University of Jyväskylä - Course TIEJ6003

Introduction to Quantum Computing

Day-02

Prof. Ofer Shir
oshir@alumni.Princeton.EDU

JYVÄSKYLÄN YLIOPISTO
UNIVERSITY OF JYVÄSKYLÄ

Summer 2024
Jyväskylä, Finland

BUILDING BLOCKS OF COMPUTATION: QUBITS AND Q-GATES

$$|0\rangle := \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad |1\rangle := \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

the single qubit

The lowest computational unit is a single spin-$\frac{1}{2}$ particle whose Hamiltonian is under control — and is called a **qubit**.

It is a complex superposition of the 'up' and 'down' eigenkets (denoted as either $\{|\uparrow\rangle, |\downarrow\rangle\}$, $\{|+\rangle, |-\rangle\}$, or $\{|0\rangle, |1\rangle\}$):

$$|\psi\rangle := \alpha\,|\uparrow\rangle + \beta\,|\downarrow\rangle = \alpha\,|0\rangle + \beta\,|1\rangle = \begin{pmatrix}\alpha\\ \beta\end{pmatrix}, \tag{1}$$

with $|\alpha|^2 + |\beta|^2 = 1$.

producing any state?

One can produce any state by setting the SGE apparatus to a certain rotation angle. For a rotation over an angle θ about the $\hat{z}$-axis, the *rotated spin operator* becomes (using the fact that Pauli's matrices are unitary, $\sigma_z^2 = \mathbf{1}$)

$$S_{\theta|\hat{z}} = \exp\left(i\theta \cdot \frac{\sigma_z}{2}\right) = \cos\left(\frac{\theta}{2}\right)\mathbf{1} + i\sin\left(\frac{\theta}{2}\right)\sigma_z. \tag{2}$$

generalization

Let the vector $\hat{r} := (\cos\varphi \cdot \sin\theta,\ \ \cos\theta \cdot \sin\theta,\ \ \cos\theta)^T$ represent a target direction in the 3D space of the SGE, then the following operator, which possesses eigenvalues of $\frac{\hbar}{2}$,

$$S_{\hat{r}} := \begin{bmatrix} \cos\theta & \sin\theta \cdot \exp(-i\varphi) \\ \sin\theta \cdot \exp(i\varphi) & -\cos\theta \end{bmatrix}, \tag{3}$$

becomes the measurement of this generalized SGE in the $\hat{r}$-direction.

Given this setup, we are able to construct any desired qubit,

$$|\psi\rangle := \cos\left(\frac{\theta}{2}\right)|0\rangle + \exp(i\varphi)\sin\left(\frac{\theta}{2}\right)|1\rangle$$

up to an undetectable global phase.*

global phase and the Bloch vector

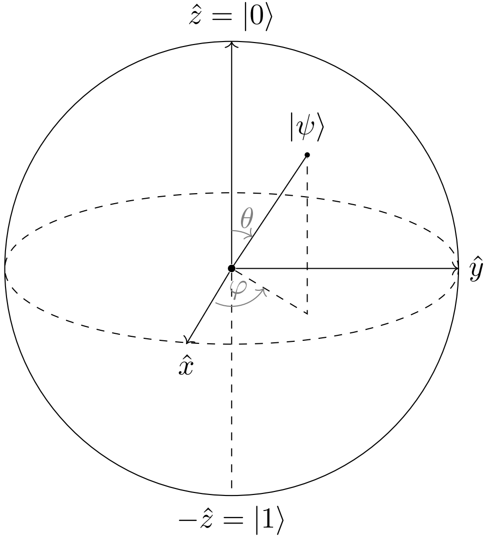
*A generic quantum state is described by

$$|\psi\rangle := \exp(i\gamma)\left[\cos\left(\frac{\theta}{2}\right)|0\rangle + \exp(i\varphi)\sin\left(\frac{\theta}{2}\right)|1\rangle\right],$$

with γ entitled the *global phase*, which is undetectable.

