COL7160 : Quantum Computing

Lecture 4: Unitary Operations and Quantum Gates

Instructor: Rajendra Kumar **Scribe:** Rupanshu Shah

1 Fundamental Laws of Quantum Mechanics

- **Linearity of Operations:**
  - Every valid quantum operation U must be linear.
  - Linearity allows operations to be represented as matrix multiplication.
  - For an n-qubit state, U is represented by a $2^n \times 2^n$ complex matrix.
  - Quantum Operation $U : |\psi_{in}\rangle \rightarrow |\psi_{out}\rangle$
- **Preservation of Normalization:**
  - A quantum operation must take a valid quantum (normalized) state and produce another valid quantum (normalized) state.
  - This implies $\langle\psi_{in}|\psi_{in}\rangle = \langle\psi_{out}|\psi_{out}\rangle = \langle\psi_{in}|U^\dagger U|\psi_{in}\rangle$.
  - For this to hold for every $|\psi_{in}\rangle$, the condition $U^\dagger U = I$ must be satisfied.
  - Such matrices U are called **unitary** matrices.

2 Measurement vs. Quantum Operations

- **Quantum Operations:**
  - These are reversible and deterministic.
  - Determinism means that given a fixed $|\psi_{in}\rangle$ and U, you always get a fixed $|\psi_{out}\rangle$.
- **Measurement:**
  - Unlike unitaries, measurement is probabilistic and irreversible.
  - The inclusion of measurement makes quantum algorithms inherently probabilistic.

3 Structure of Quantum Algorithms

- **Basic Workflow:**
  - Algorithms typically start with all qubits in the $|0\rangle$ state.
  - They apply a sequence of Unitary operations and Measurements.
- **Operational Rules:**
  - Multiple consecutive unitaries can be combined into a single unitary matrix.
  - The input to the algorithm determines which unitaries are applied.

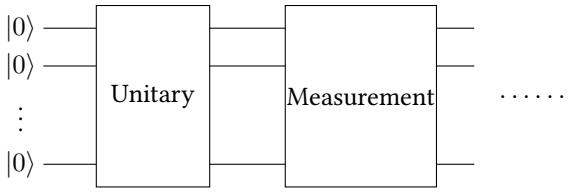

Figure 1: General structure of a quantum algorithm.

Example 1: Hadamard Transform

- **Matrix:** $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$
- **Action on Computational Basis:**
  - $H|0\rangle = |+\rangle$
  - $H|1\rangle = |-\rangle$
- **Action on Hadamard Basis:**
  - $H|+\rangle = |0\rangle$
  - $H|-\rangle = |1\rangle$
- **Property:** $H^\dagger = H$ (Self-adjoint).

Usage: Sampling a random bit

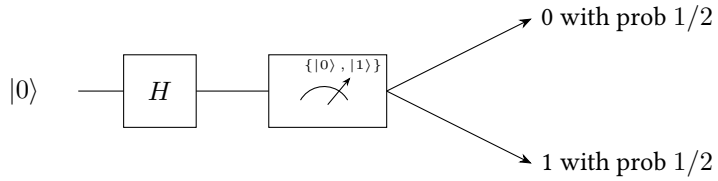

Figure 2: Quantum circuit for sampling a random bit.

Example 2: Rotation Matrix $R(\theta)$

- The rotation matrix $R(\theta)$ rotates a state by an angle of $\theta/2$ on a single application:

$$R(\theta) = \begin{pmatrix} \cos(\theta/2) & -\sin(\theta/2) \\ \sin(\theta/2) & \cos(\theta/2) \end{pmatrix}$$

- Let's focus on the case where $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, where $\alpha, \beta \in \mathbf{R}$ and $\alpha^2 + \beta^2 = 1$.

