A Hand-on Introduction to Quantum Computing with NVIDIA's CUDA-Q

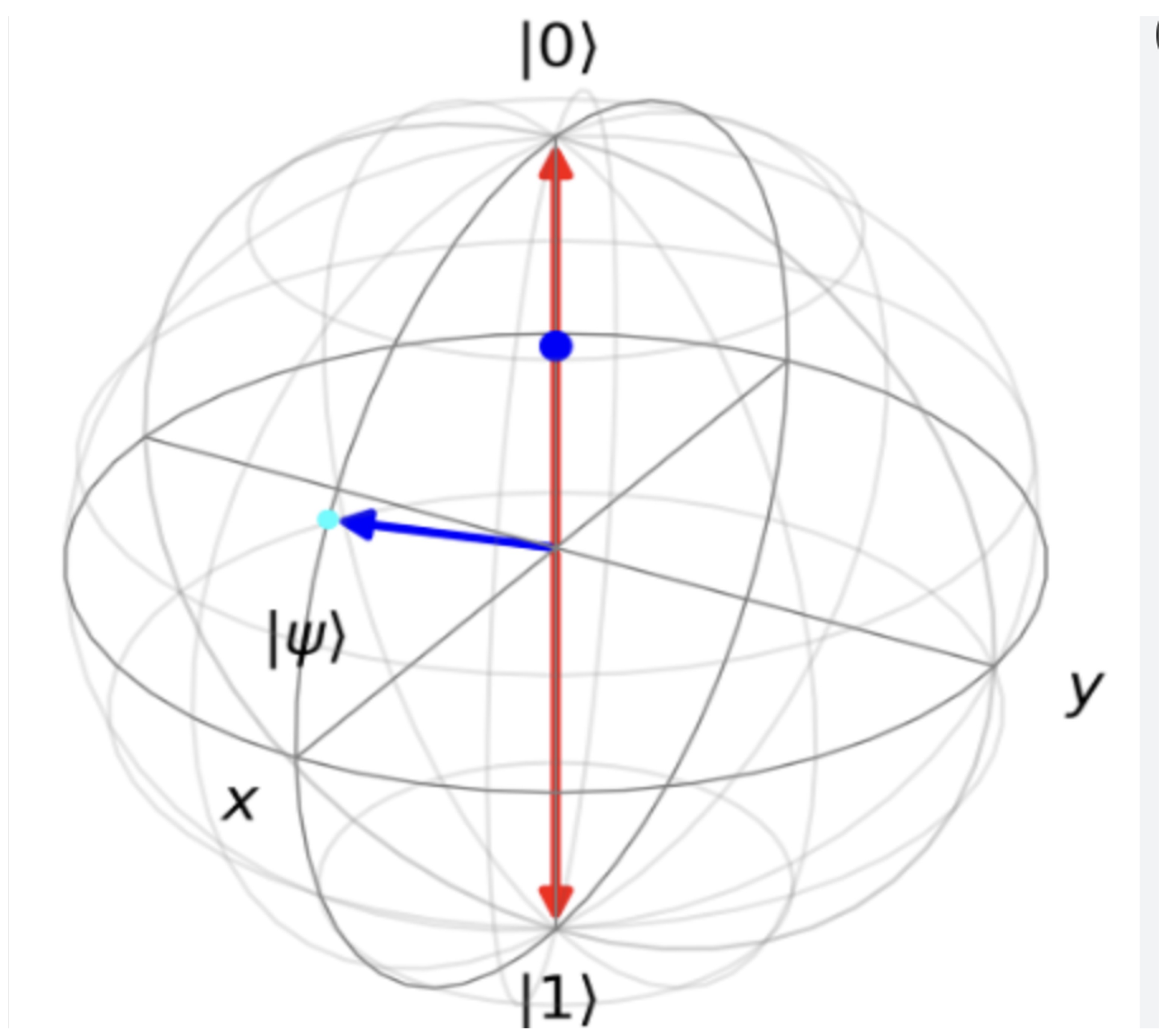
Marwa Farag, Quantum Algorithm Engineer | May 10, 2024.

Classical bit vs. quantum bit

Bit

0

1



Quantum states $|0\rangle$ and $|1\rangle$ form orthogonal basis also called computational basis or canonical basis.