Conventionally, $\hat{r}$ is called the Bloch vector, and the corresponding Bloch Sphere (next chart) provides a spatial description and a visualization of the qubit's state.
A so-called *pure* state always resides on the sphere's surface; *ensembles*, which are not discussed in this course, reside within.

the Bloch sphere



quantum gates

Operators that are applied to qubits must be **unitary**:

$$\mathcal{U}\mathcal{U}^\dagger = \mathbf{1}.$$

Why?

quantum gates

Operators that are applied to qubits must be **unitary**:

$$\mathcal{U}\mathcal{U}^\dagger = \mathbf{1}.$$

Why?

- Probabilities remain consistent across quantum operations.
- Quantum computations are *reversible*.

quantum gates

Operators that are applied to qubits must be **unitary**:

$$\mathcal{U}\mathcal{U}^\dagger = \mathbf{1}.$$

Why?

- Probabilities remain consistent across quantum operations.
- Quantum computations are *reversible*.

A basic example is the so-called phase gate (Pauli's Z!):

$$\phi := \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}. \tag{4}$$

$$\underset{\text{initial state}}{\alpha|0\rangle+\beta|1\rangle} \;\text{———}\boxed{\phi}\text{———}\; \alpha\,|0\rangle - \beta\,|1\rangle$$

the Hadamard gate

The Hadamard gate allows to obtain an equal superposition between the states, which makes it especially useful in the starting point of quantum computations:

$$H := \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \tag{5}$$

$$\underset{\text{initial state}}{\alpha|0\rangle + \beta|1\rangle} \;\text{———}\boxed{H}\text{———}\; \alpha\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right) + \beta\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)$$

other 1-qubit gates

The phase gate (denoted as S), and the T gate (a.k.a. the $\frac{\pi}{8}$, for historical reasons):

$$S := \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} \qquad T := \begin{bmatrix} 1 & 0 \\ 0 & \exp(i\pi/4) \end{bmatrix} \tag{6}$$

Recall the Pauli operators:

$$\sigma_x = X := \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \qquad \sigma_y = Y := \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \qquad \sigma_z = Z := \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \tag{7}$$

2 qubits

The Hilbert space of a 2-qubit system holds four states:

$$\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$$

Notation may differ in the literature, e.g., when using commas to distinguish the qubits ($|0,0\rangle$), or when aggregating kets ($|0\rangle|0\rangle$) — but we will use herein $|00\rangle$.

Every state may be represented as

$$|\psi\rangle := \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle,$$

subject to $\sum_{i,j=0}^{1} |\alpha_{ij}|^2 = 1$.

2-qubit representation

The explicit representation is scaled-up by applying a tensor multiplication:

$$|00\rangle := |0\rangle \otimes |0\rangle = \begin{pmatrix} 1 & \times & \begin{pmatrix} 1 \\ 0 \end{pmatrix} \\ 0 & \times & \begin{pmatrix} 1 \\ 0 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}. \tag{8}$$

2-qubit measurement

given a 2-qubit state, a measurement may target the pair (leading to a 2-qubit state collapse according to (P-5)), or alternatively, target only a single qubit, e.g., measuring the first qubit:

$$|\psi\rangle \xrightarrow[\text{measurement}]{1^{\text{st}}\text{-qubit}} \begin{cases} 0 & \text{with probability } \left|\alpha_{00}\right|^2 + \left|\alpha_{01}\right|^2 \\ 1 & \text{with probability } \left|\alpha_{10}\right|^2 + \left|\alpha_{11}\right|^2 \end{cases}, \tag{9}$$

and leading to a *partial* (1-qubit) state collapse: $|\psi_0\rangle = \frac{\alpha_{00}|0\rangle + \alpha_{01}|1\rangle}{\sqrt{\left|\alpha_{00}\right|^2 + \left|\alpha_{01}\right|^2}}$ if $|0\rangle$ is measured, or $|\psi_1\rangle = \frac{\alpha_{10}|0\rangle + \alpha_{11}|1\rangle}{\sqrt{\left|\alpha_{10}\right|^2 + \left|\alpha_{11}\right|^2}}$ if otherwise $|1\rangle$ is measured.

entanglement

Certain states, e.g., $|\psi\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$ clearly possess high correlation between the two qubits — and therefore, measuring only a single qubit provides information on the other qubit without leading to its collapse. Such states feature the so-called **entanglement** property, which is highly beneficial for computation and communication.