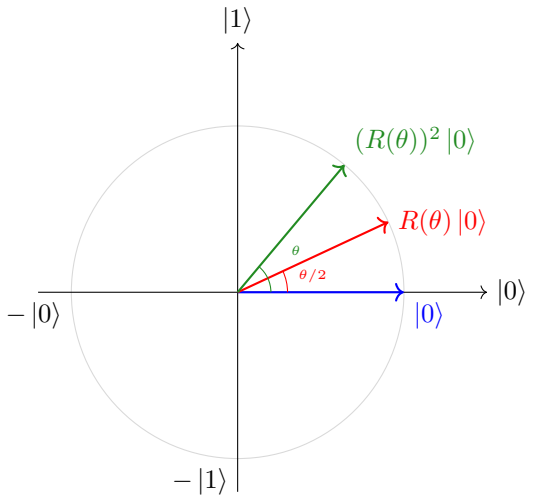

Figure 3: Rotation of a quantum state on the real unit circle.

Observation: $(R(\pi/2))^2\,|0\rangle = |1\rangle$. This follows because applying $R(\pi/2)$ twice results in a total rotation of $\pi/2$ (or $90°$).

4 Elitzur-Vaidman Bomb Testing

- **Setup:**
  - There is a bomb that is either functional (working) or non-functional (not working).
  - We can send a single qubit state $|\psi\rangle$ to the bomb to test its status without exploding it.
  - **Functional Bomb:** Measures the qubit in the computational basis.
    - If the measurement result is 1, the bomb explodes.
    - If the result is 0, it returns the state $|0\rangle$.
  - **Non-functional Bomb:** Acts as an identity operation; it takes input $|\psi\rangle$ and outputs the same state $|\psi\rangle$ without any interaction.

Protocol and Feedback Circuit

The protocol involves a sequence of rotations and interactions with the bomb. If the bomb does not explode, the output is fed back as the input for the next iteration.

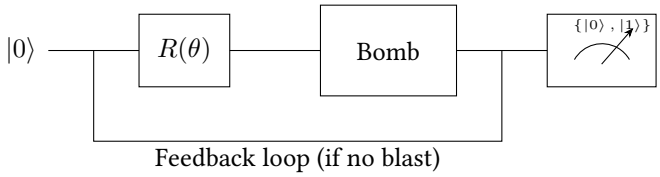

Figure 4: Feedback circuit for Elitzur-Vaidman bomb testing.

Detailed Analysis

One Iteration (Functional Bomb)

- Starting with $|0\rangle$, we apply $R(\theta)$ to get: $R(\theta)\,|0\rangle = \cos(\theta/2)\,|0\rangle + \sin(\theta/2)\,|1\rangle$.

- The functional bomb measures this state.
- **Probability of Blast:** $P(\text{blast}) = |\sin(\theta/2)|^2 = \sin^2(\theta/2)$.
- **Probability of No Blast:** $P(\text{no blast}) = |\cos(\theta/2)|^2 = \cos^2(\theta/2)$.
- If there is no blast, the bomb returns state $|0\rangle$, which is fed back into the next iteration.

Multi-Iteration Analysis (n iterations)

- **Case 1: Bomb is Functional**
  - The probability that the bomb does not explode after n iterations is $(\cos^2(\theta/2))^n = \cos^{2n}(\theta/2)$.
  - **Total Blast Probability:** $P(\text{at least 1 blast}) = 1 - (\cos^2(\theta/2))^n$.
  - Using $\cos^2(\theta/2) = 1 - \sin^2(\theta/2)$, we get:

$$P(\text{blast}) = 1 - (1 - \sin^2(\theta/2))^n \approx 1 - (1 - n\sin^2(\theta/2)) = n\sin^2(\theta/2)$$

  - If the bomb does not explode, the final measurement in the standard basis will yield 0 with probability 1.
- **Case 2: Bomb is Non-functional**
  - The state simply rotates n times: $(R(\theta))^n |0\rangle = R(n\theta) |0\rangle$.
  - We choose $n = \pi/\theta$ so that the total rotation is $\pi/2$.
  - The final state is $R(\pi) |0\rangle = |1\rangle$.
  - The final measurement in the standard basis will yield 1 with probability 1.

Efficiency and Success

- For $n = \pi/\theta$, we can distinguish a functional bomb from a non-functional one if the bomb did not explode.
- The blast probability is $P(\text{blast}) \approx \frac{\pi}{\theta} \cdot \sin^2(\theta/2) \leq \frac{\pi}{\theta} \cdot \frac{\theta^2}{4} = \frac{\pi\theta}{4}$.
- By decreasing θ (and increasing n), the probability of exploding the bomb during testing can be made arbitrarily small.

