VI Workshop Escola de Computação e Informação Quântica - unifal-mg.edu.br/weciq

Introduction to Quantum Programming with Ket

⟨G|C|Q⟩ UFSC

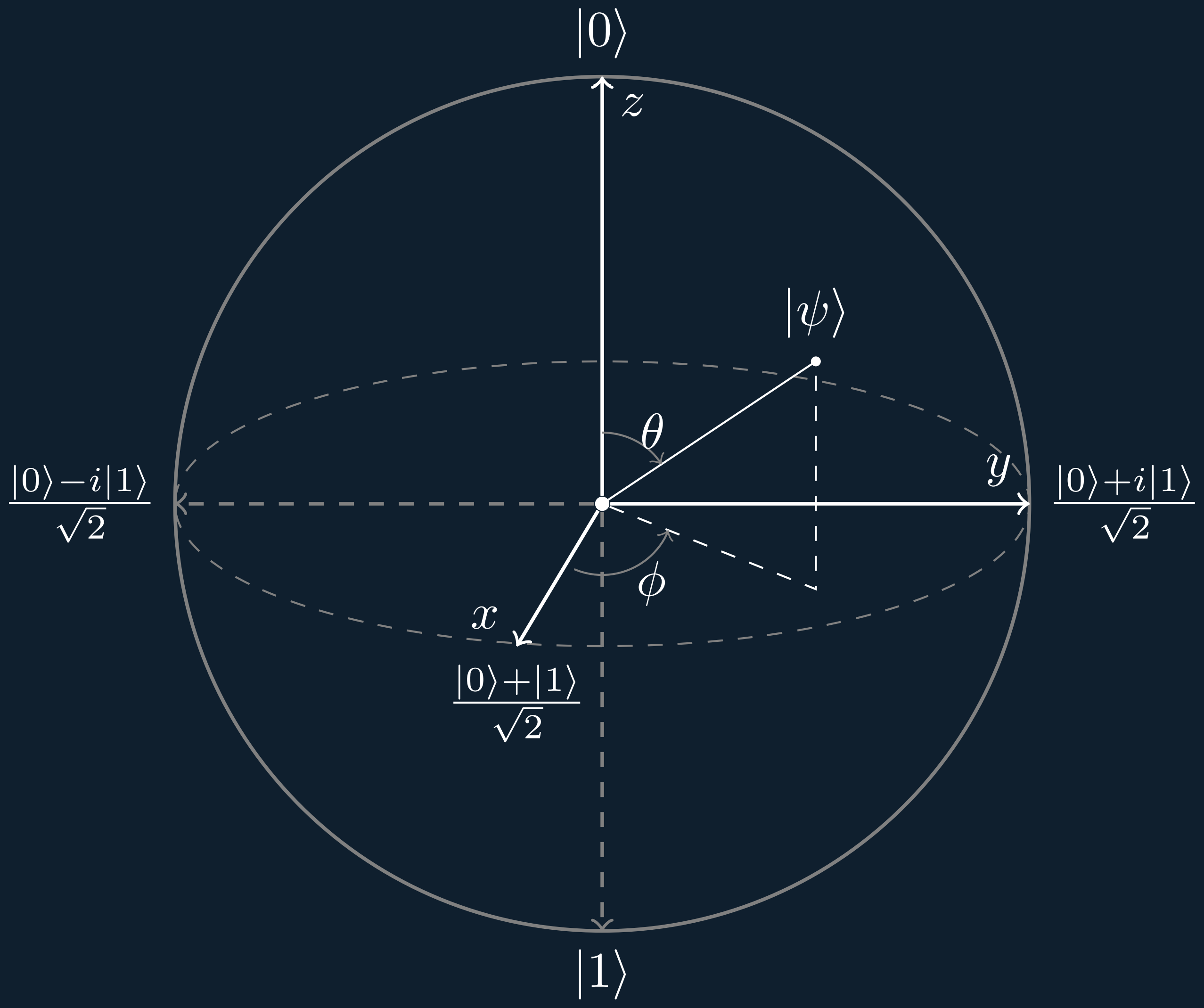
quantuloop

Agenda

- Quantum Computing in a Nutshell
- Quantum Programming Today
- Quantum Bit & Superposition
- Quantum Gates & Entanglement
- Quantum Measurement
- Postulates of Quantum Mechanics
- Quantum Algorithms

Quantum Computing

in a Nutshell



Qubit

$|0\rangle$ & $|1\rangle$

Superposition

- $\alpha\,|0\rangle + \beta\,|1\rangle$
- $|\alpha|^2 + |\beta|^2 = 1$

2-Qubits

- $\alpha\left|00\right\rangle + \beta\left|01\right\rangle + \gamma\left|10\right\rangle + \delta\left|11\right\rangle$
- $|\alpha|^2 + |\beta|^2 + |\gamma|^2 + |\delta|^2 = 1$

n-Qubits

- $\sum_{k=0}^{2^n-1} \alpha_k \left|k\right\rangle$
- $\sum_{k=0}^{2^n-1} \left|\alpha_k\right|^2 = 1$

Tensor Product

$$|\psi\rangle \otimes |\varphi\rangle = |\psi\rangle\,|\varphi\rangle = |\psi\varphi\rangle$$

$$(\alpha\,|0\rangle + \beta\,|1\rangle) \otimes (\gamma\,|0\rangle + \delta\,|1\rangle) = \alpha\gamma\,|00\rangle + \alpha\delta\,|01\rangle + \beta\gamma\,|10\rangle + \beta\delta\,|11\rangle$$

Entanglement

$$(\alpha\,|0\rangle + \beta\,|1\rangle) \otimes (\gamma\,|0\rangle + \delta\,|1\rangle) \neq \frac{1}{\sqrt{2}}\,|00\rangle + \frac{1}{\sqrt{2}}\,|11\rangle$$

Measurement

$$\alpha\left|0\right\rangle + \beta\left|1\right\rangle$$

- $p(0) = |\alpha|^2 \Rightarrow \frac{\alpha}{|\alpha|}\left|0\right\rangle$
- $p(1) = |\beta|^2 \Rightarrow \frac{\beta}{|\beta|}\left|1\right\rangle$

Measurement

$$\sum_{k=0}^{2^n-1} \alpha_k \left|k\right\rangle$$

- $p(k) = |\alpha_k|^2 \Rightarrow \frac{\alpha_k}{|\alpha_k|} \left|k\right\rangle$

Measurement

$$\alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle$$

- $p(0_0) = |\alpha|^2 + |\beta|^2 \Rightarrow \frac{\alpha|00\rangle + \beta|01\rangle}{\sqrt{|\alpha|^2 + |\beta|^2}}$
- $p(0_1) = |\alpha|^2 + |\gamma|^2 \Rightarrow \frac{\alpha|00\rangle + \gamma|10\rangle}{\sqrt{|\alpha|^2 + |\gamma|^2}}$
- $p(1_0) = |\gamma|^2 + |\delta|^2 \Rightarrow \frac{\gamma|10\rangle + \delta|11\rangle}{\sqrt{|\gamma|^2 + |\delta|^2}}$
- $p(1_1) = |\beta|^2 + |\delta|^2 \Rightarrow \frac{\beta|01\rangle + \delta|11\rangle}{\sqrt{|\beta|^2 + |\delta|^2}}$

Quantum Programming

Today

Quantum Computing (QC)

- ✅ Use Quantum Mechanics to Compute
- ❌ Science Fiction
- ❌ Substitute for Classical Computing

QC Motivation

- Simulation of Quantum Systems [Feynman 1982]
- Integer Factoring [Shor 1997]
- Acceleration in
  - Artificial Intelligence
  - Chemistry & Biomedicine
  - Logistics & Optimization

QC Today

- Quantum Advantage Milestone [Arute *et al.* 2019]
- Noisy Intermediate-Scale Quantum (NISQ) era
- Cloud-Based Quantum Computers
- Test Applications Using Quantum Simulator