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

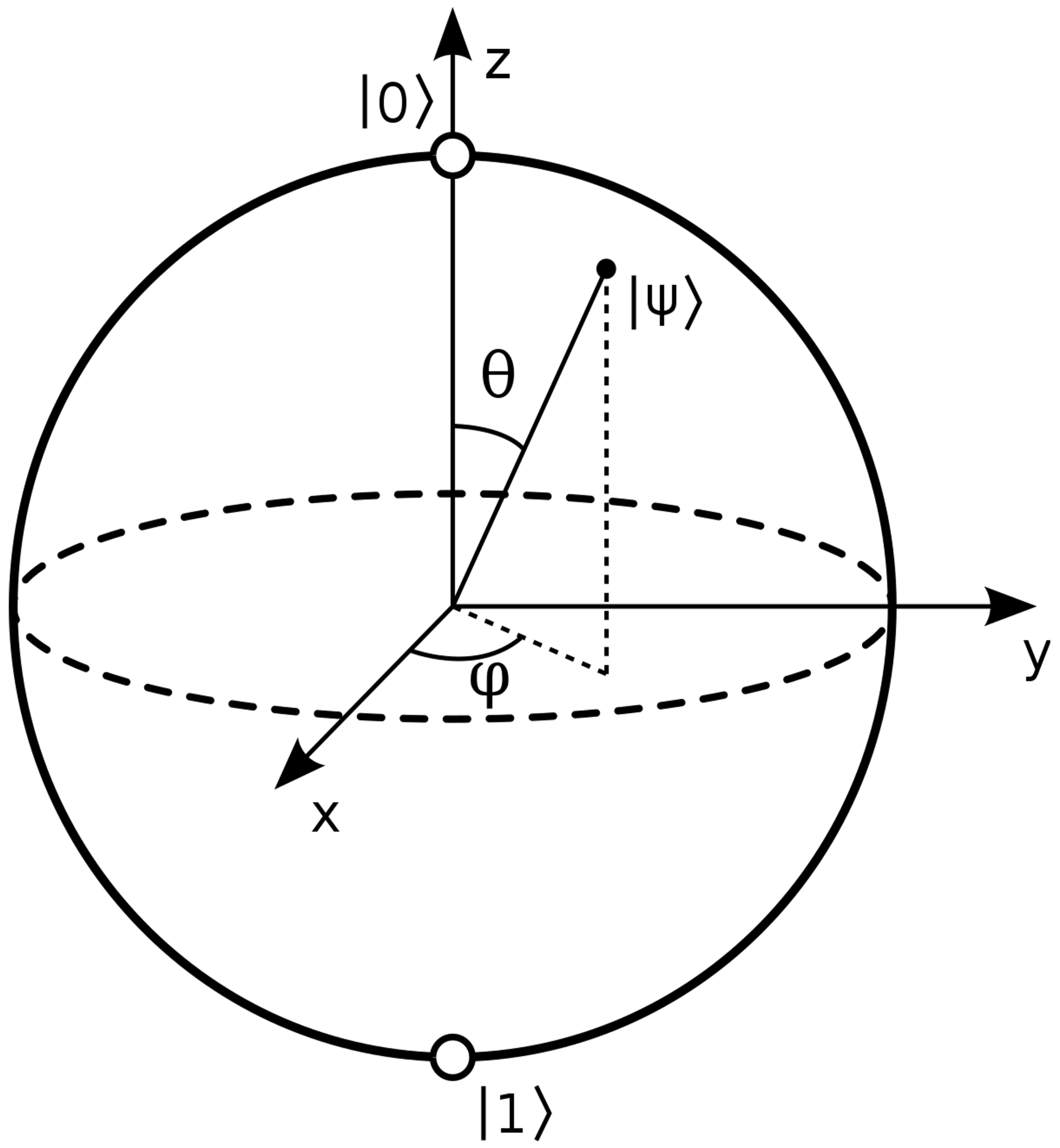
Qubit is a two-dimensional complex vector:

$$\begin{pmatrix} \alpha \\ \beta \end{pmatrix}.$$

- Classical bit can be either $|0\rangle$ or $|1\rangle$
- Quantum bit (qubit): can exist in $|0\rangle$ state, $|1\rangle$ state, or any state that is a linear combination of $|0\rangle$ and $|1\rangle$. The state of a qubit can be expressed as:

$|\phi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$ where α , β are complex numbers. → $|\alpha|^2 + |\beta|^2 = 1$

