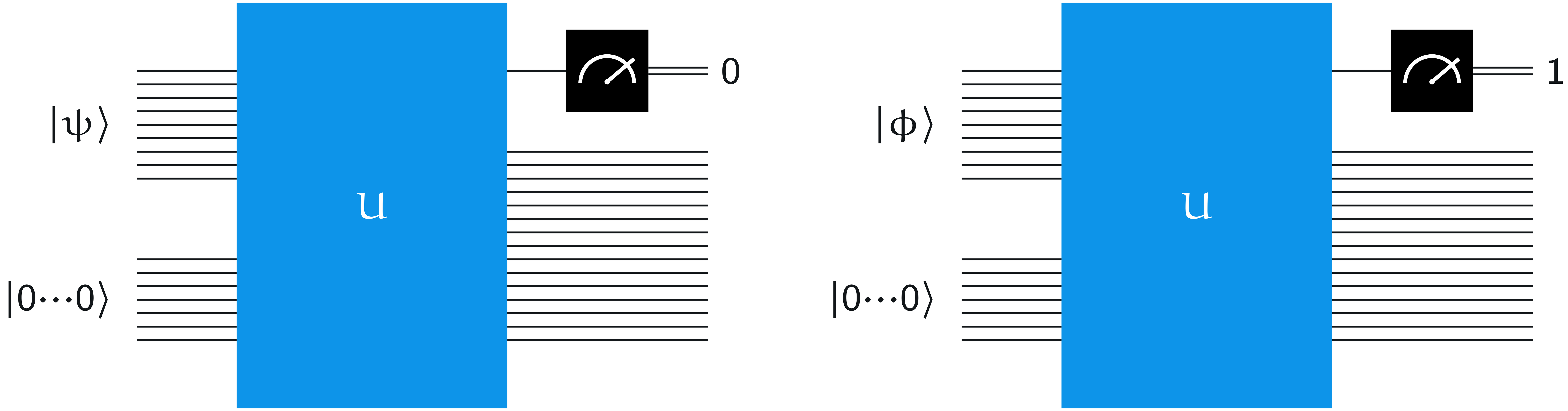
Discriminating non-orthogonal states

It is not possible to *perfectly discriminate* two non-orthogonal quantum states. Equivalently, if we can discriminate two quantum states perfectly, then they must be orthogonal.

Two states $|\psi\rangle$ and $|\phi\rangle$ can be discriminated perfectly if there is a unitary operation U that works like this:



Discriminating non-orthogonal states



$$U(|0\cdots0\rangle|\psi\rangle) = |\pi_0\rangle|0\rangle \qquad\qquad U(|0\cdots0\rangle|\phi\rangle) = |\pi_1\rangle|1\rangle$$

$$|0\cdots0\rangle|\psi\rangle = U^\dagger(|\pi_0\rangle|0\rangle) \qquad\qquad |0\cdots0\rangle|\phi\rangle = U^\dagger(|\pi_1\rangle|1\rangle)$$

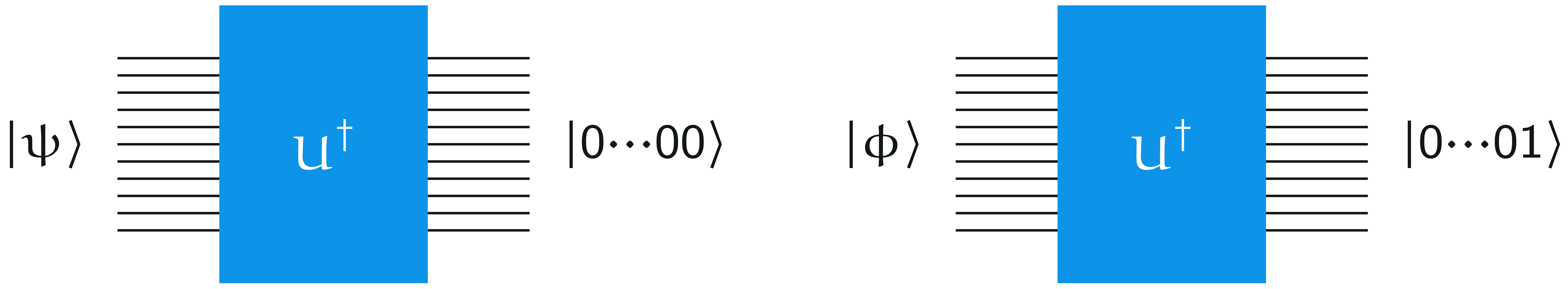
$$\begin{aligned}\langle\psi|\phi\rangle &= \langle 0\cdots0|0\cdots0\rangle\langle\psi|\phi\rangle \\ &= (\langle\pi_0|\langle 0|)UU^\dagger(|\pi_1\rangle|1\rangle) = \langle\pi_0|\pi_1\rangle\langle 0|1\rangle = 0\end{aligned}$$

Discriminating non-orthogonal states

Conversely, orthogonal quantum states can be perfectly discriminated.

In particular, if $|\psi\rangle$ and $|\phi\rangle$ are orthogonal, then any unitary matrix whose first two columns are $|\psi\rangle$ and $|\phi\rangle$ will work.

$$U = \begin{pmatrix} \vdots & \vdots & \\ |\psi\rangle & |\phi\rangle & \boxed{\;?\;} \\ \vdots & \vdots & \end{pmatrix}$$



Discriminating non-orthogonal states

Alternatively, we can define a projective measurement $\{\Pi_0, \Pi_1\}$ like this:

$$\Pi_0 = |\psi\rangle\langle\psi| \qquad \Pi_1 = \mathbb{1} - |\psi\rangle\langle\psi|$$

If we measure the state $|\psi\rangle$...

$$\Pr[\text{outcome is } 0] = \big\| \Pi_0 |\psi\rangle \big\|^2 = \big\| |\psi\rangle \big\|^2 = 1$$
$$\Pr[\text{outcome is } 1] = \big\| \Pi_1 |\psi\rangle \big\|^2 = \big\| 0 \big\|^2 = 0$$

If we measure any state $|\phi\rangle$ orthogonal to $|\psi\rangle$...

$$\Pr[\text{outcome is } 0] = \big\| \Pi_0 |\phi\rangle \big\|^2 = \big\| 0 \big\|^2 = 0$$
$$\Pr[\text{outcome is } 1] = \big\| \Pi_1 |\phi\rangle \big\|^2 = \big\| |\phi\rangle \big\|^2 = 1$$