Ket Quantum Programming

Classical-Quantum Programming Language **Ket**

- Python-Embedded Language 🐍
- Open-Source Project 🔓

Quantum Bit

Quantum Computing from a **Computer Science** perspective

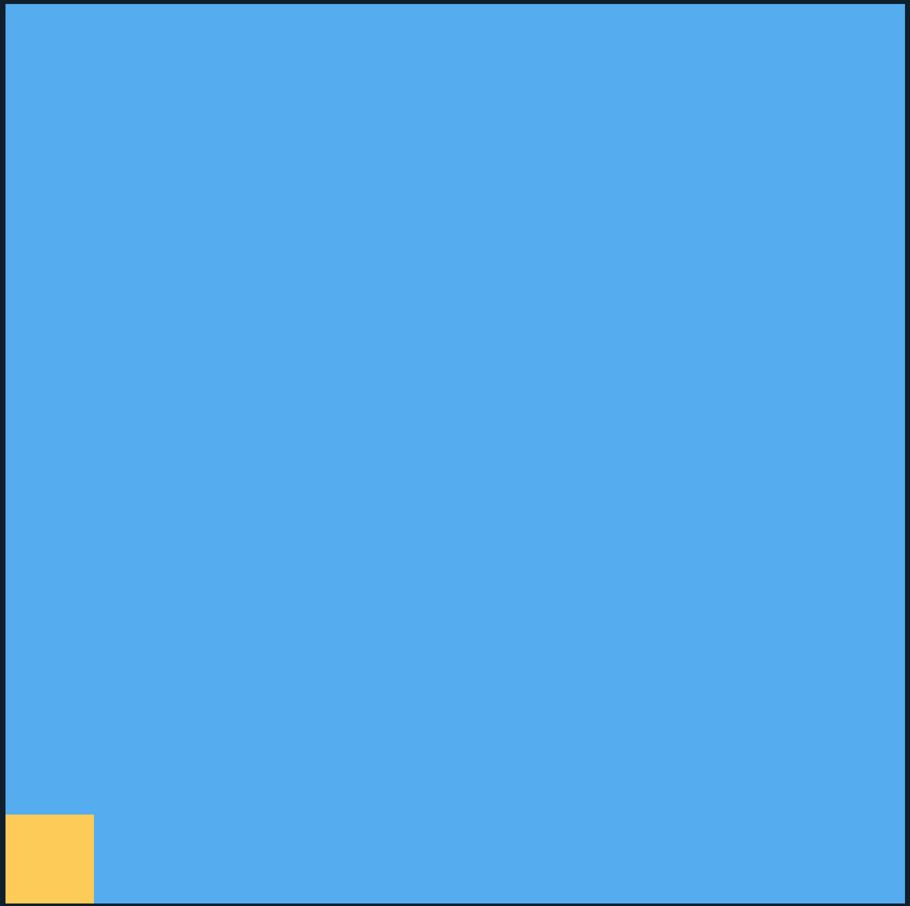
Qubit

$$\alpha |0\rangle + \beta |1\rangle$$

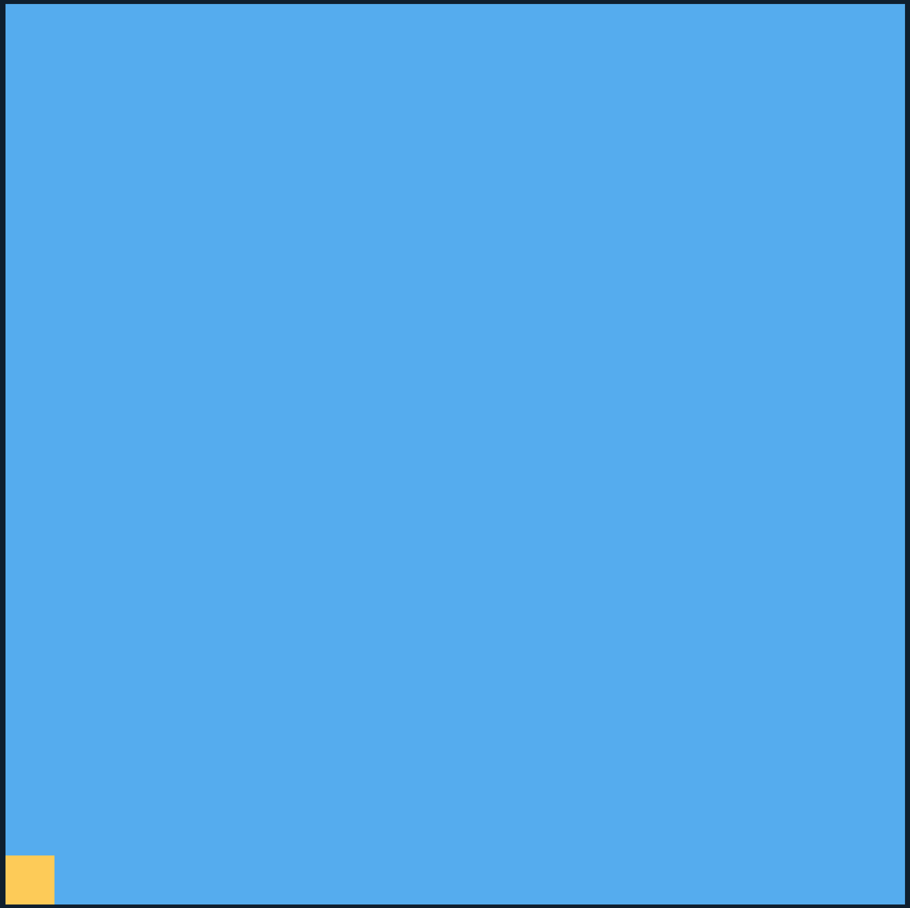
Quantum Superposition

n-Qubits $\equiv 2^n$-Bits

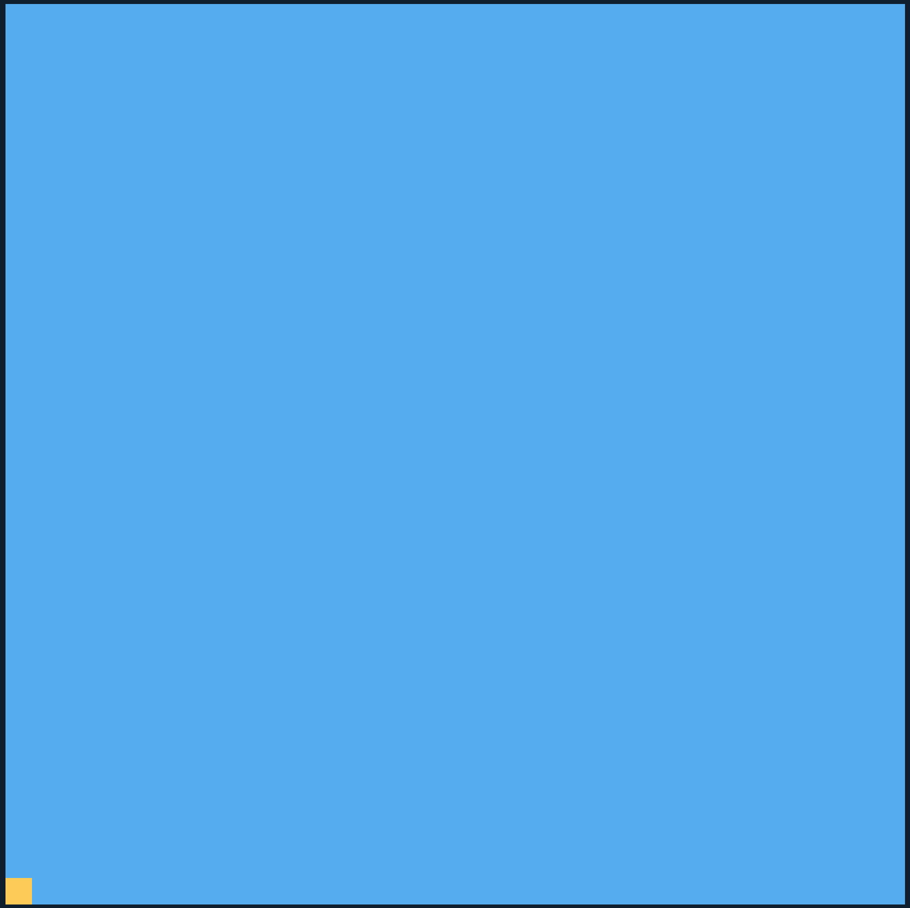
- 1-Qubit $\equiv$ 2-Bits
  $[|0\rangle]_1, [|1\rangle]_2, [|0\rangle + |1\rangle]_3$
- 2-Qubit $\equiv$ 4-Bits
  $[|00\rangle]_1, [|01\rangle]_2, [|10\rangle]_3, [|11\rangle]_4,$
  $[|00\rangle + |01\rangle]_5, [|00\rangle + |10\rangle]_6, [|00\rangle + |11\rangle]_7,$
  $[|01\rangle + |10\rangle]_8, [|01\rangle + |11\rangle]_9, [|10\rangle + |11\rangle]_{10},$
  $[|00\rangle + |01\rangle + |10\rangle]_{11}, [|00\rangle + |01\rangle + |11\rangle]_{12},$
  $[|00\rangle + |10\rangle + |11\rangle]_{13}, [|01\rangle + |10\rangle + |11\rangle]_{14},$
  $[|00\rangle + |01\rangle + |10\rangle + |11\rangle]_{15}$