System of qubits



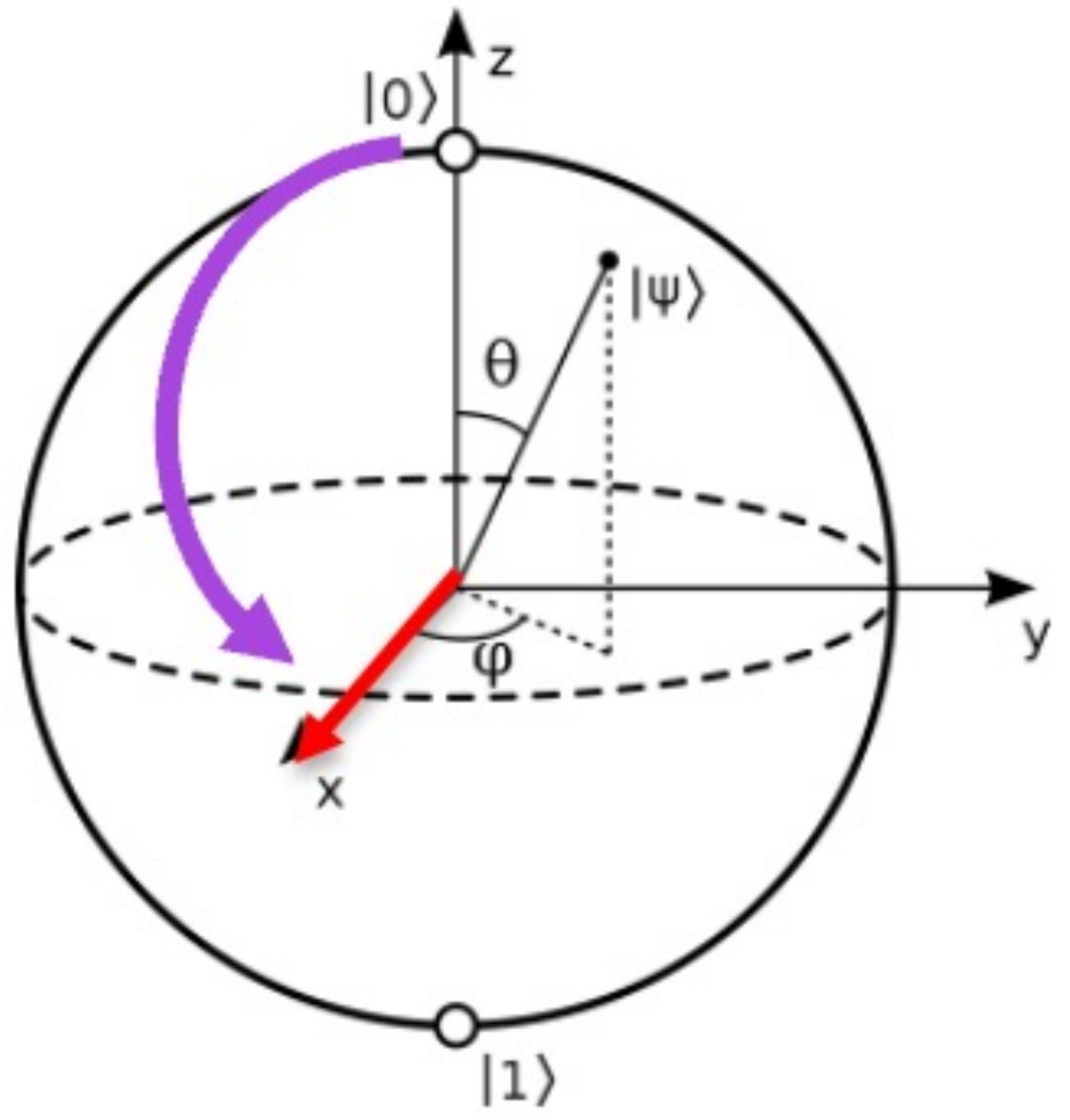
- Mathematical structure of a qubit generalized to higher dimensional quantum systems.
- The state of any quantum system is a normalized vector (a vector of norm 1) in a complex vector space.
- The joint state of a system of qubits is described using an operation known as the tensor product.

$$|\phi\rangle \otimes |\phi'\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \otimes \begin{pmatrix} \alpha' \\ \beta' \end{pmatrix} = \begin{pmatrix} \alpha\alpha' \\ \alpha\beta' \\ \beta\alpha' \\ \beta\beta' \end{pmatrix}$$

$$\begin{aligned} |\gamma_1\gamma_2\gamma_3\rangle &= |\gamma_1\rangle \otimes |\gamma_2\rangle \otimes |\gamma_3\rangle \\ &= \alpha_1\alpha_2\alpha_3 |000\rangle + \alpha_1\alpha_2\beta_3 |001\rangle + \alpha_1\beta_2\alpha_3 |010\rangle + \alpha_1\beta_2\beta_3 |011\rangle \\ &\quad + \beta_1\alpha_2\alpha_3 |100\rangle + \beta_1\alpha_2\beta_3 |101\rangle + \beta_1\beta_2\alpha_3 |110\rangle + \beta_1\beta_2\beta_3 |111\rangle \end{aligned}$$