Bell states

The 4 states in which the 2 qubits are entangled:

$$
\begin{aligned}
|\phi_+\rangle = |\beta_{00}\rangle &:= \quad \frac{1}{\sqrt{2}} \left(|00\rangle + |11\rangle\right) \\
|\psi_+\rangle = |\beta_{01}\rangle &:= \quad \frac{1}{\sqrt{2}} \left(|01\rangle + |10\rangle\right) \\
|\phi_-\rangle = |\beta_{10}\rangle &:= \quad \frac{1}{\sqrt{2}} \left(|00\rangle - |11\rangle\right) \\
|\psi_-\rangle = |\beta_{11}\rangle &:= \quad \frac{1}{\sqrt{2}} \left(|01\rangle - |10\rangle\right)
\end{aligned}
$$

Notably, these states form a *basis*.

2-qubit gates

2-qubit gates are 4×4 unitary matrices, which may be scaled-up using a tensor product, as in the Hadamard case:

$$H^{\otimes 2} := H \otimes H = \frac{1}{2} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}. \tag{10}$$

An application example:

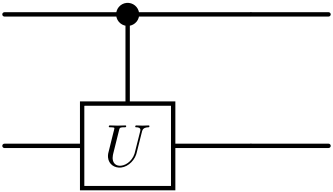
$$H^{\otimes 2} |00\rangle = \frac{1}{2} (|00\rangle + |10\rangle + |01\rangle + |11\rangle)$$

controlled operations

"if A is `true` then do B" is a common type of controlled operation that is very useful in computation. In QC, a controlled-U operation is a 2-qubit gate, with a *control* qubit and a *target* qubit, and an arbitrary 1-qubit unitary operation U.

If the control qubit is `true` then U is applied to the target qubit, otherwise it is unchanged:

$$|c\rangle\,|t\rangle \rightarrow |c\rangle\, U^c\,|t\rangle$$



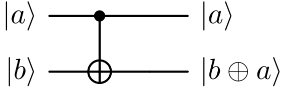
controlled-NOT

The controlled–NOT operation is the most widely-used controlled gate featuring a XOR:

$$|c\rangle\,|t\rangle \to |c\rangle \oplus |t\rangle$$

It is called the CNOT gate, whose matrix representation and circuit are as follows:

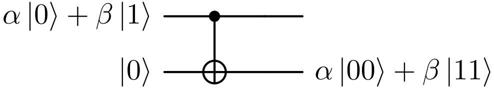
$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$



2-qubit entanglement: aftermath

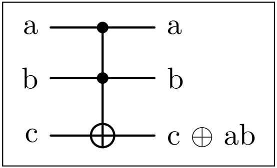
The unitary gates operating on 2-qubit systems may either act on each qubit independently (and thus be represented as a tensor product of 1-qubit operators, as in the Hadamard case above), or act in a correlated manner (featuring entanglement, and thus having no tensor product form — as in the CNOT gate).