- 10-Qubits ($\equiv$ 1.024-Bits)
- 10-Bits

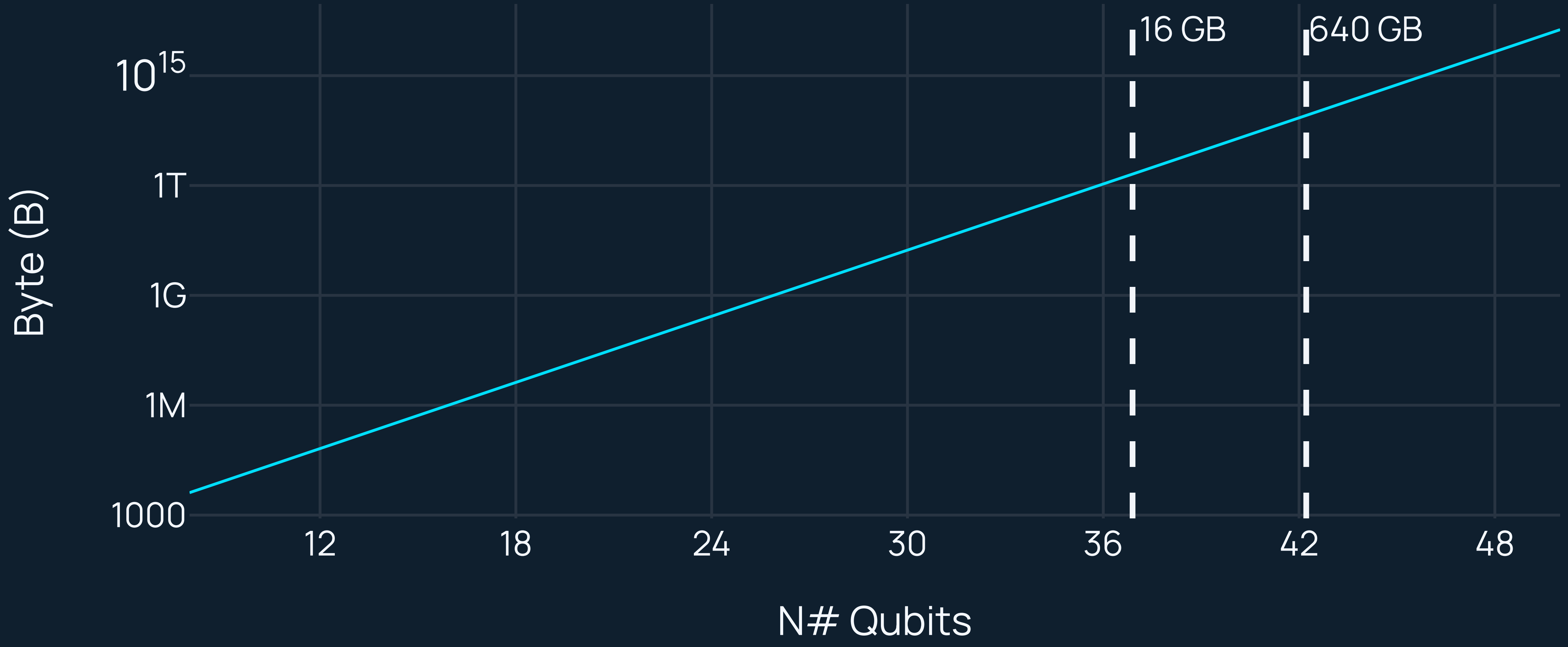


- 12-Qubits ($\equiv$ 4.096-Bits)
- 12-Bits



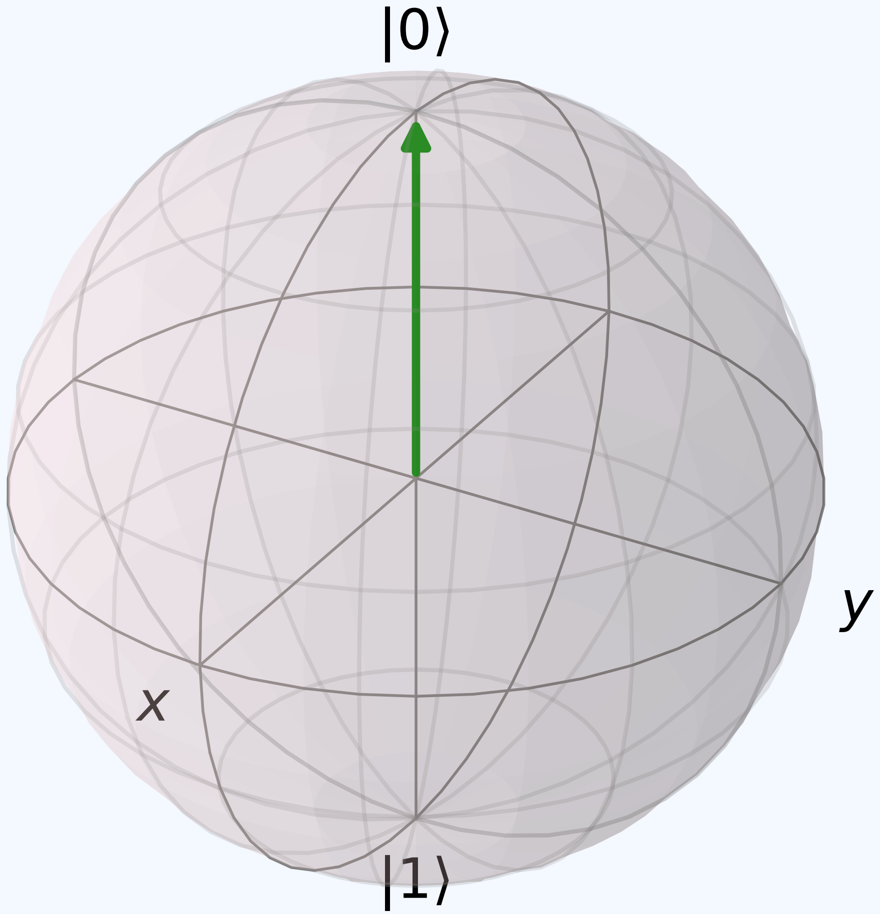
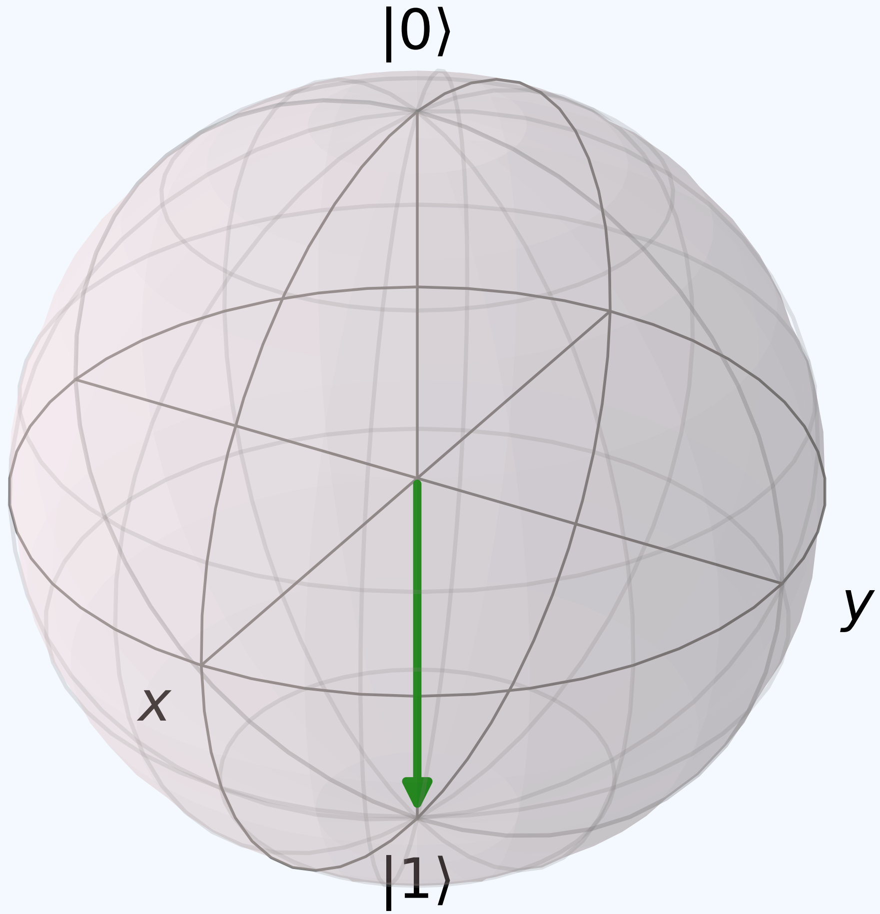
- 14-Qubits ($\equiv$ 16.384-Bits)
- 14-Bits