$$|\gamma_j\rangle = \alpha_j |0\rangle + \beta_j |1\rangle$$

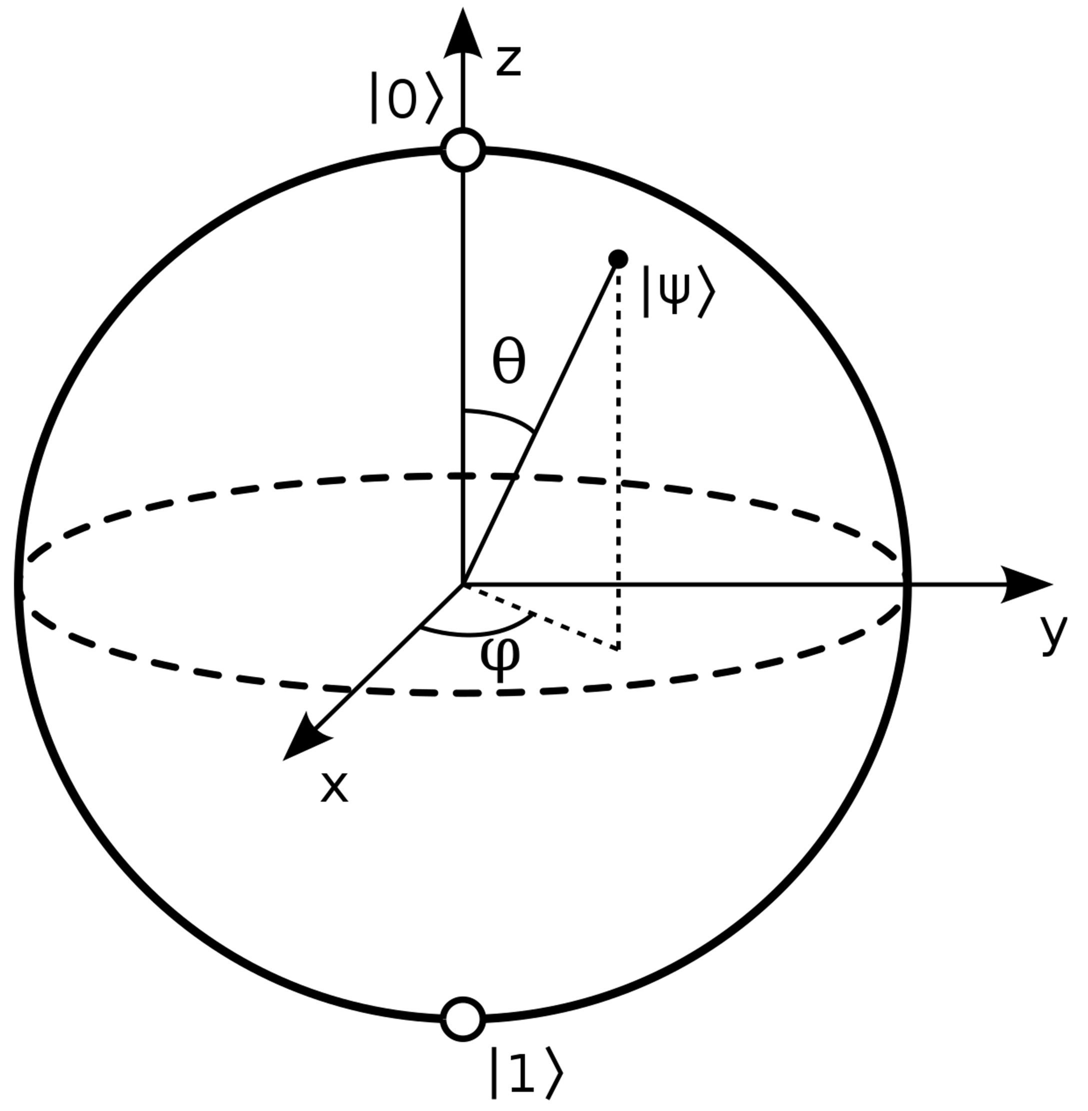
Superposition and entanglement



- **Superposition:** Any quantum state can be expressed as a linear combination of a few basis state.
- Qubit can be expressed as a linear combination of $|0\rangle$, $|1\rangle$. Similarly, the state of any n qubit system.
- Three qubits: complete state was the tensor product of three different single qubit state.
- **Entanglement:** state cannot be written as a tensor product of states of its individual subsystems.