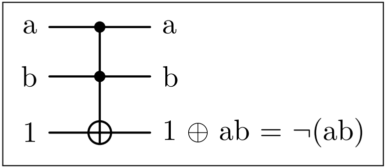
Obtaining entanglement:



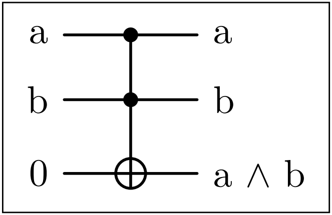
classical computational universality

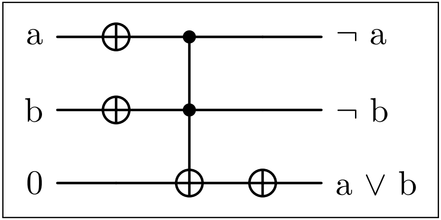
Simulating classical circuits on a quantum computer is feasible using quantum gates.
Obtaining such a computational universality is realizable simply by simulating the `NAND` logical gate.
The **Toffoli** gate is a 3-qubit gate that flips the state of the third qubit if the first two qubits are both in state $|1\rangle$:





Toffoli as `AND` & `OR`





TODO: verify truth tables!

no-cloning theorem for qubits

The no-cloning theorem is a fundamental result in QM that states it is impossible to create an identical copy of an arbitrary unknown quantum state. Formally, the theorem can be stated as follows —

no-cloning theorem for qubits

The no-cloning theorem is a fundamental result in QM that states it is impossible to create an identical copy of an arbitrary unknown quantum state. Formally, the theorem can be stated as follows —

Theorem: There does not exist a unitary operation $\mathcal{U}$ such that for any arbitrary quantum state $|\psi\rangle$ and a fixed state $|0\rangle$, the following transformation holds:

$$\mathcal{U}\left(|\psi\rangle\,|0\rangle\right) = |\psi\rangle\,|\psi\rangle$$

no-cloning theorem - proof

Proof (by contradiction):

Consider two arbitrary quantum states $|\psi\rangle$ and $|\phi\rangle$.
Assume the opposite that there exists a unitary cloning operator $\mathcal{U}$,

$$\mathcal{U}\left(|\psi\rangle\,|0\rangle\right) = |\psi\rangle\,|\psi\rangle$$

$$\mathcal{U}\left(|\phi\rangle\,|0\rangle\right) = |\phi\rangle\,|\phi\rangle$$

no-cloning theorem - proof

Proof (by contradiction):
Consider two arbitrary quantum states $|\psi\rangle$ and $|\phi\rangle$.
Assume the opposite that there exists a unitary cloning operator $\mathcal{U}$,

$$\mathcal{U}\left(|\psi\rangle\,|0\rangle\right) = |\psi\rangle\,|\psi\rangle$$

$$\mathcal{U}\left(|\phi\rangle\,|0\rangle\right) = |\phi\rangle\,|\phi\rangle$$

Since $\mathcal{U}$ is a linear operator, it must preserve the inner product:

$$\left(\langle\psi|\,\langle 0|\right)\mathcal{U}^{\dagger}\mathcal{U}\left(|\phi\rangle\,|0\rangle\right) = \left(\langle\psi|\,\langle\psi|\right)\left(|\phi\rangle\,|\phi\rangle\right)$$

Given that $\mathcal{U}^{\dagger}\mathcal{U} = \mathbf{1}$, we obtain the following result:

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

no-cloning theorem - proof cont'd

But $|\psi\rangle$ and $|\phi\rangle$ are arbitrary states that generally satisfy

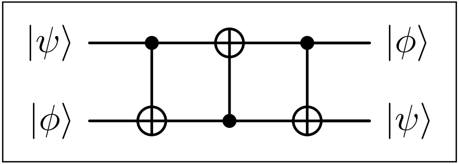
$$0 \leq \langle\psi|\phi\rangle \leq 1,$$

and thus the contradiction is achieved when $|\psi\rangle$ and $|\phi\rangle$ are chosen not to be orthogonal (nor identical).

Hence, no such unitary operator $\mathcal{U}$ exists, and the theorem holds. $\blacksquare$

swapping rather than cloning

Cloning is not possible, but swapping is:



Information-wise, think of the swap as *rearranging* the existing information between the two qubits (rather than information exchange). The CNOT sequence might make the information accessible in a different way, but the total information content remains the same.

Tomorrow: teleporting rather than cloning