Qubits vs. Bytes

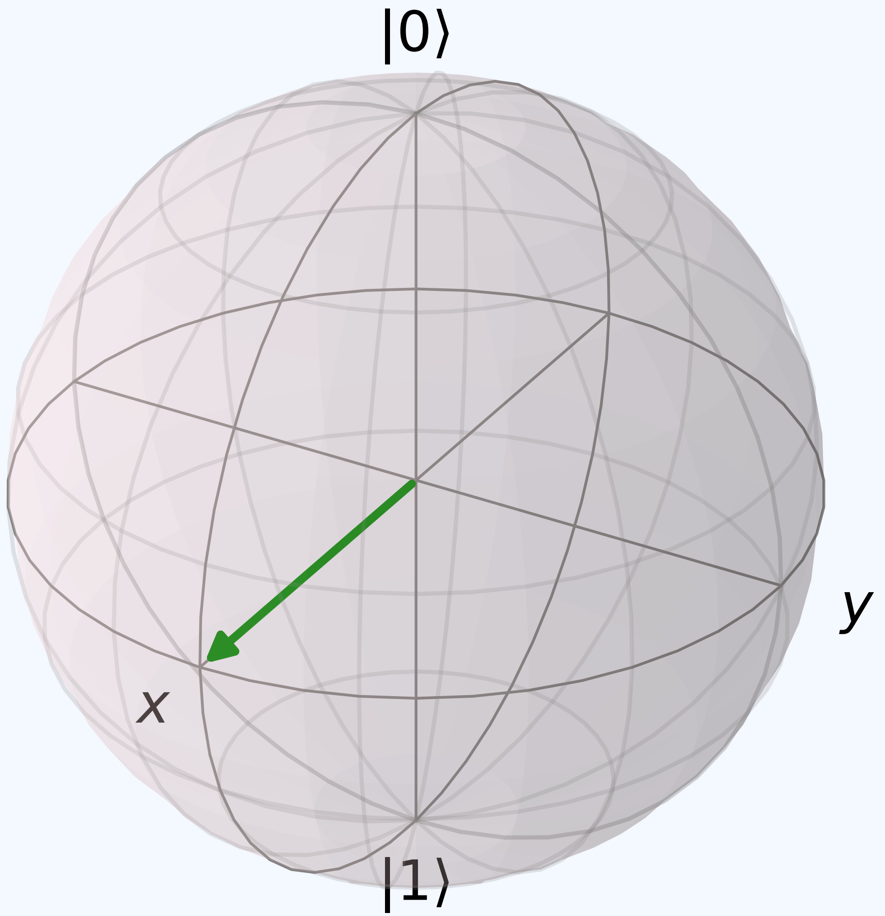


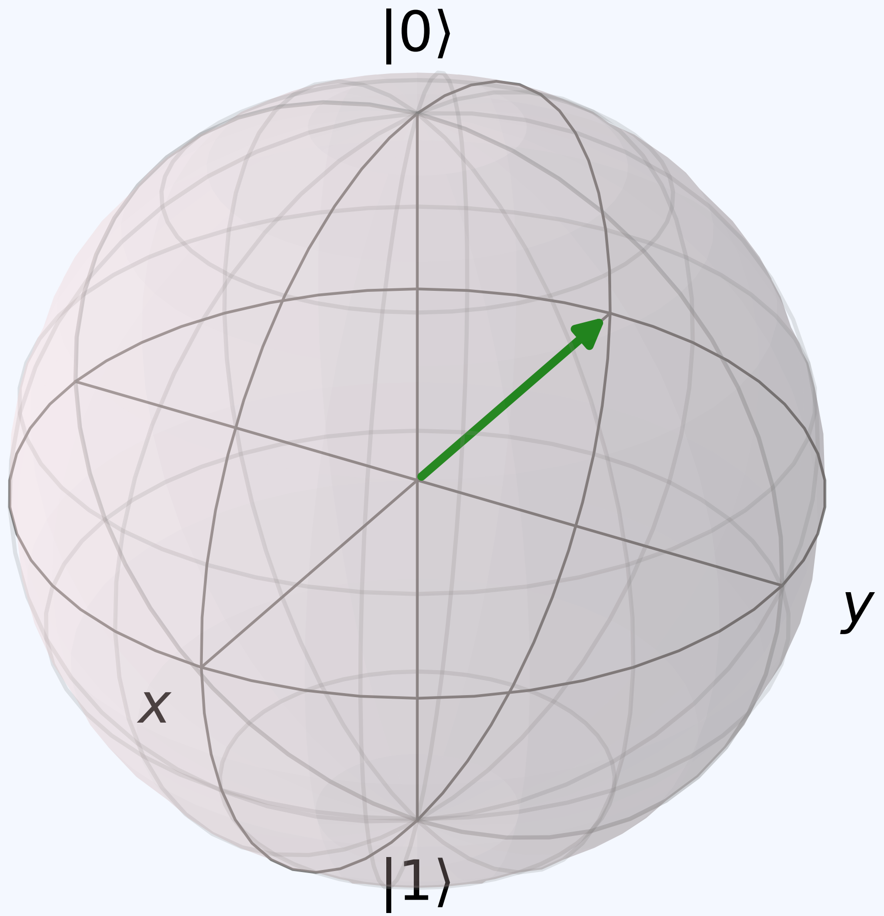
Bloch Sphere

Geometric Representation of **1 Qubit**

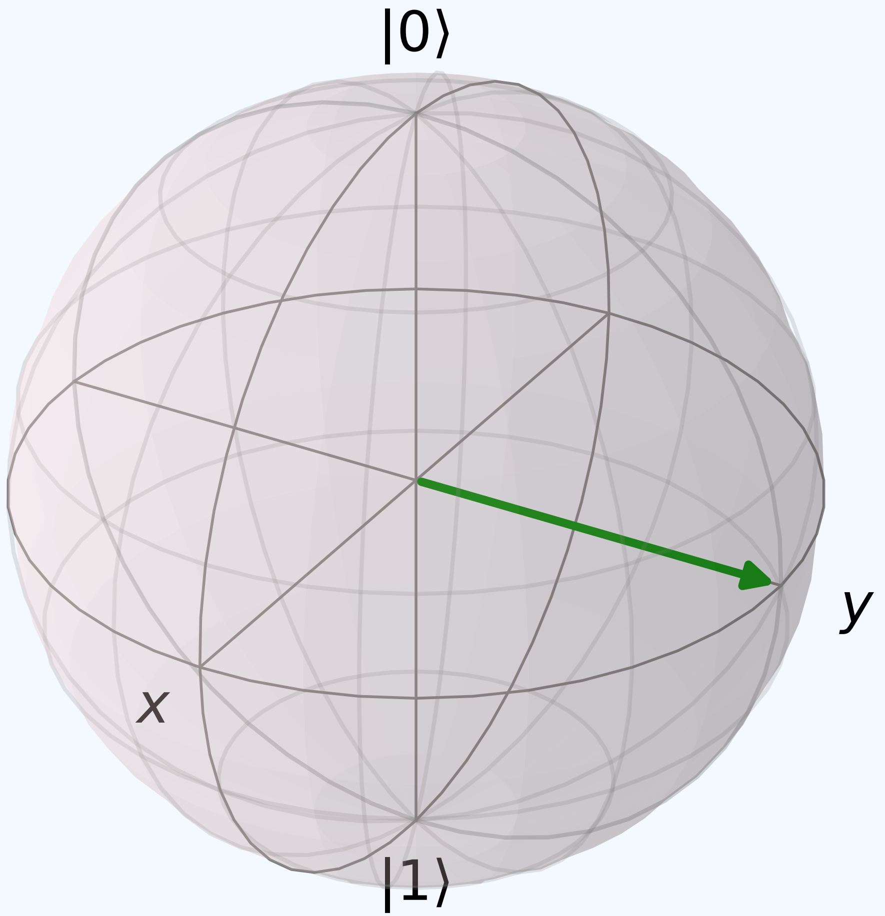
$\vert 0\rangle$	$\vert 1\rangle$
	

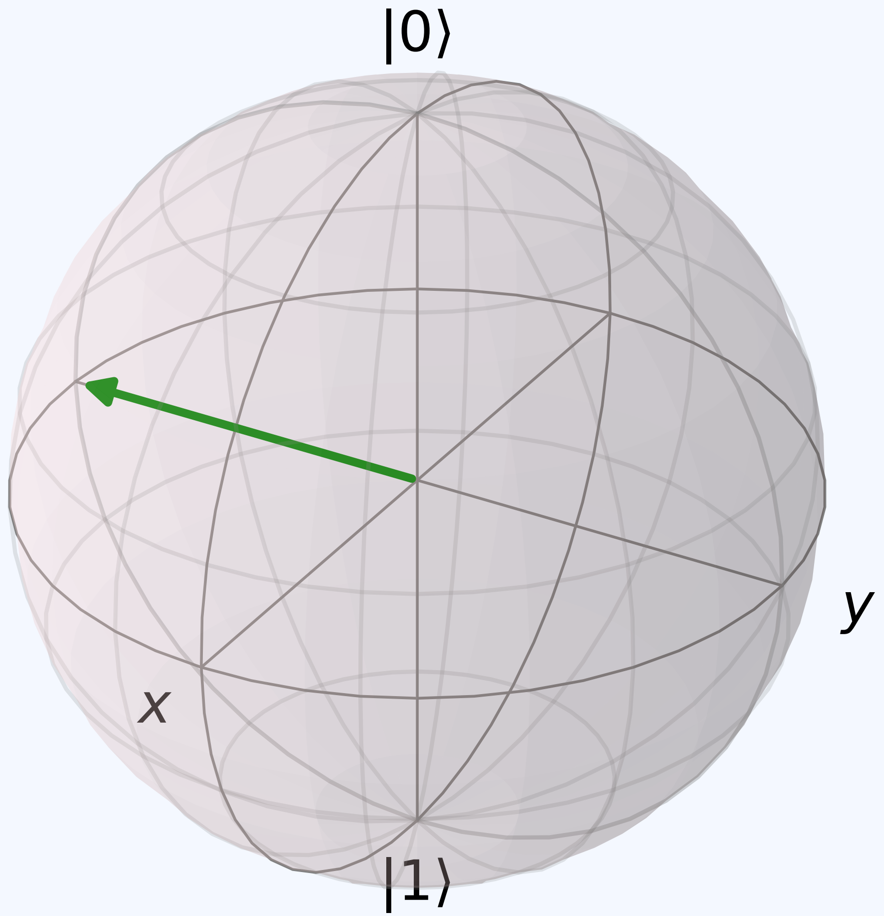
$$\frac{1}{\sqrt{2}}\left|0\right\rangle + \frac{1}{\sqrt{2}}\left|1\right\rangle \qquad \frac{1}{\sqrt{2}}\left|0\right\rangle - \frac{1}{\sqrt{2}}\left|1\right\rangle$$





$$\frac{1}{\sqrt{2}}\left|0\right\rangle + \frac{i}{\sqrt{2}}\left|1\right\rangle \qquad \frac{1}{\sqrt{2}}\left|0\right\rangle - \frac{i}{\sqrt{2}}\left|1\right\rangle$$





Hands-On with Ket

Jupyter Notebook 1

launch binder bit.ly/3lPgXIE

Quantum Gates

Manipulating the Quantum State to Compute

Pauli Gate

Pauli X	Pauli Y	Pauli Z
$X\|0\rangle = \|1\rangle$	$Y\|0\rangle = i\|1\rangle$	$Z\|0\rangle = \|0\rangle$
$X\|1\rangle = \|0\rangle$	$Y\|1\rangle = -i\|0\rangle$	$Z\|1\rangle = -\|1\rangle$

Hadamard Gate

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

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

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

$$H\left[\frac{1}{\sqrt{2}}\left(\left|0\right\rangle - \left|1\right\rangle\right)\right] = \left|1\right\rangle$$

Phase Gate

$$P(\lambda)\left|0\right\rangle = \left|0\right\rangle$$

$$P(\lambda)\left|1\right\rangle = e^{i\lambda}\left|1\right\rangle$$

- $e^{i\lambda} = \cos\lambda + i\sin\lambda$
- Z Gate: $\lambda = \pi \to -1$
- S Gate: $\lambda = \frac{\pi}{2} \to i$
- T Gate: $\lambda = \frac{\pi}{4} \to \frac{1+i}{\sqrt{2}}$