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$$

Inner product and outer product



$$|\phi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$$

$$\begin{pmatrix}\alpha \\ \beta\end{pmatrix}$$

- **Inner product**: overlap between between two quantum state.
- Quantum states are vectors in complex vectors spaces.

$$|\phi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \text{ and } |\psi\rangle = \gamma\,|0\rangle + \delta\,|1\rangle$$

$$\langle\psi|\phi\rangle = \gamma^*\alpha + \delta^*\beta, \qquad |\phi\rangle = \begin{pmatrix}\alpha \\ \beta\end{pmatrix} \qquad \langle\phi| = \begin{pmatrix}\alpha^* & \beta^*\end{pmatrix}$$

- Overlap of a state with a bit string state will produce the corresponding coefficient. $\langle 0|\phi\rangle = \alpha$ and $\langle 1|\phi\rangle = \beta.$ $\langle 001|\gamma_1\gamma_2\gamma_3\rangle = \alpha_1\alpha_2\beta_3$

- Outer product of two states produces a matrix.

$$|\psi\rangle\langle\phi| = \begin{pmatrix}\alpha \\ \beta\end{pmatrix}\begin{pmatrix}\gamma^* & \delta^*\end{pmatrix} = \begin{pmatrix}\alpha\gamma^* & \alpha\delta^* \\ \beta\gamma^* & \beta\delta^*\end{pmatrix}$$

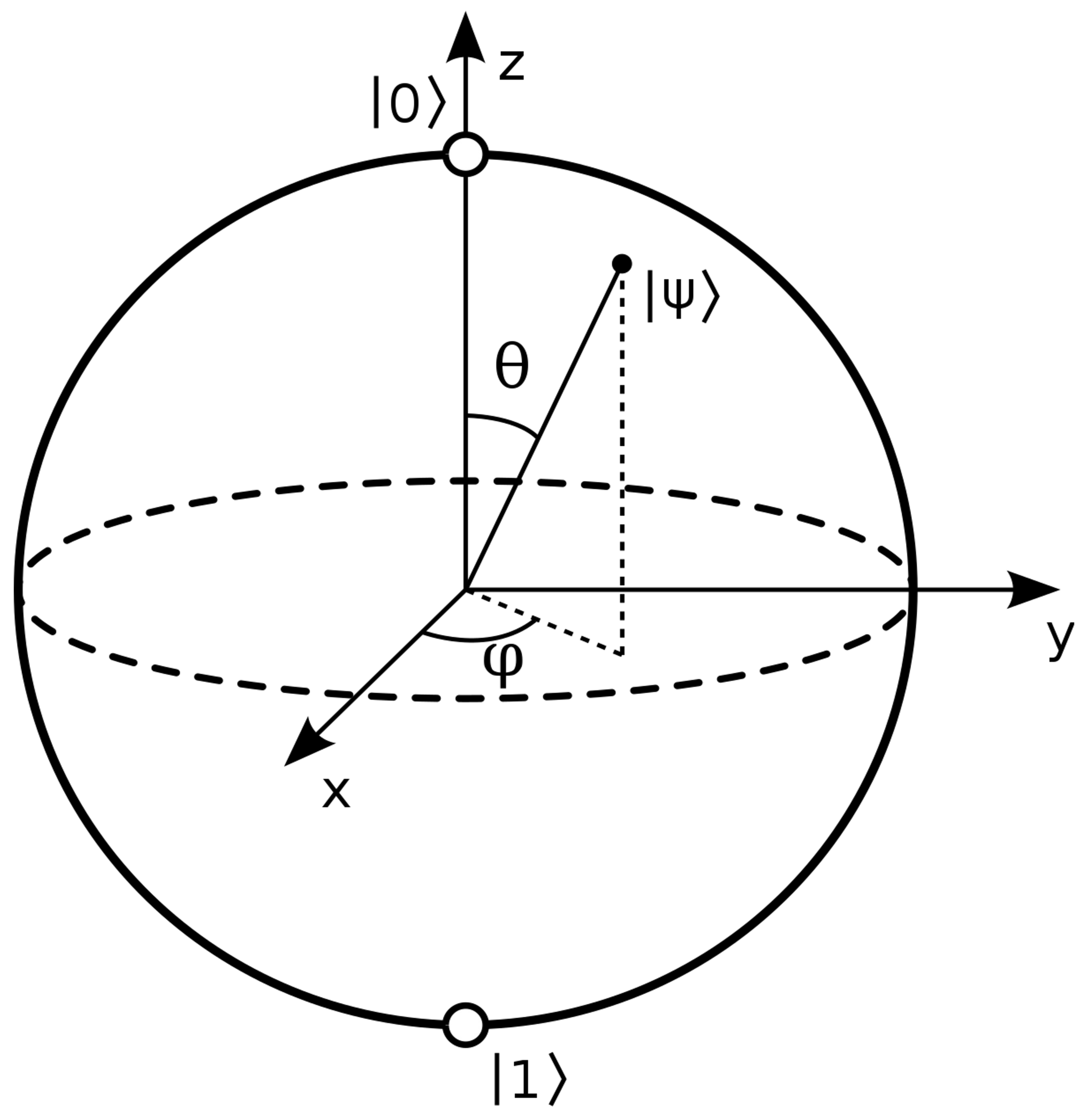
- Any matrix can be written as a linear combination of outer product between bit-string.