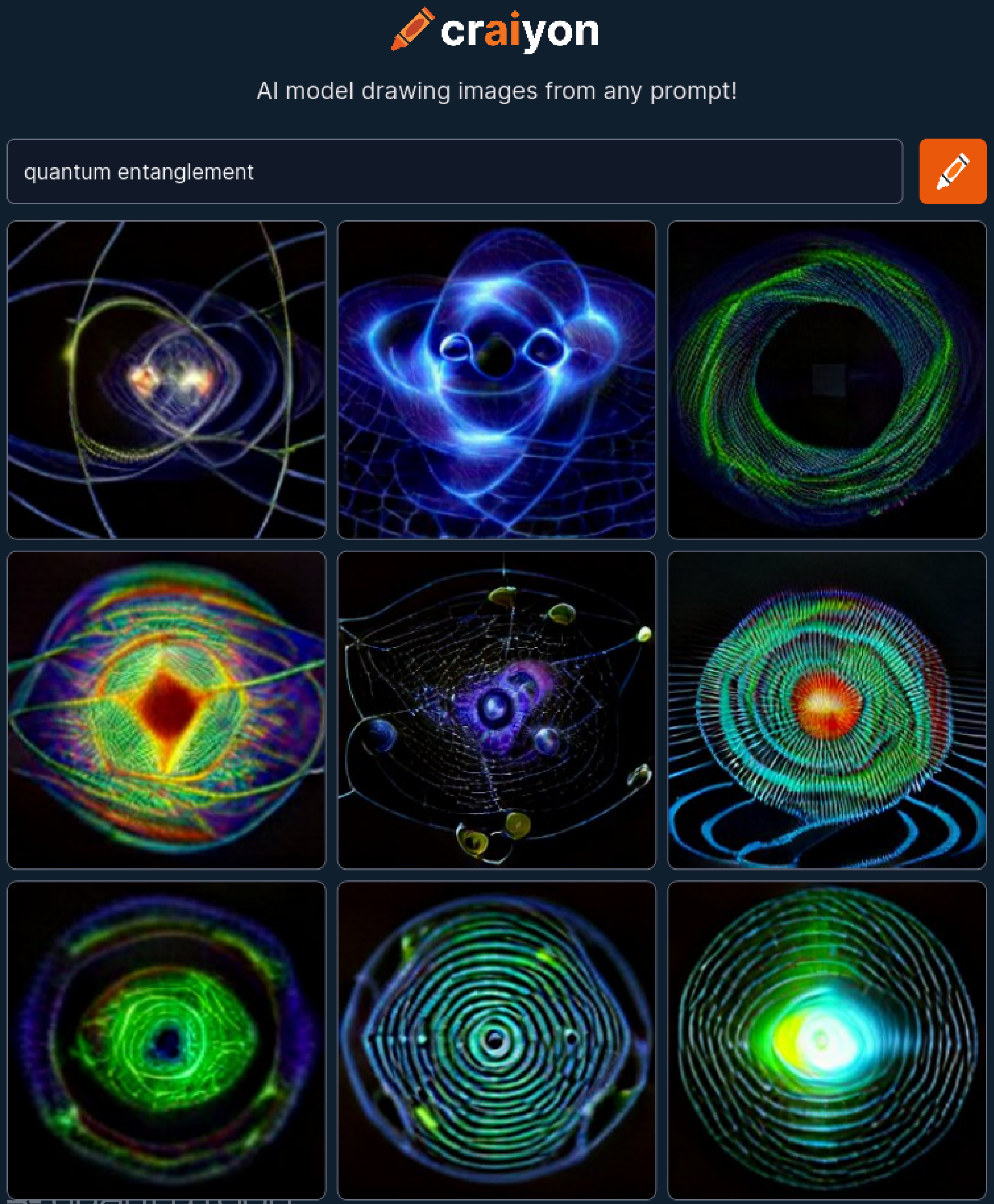
Controlled Quantum Gate

Multiple Qubit Quantum Gate

$$\mathrm{CG}\left|\mathrm{control}\right\rangle\left|\mathrm{target}\right\rangle = \begin{cases} \left|\mathrm{control}\right\rangle\left(\mathrm{G}\left|\mathrm{target}\right\rangle\right), & \text{if } \left|\mathrm{control}\right\rangle = \left|1\cdots1\right\rangle \\ \left|\mathrm{control}\right\rangle\left|\mathrm{target}\right\rangle, & \text{otherwise} \end{cases}$$

CNOT Gate

$$\text{CNOT}\,|00\rangle = |00\rangle$$
$$\text{CNOT}\,|01\rangle = |01\rangle$$
$$\text{CNOT}\,|10\rangle = |11\rangle$$
$$\text{CNOT}\,|11\rangle = |10\rangle$$



Quantum Entanglement

Reversible Computing

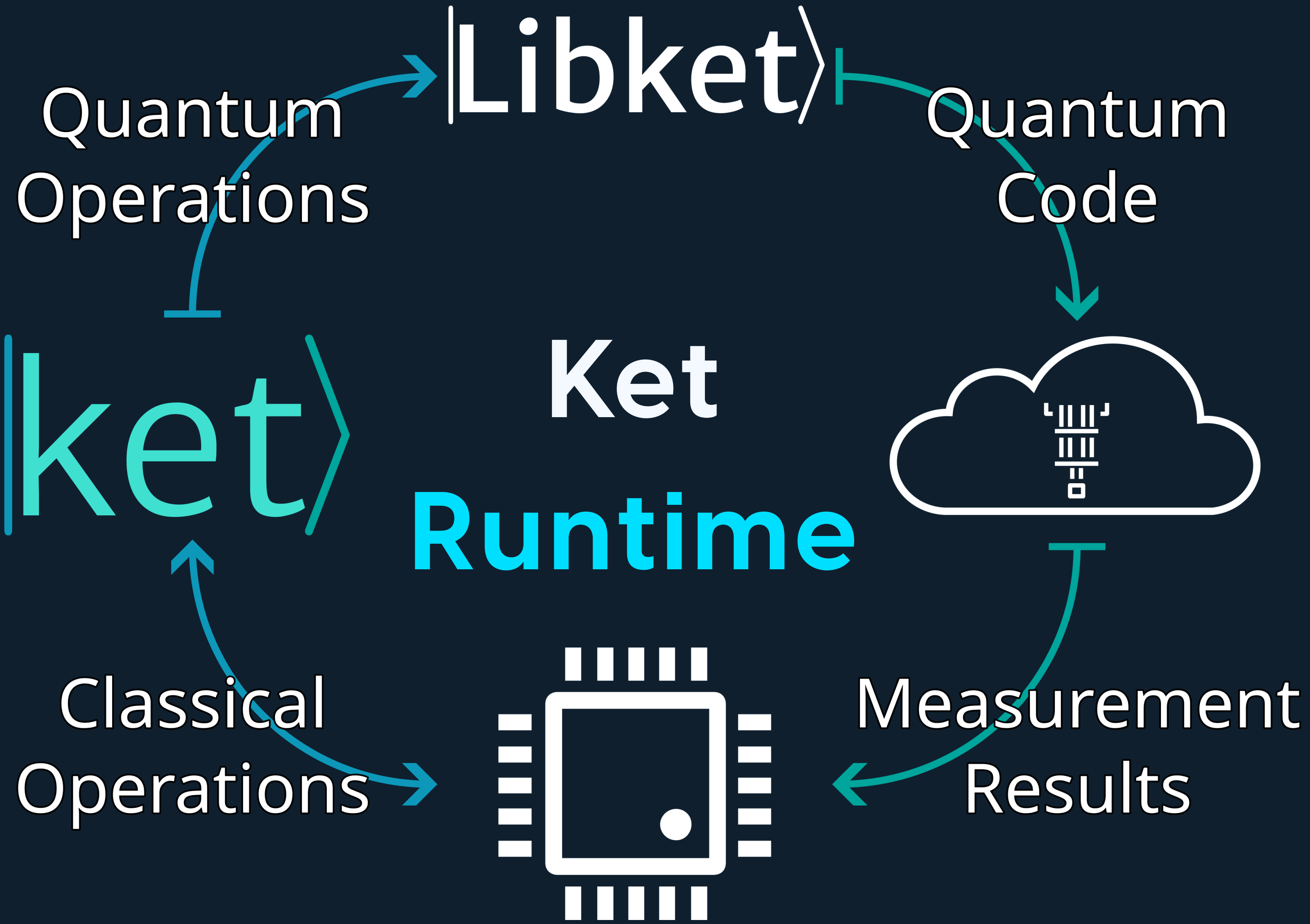
Quantum **Measurement**

Getting **Classical Information** form Quantum Data

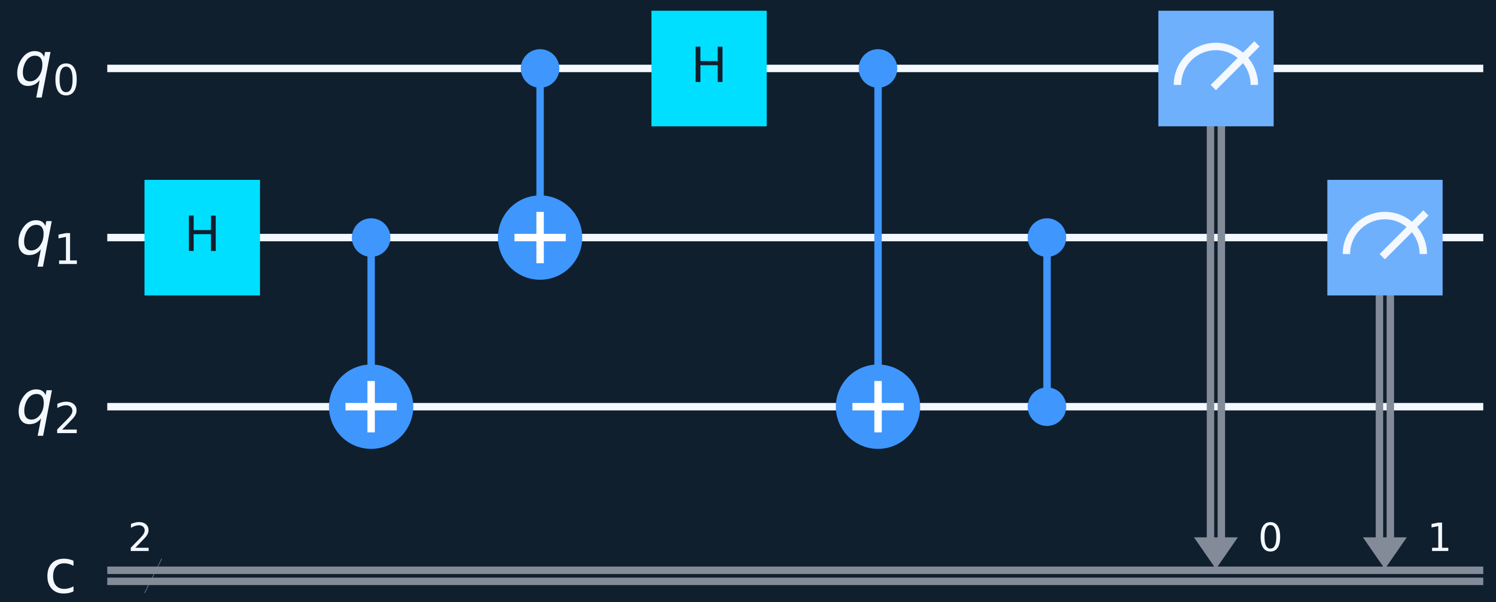
Hands-On with Ket

Jupyter Notebook 2

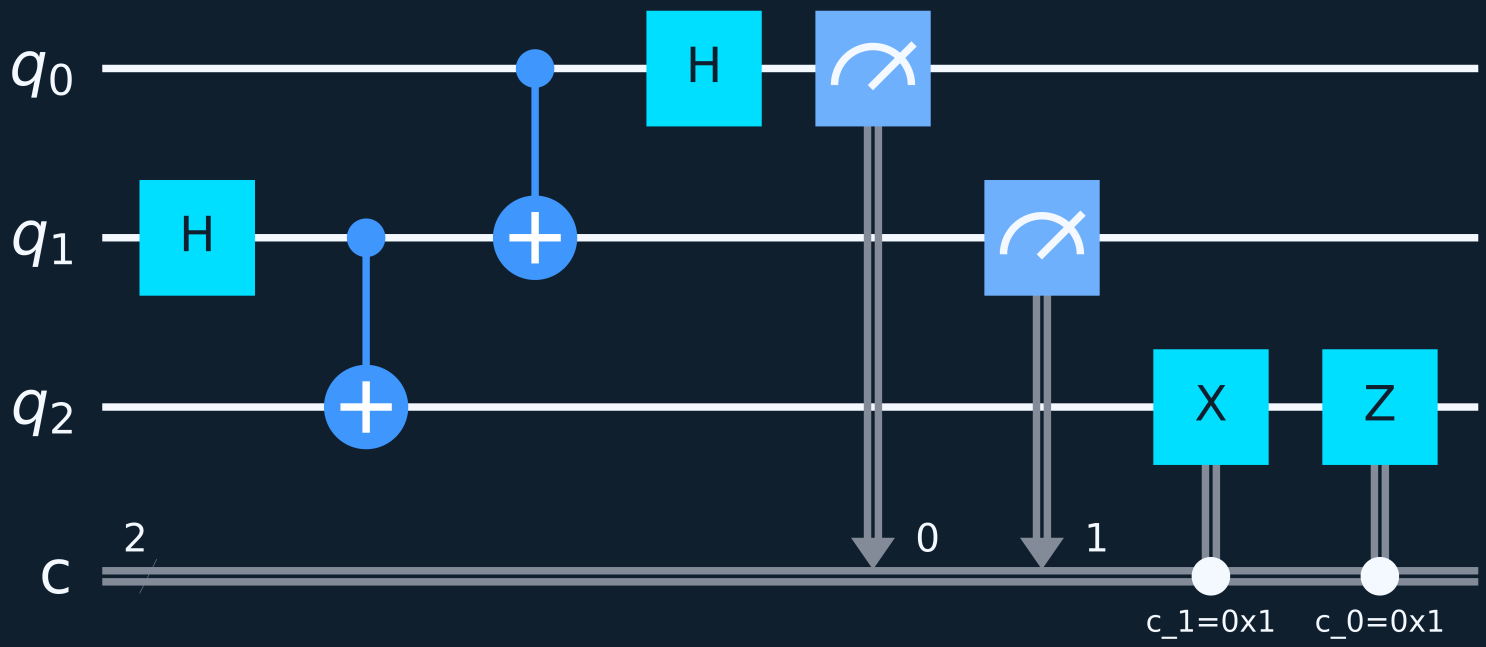
launch binder bit.ly/3o7dawB


|Libket⟩
Quantum Operations
Quantum Code
|ket⟩
Ket
Runtime
Classical Operations
Measurement Results

Quantum Teleportation

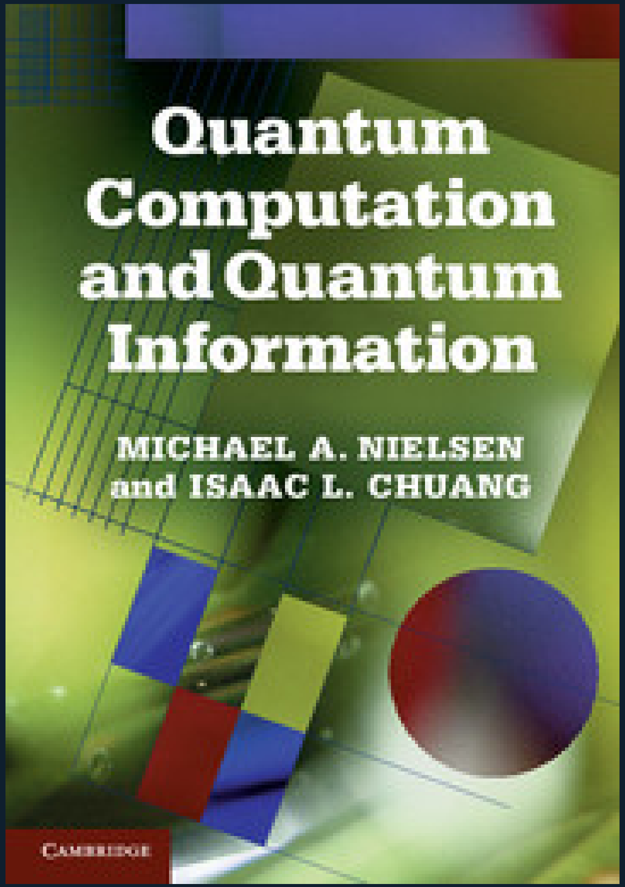


Quantum Teleportation



Postulates of Quantum Mechanics

Mathematical Formulation of Quantum Mechanics



Quantum Computation and Quantum Information

10th Anniversary Edition

- **Postulate 1**: Associated to any isolated physical system is a complex vector space with inner product (that is, a Hilbert space) known as the state space of the system. The system is completely described by its state vector, which is a unit vector in the system's state space.