$$A = \begin{pmatrix}A_{00} & A_{01} \\ A_{10} & A_{11}\end{pmatrix} = A_{00}\,|0\rangle\langle 0| + A_{01}\,|0\rangle\langle 1| + A_{10}\,|1\rangle\langle 0| + A_{11}\,|1\rangle\langle 1|$$

- Acting on a state with a matrix: overlap between states

$$\begin{aligned} A\,|\phi\rangle &= A_{00}\,|0\rangle\langle 0|\phi\rangle + A_{01}\,|0\rangle\langle 1|\phi\rangle + A_{10}\,|1\rangle\langle 0|\phi\rangle + A_{11}\,|1\rangle\langle 1|\phi\rangle, \\ &= (A_{00}\alpha + A_{01}\beta)\,|0\rangle + (A_{10}\alpha + A_{11}\beta)\,|1\rangle = \begin{pmatrix}A_{00}\alpha + A_{01}\beta \\ A_{10}\alpha + A_{11}\beta\end{pmatrix}. \end{aligned}$$

Measurement in computational basis



- Measurement corresponds to transforming the quantum information into classical information.
- Measuring a qubit typically corresponds to reading out a classical bit.

$$|\phi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$$

- The probability of obtaining $|0\rangle$ after measurement is $|\langle 0|\phi\rangle|^2$
- The probability of obtaining $|1\rangle$ after measurement is $|\langle 1|\phi\rangle|^2$

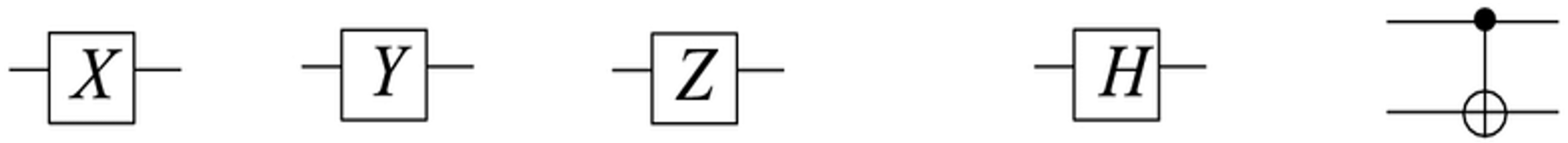
- Measurement can be represented as the squared absolute values of overlaps.
- A central principle of quantum mechanics is that measurement outcomes are probabilistic.

- Generalizing: the probability of getting the bit string $|x_1 \ldots x_n\rangle$

after measuring an n qubit state $|\phi\rangle$ is then $|\langle x_1 \ldots x_n|\phi\rangle|^2$

$|\psi\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$ → Probability is 0.5

Unitary transformation and quantum gates



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

- Gates are unitary transformation
- Quantum gates are reversible
- Reversible means that the gate's input can always be reconstructed from the gate's output.

- A qubit or a system of qubits changes its state by going through a series of unitary transformation.
- A matrix U is called unitary if:

$$UU^\dagger = U^\dagger U = I$$

$U^\dagger \rightarrow$ The transposed, complex conjugate of U (Hermitian operator)

- A qubit state $|\phi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$ evolves under the action of $2\ x\ 2$ matrix U as

$$|\phi\rangle \rightarrow U\,|\phi\rangle = \begin{pmatrix} U_{00} & U_{01} \\ U_{10} & U_{11} \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} U_{00}\alpha + U_{01}\beta \\ U_{10}\alpha + U_{11}\beta \end{pmatrix}$$

- Operators acting on different qubits can be combined using tensor product. $U_1 \otimes U_2$

Observable and expectation values

$$\langle\phi|Z|\phi\rangle = \langle\phi|0\rangle\langle 0|\phi\rangle - \langle\phi|1\rangle\langle 1|\phi\rangle = |\alpha|^2 - |\beta|^2$$

$$|\phi\rangle = \alpha|0\rangle + \beta|1\rangle \qquad Z = |0\rangle\langle 0| - |1\rangle\langle 1| = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