Computational Basis

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

$$|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

$$\alpha\,|0\rangle + \beta\,|1\rangle = \begin{bmatrix} \alpha \\ \beta \end{bmatrix}$$

- **Postulate 2**: The evolution of a closed quantum system is described by a unitary transformation. That is, the state $|\psi\rangle$ of the system at time t_1 is related to the state $|\psi'\rangle$ of the system at time t_2 by a unitary operator U which depends only on the times t_1 and t_2,

$$|\psi'\rangle = U\,|\psi\rangle\,.$$

Quantum Gates Matrices

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

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

$$H\left[\frac{\left|0\right\rangle + \left|1\right\rangle}{\sqrt{2}}\right] = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\1 & -1\end{bmatrix}\frac{1}{\sqrt{2}}\begin{bmatrix}1\\1\end{bmatrix} = \begin{bmatrix}1\\0\end{bmatrix} = \left|0\right\rangle$$

- **Postulate 3**: Quantum measurements are described by a collection M_m of measurement operators. These are operators acting on the state space of the system being measured. The index m refers to the measurement outcomes that may occur in the experiment. If the state of the quantum system is $|\psi\rangle$ immediately before the measurement then the probability that result m occurs is given by

$$p(m) = \langle\psi| M_m^\dagger M_m |\psi\rangle , \ldots$$

- **Postulate 3**: ...and the state of the system after the measurement is

$$\frac{M_m \left|\psi\right\rangle}{\sqrt{\left\langle\psi\right| M_m^\dagger M_m \left|\psi\right\rangle}}.$$

Measurement Operators for the Computational Basis

$$M_0 = |0\rangle\langle 0| = \begin{bmatrix}1\\0\end{bmatrix}\begin{bmatrix}1 & 0\end{bmatrix} = \begin{bmatrix}1 & 0\\0 & 0\end{bmatrix}$$

$$M_1 = |1\rangle\langle 1| = \begin{bmatrix}0\\1\end{bmatrix}\begin{bmatrix}0 & 1\end{bmatrix} = \begin{bmatrix}0 & 0\\0 & 1\end{bmatrix}$$

Probability of Measuring 0

- $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$

$$p(0) = (\alpha^\dagger\langle 0| + \beta^\dagger\langle 1|)\,|0\rangle\langle 0|0\rangle\langle 0|\,(\alpha|0\rangle + \beta|1\rangle)$$

$$p(0) = (\alpha^\dagger\langle 0|0\rangle + \beta^\dagger\langle 1|0\rangle)\,\langle 0|0\rangle\,(\alpha\langle 0|0\rangle + \beta\langle 0|1\rangle)$$

$$p(0) = \alpha^\dagger\alpha = |\alpha|^2$$

State After Measuring 0

- $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$

$$\frac{|0\rangle\langle 0|(\alpha|0\rangle + \beta|1\rangle)}{\sqrt{|\alpha|^2}} = \frac{\alpha|0\rangle}{|\alpha|}$$

- **Postulate 4**: The state space of a composite physical system is the tensor product of the state spaces of the component physical systems. Moreover, if we have systems numbered 1 through n, and system number i is prepared in the state $|\psi_i\rangle$, then the joint state of the total system is $|\psi_1\rangle \otimes |\psi_2\rangle \otimes \cdots |\psi_n\rangle$.

$$|0\rangle \otimes |0\rangle = \begin{bmatrix} 1 \begin{bmatrix} 1 \\ 0 \end{bmatrix} \\ 0 \begin{bmatrix} 1 \\ 0 \end{bmatrix} \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} = |00\rangle$$

$$H \otimes I = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} & 1 \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \\ 1 \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} & -1 \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & -1 & 0 & -1 \end{bmatrix}$$

$$H_0 \left|00\right\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & -1 & 0 & -1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \end{bmatrix} = \frac{\left|00\right\rangle + \left|10\right\rangle}{\sqrt{2}}$$

$$\text{CNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

$$\text{CNOT}\left[\frac{|00\rangle + |10\rangle}{\sqrt{2}}\right] = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

Quantum Algorithms

Shor's Factorization Algorithm

- **Input**: A composite number N
- **Outputs**: A non-trivial factor of N.
- **Procedure**:
  1. If N is even, return the factor 2.
  2. Determine whether $N = a^b$ for integers $a \geq 1$ and $b \geq 2$, and if so return the factor a.
  3. …

- **Procedure**: ...
  3. Randomly choose x in the range 1 to $N-1$. If $\gcd(x, N) > 1$ then return the factor $\gcd(x, N)$.
  4. Use the *order-finding quantum subroutine* to find the order r of $f(j) = x^j \mod N$.
  5. If r is even and $x^{r/2} \neq -1 \mod N$ then compute $\gcd(x^{r/2} - 1, N)$ and $\gcd(x^{r/2} + 1, N)$, and test to see if one of these is a non-trivial factor, returning that factor if so. Otherwise, the algorithm fails.

Quantum **Order-Finding**

- **Inputs**: **(1)** A black box $U_{x,N}$ which performs the transformation $|j\rangle\,|k\rangle \to |j\rangle\,|x^j k \mod N\rangle$ for x co-prime to the L-bit number N, **(2)** L qubits initialized to $|0\rangle$, and **(3)** L qubits initialized to the state $|1\rangle$.
- **Outputs**: The least integer $r > 0$ such that $xr = 1 \mod N$.

- **Procedure**:
  1. Initial state
     $|0\rangle\,|1\rangle$
  2. Create Superposition
     $\frac{1}{\sqrt{2^L}}\sum_{j=0}^{2^L-1}|j\rangle\,|1\rangle$
  3. Apply $U_{x,N}$
     $\frac{1}{\sqrt{2^L}}\sum_{j=0}^{2^L-1}|j\rangle\,|x^j \mod N\rangle$
  4. ...

- **Procedure**:...

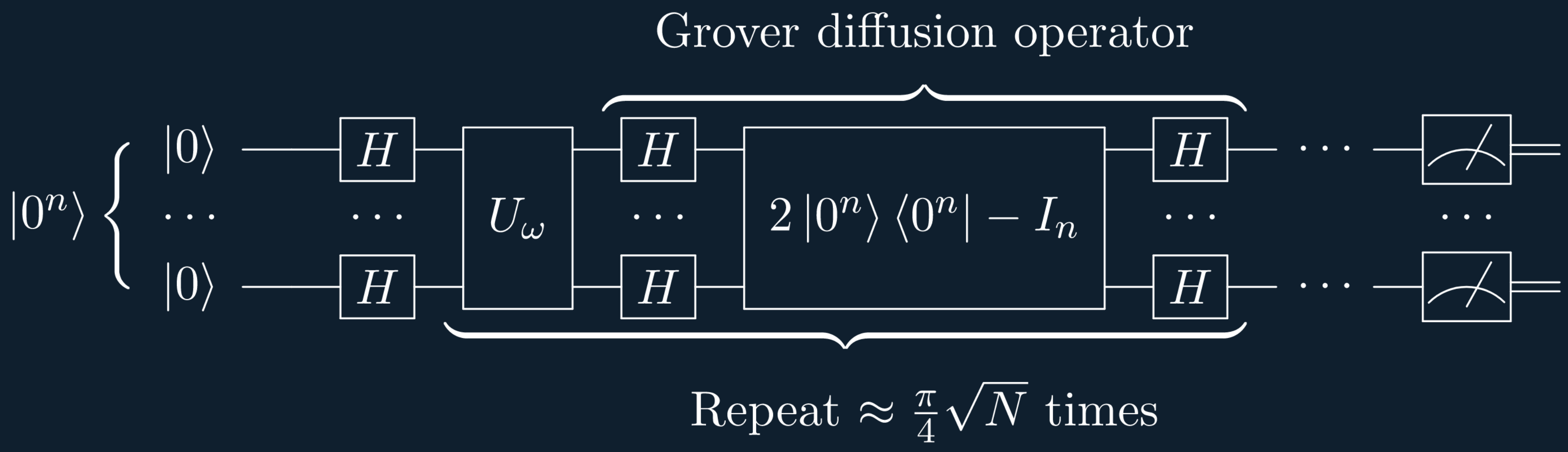
4. Apply inverse quantum Fourier transform
$\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} e^{i\theta_s} \left|s \frac{2^L}{r}\right\rangle \left|\varphi\right\rangle$
5. Measure: r

Hands-On with Ket

Jupyter Notebook 3

launch binder bit.ly/3PvWMRX

Grover's Search Algorithm



$$U_w\,|x\rangle = \begin{cases} -\,|x\rangle\,, & \text{if } x = w \\ |x\rangle\,, & \text{otherwise} \end{cases}$$

Hands-On with Ket

Jupyter Notebook 4

launch binder bit.ly/3aFUaCf

Introduction to Quantum Programming with Ket

⟨G| C |Q⟩
UFSC

quantuloop

VI Workshop Escola de Computação e Informação Quântica - 2022