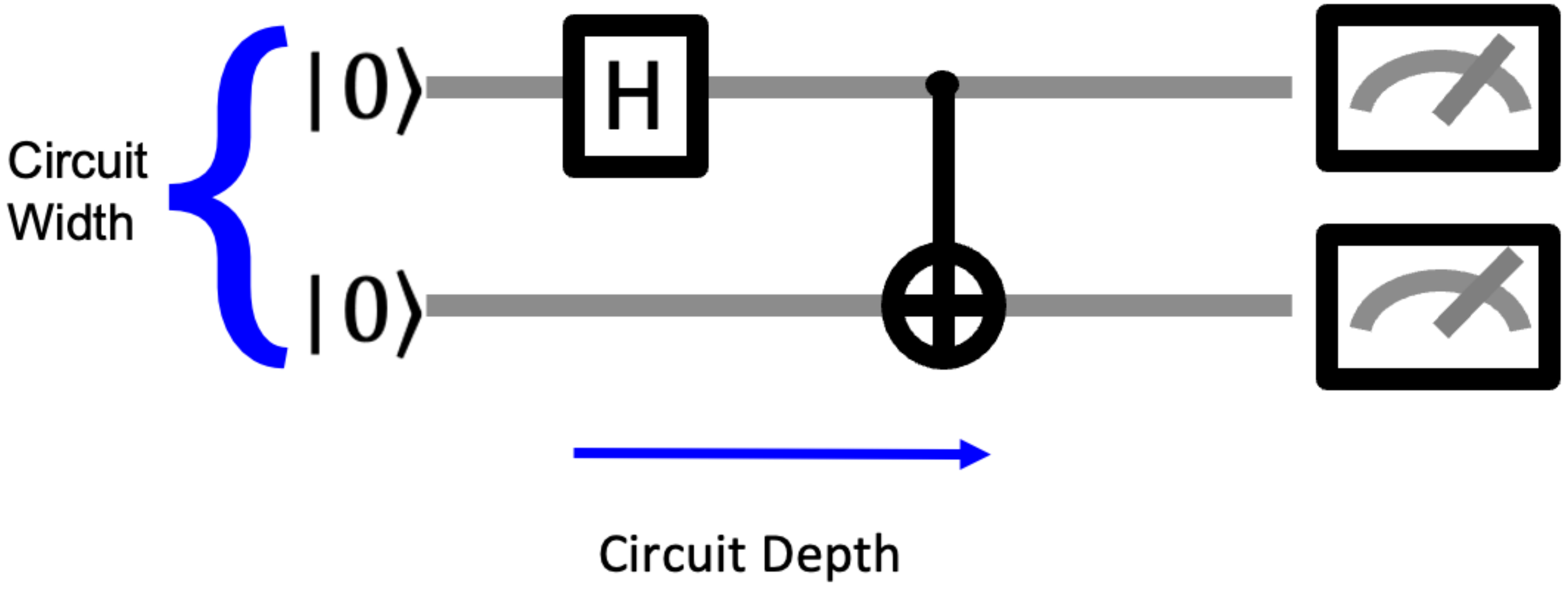
Z operator is called the observable. And the quantity $\langle\phi|Z|\phi\rangle$ is called its expectation value.

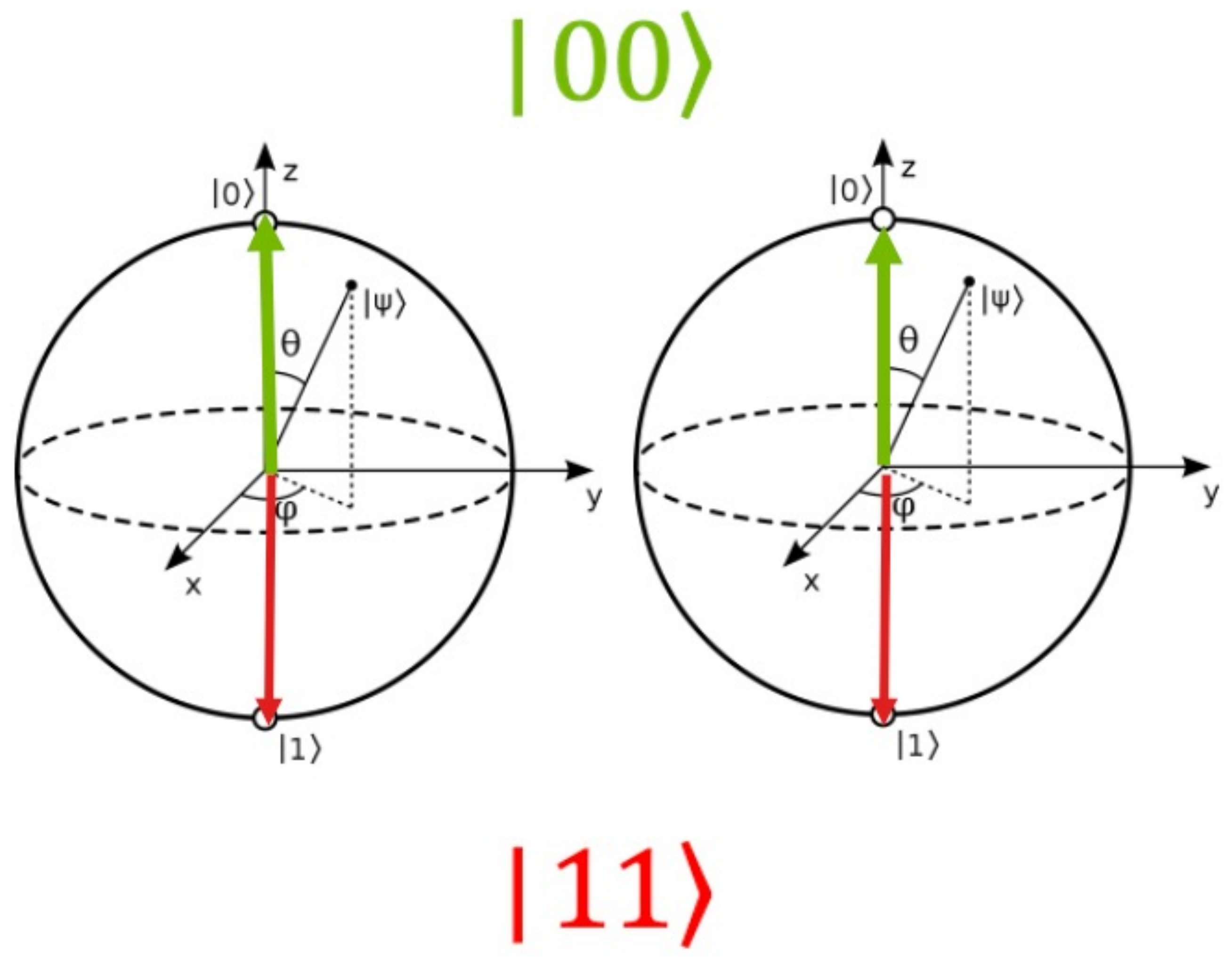
$$O \equiv \sum_i a_i |\Phi_i\rangle\langle\Phi_i| \qquad \langle\psi|O|\psi\rangle = \sum_i a_i \langle\psi|\Phi_i\rangle\langle\Phi_i|\psi\rangle = \sum_i a_i |\langle\Phi_i|\psi\rangle|^2$$

O is called Hermitian operator. These operators are equal to their Hermitian conjugates $(O = O^\dagger)$.

In quantum mechanics, any Hermitian operator is a valid observable.

Quantum circuit





$$\mathrm{CNOT}_{12}\,(H \otimes I)\,|00\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle).$$

Hadamard Gate:

$\mathrm{Had}|0\rangle = |0\rangle + |1\rangle$

$\mathrm{Had}|1\rangle = |0\rangle - |1\rangle$

CNOT Gate:

$\mathrm{CNOT}|10\rangle = |11\rangle$

$\mathrm{CNOT}|11\rangle = |10\rangle$

$$H \otimes I\,|00\rangle = (H\,|0\rangle) \otimes (I\,|0\rangle) = \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) \otimes |0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle)$$

$$\mathrm{CNOT}_{12}\left(\frac{1}{\sqrt{2}}(|00\rangle + |10\rangle)\right) = \frac{1}{\sqrt{2}}(\mathrm{CNOT}_{12}\,|00\rangle + \mathrm{CNOT}_{12}\,|10\rangle) = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

No-cloning theorem

No-cloning theorem: copying of state is prohibited.

$$U\,|\varphi\rangle\,|0\rangle \;=\; |\varphi\rangle\,|\varphi\rangle, \qquad U\,|\phi\rangle\,|0\rangle = |\phi\rangle|\phi\rangle$$

It follows from linearity that

$$U\,(a\,|\varphi\rangle + b\,|\phi\rangle\,)|0\rangle = a\,U\,|\varphi\rangle\,|0\rangle + b\,U|\phi\rangle|0\rangle = a\,|\varphi\rangle\,|\varphi\rangle + b\,|\phi\rangle\,|\phi\rangle$$

But if U cloned arbitrary inputs, we would have

$$U(a\,|\varphi\rangle + b\,|\phi\rangle\,)|0\rangle \;= (a\,|\varphi\rangle + b\,|\phi\rangle)(a\,|\varphi\rangle + b\,|\phi\rangle) = \;a^2\,|\varphi\rangle\,|\varphi\rangle$$
$$+\; b^2\,|\phi\rangle\,|\phi\rangle + ab\,|\varphi\rangle|\phi\rangle + ba\,|\phi\rangle|\varphi\rangle$$

NVIDIA