5 Properties of Unitary Maps

In this section, we explore the fundamental relationship between unitary matrices and orthonormal bases.

Lemma 1. *Let U be a linear map on $\mathbf{C}^d$. Then U is unitary ($U^\dagger U = I$) iff the columns of U form an orthonormal basis.*

Proof. Let the columns of U be denoted by $|v_1\rangle, |v_2\rangle, \ldots, |v_d\rangle$. The entry at row i and column j of the product $U^\dagger U$ is given by the inner product of the i-th row of $U^\dagger$ (which is the conjugate transpose of the i-th column of U) and the j-th column of U. Thus, $(U^\dagger U)_{ij} = \langle v_i | v_j \rangle$.

- **Lemma 1.1 ($\implies$):** If U is unitary, then $U^\dagger U = I$. This implies $(U^\dagger U)_{ij} = \delta_{ij}$, where δ_{ij} is the Kronecker delta. Therefore, $\langle v_i | v_j \rangle = 1$ if $i = j$ and 0 if $i \neq j$, meaning the columns are orthonormal. Since there are d such vectors in $\mathbf{C}^d$, they form an orthonormal basis.
- **Lemma 1.2 ($\impliedby$):** If the columns form an orthonormal basis, then $\langle v_i | v_j \rangle = \delta_{ij}$. It follows that $(U^\dagger U)_{ij} = \delta_{ij}$, so $U^\dagger U = I$, making U unitary.

□

Lemma 2. *U is unitary iff it transforms any orthonormal basis of $\mathbf{C}^d$ into an orthonormal basis.*

Proof. Let $\{|e_1\rangle, \ldots, |e_d\rangle\}$ be an arbitrary orthonormal basis. The transformed basis is $\{|f_i\rangle\}$ where $|f_i\rangle = U |e_i\rangle$.

- **Lemma 2.1 ($\implies$):** Suppose U is unitary. The inner product of the transformed vectors is:

$$\langle f_i|f_j\rangle = (U|e_i\rangle)^\dagger (U|e_j\rangle) = \langle e_i| U^\dagger U |e_j\rangle$$

  Since $U^\dagger U = I$, this simplifies to $\langle e_i|e_j\rangle = \delta_{ij}$. Thus, the transformed vectors remain orthonormal and form a basis.

- **Lemma 2.2 ($\impliedby$):** If U transforms any orthonormal basis into an orthonormal basis, let it act on the standard basis $\{|0\rangle, |1\rangle, \ldots, |d-1\rangle\}$. The columns of U are exactly the images of the standard basis vectors. Since these images must be orthonormal by assumption, the columns of U are orthonormal. By Lemma 1.2, U is unitary.

□

Lemma 3. *If U transforms a specific orthonormal basis of $\mathbf{C}^d$ into another orthonormal basis, then U transforms each orthonormal basis of $\mathbf{C}^d$ into some orthonormal basis.*

Proof. Let $B_1 = \{|v_1\rangle, |v_2\rangle, \ldots, |v_d\rangle\}$ be a specific orthonormal basis that U transforms into another orthonormal basis $B_2 = \{|w_1\rangle, |w_2\rangle, \ldots, |w_d\rangle\}$. By definition, $U|v_i\rangle = |w_i\rangle$ for all i.

1. **Preservation of Inner Product for Basis Vectors:** Since B_2 is an orthonormal basis, the inner product of the transformed vectors satisfies:
$$\langle Uv_i|Uv_j\rangle = \langle w_i|w_j\rangle = \delta_{ij}$$
Since B_1 is also orthonormal, we have $\langle v_i|v_j\rangle = \delta_{ij}$. Thus, $\langle Uv_i|Uv_j\rangle = \langle v_i|v_j\rangle$ for all i, j.

2. **General Unitarity:** Any arbitrary vectors $|a\rangle, |b\rangle \in \mathbf{C}^d$ can be expanded in the basis B_1 as $|a\rangle = \sum_i a_i |v_i\rangle$ and $|b\rangle = \sum_j b_j |v_j\rangle$. Due to the linearity of U:
$$\langle Ua|Ub\rangle = \sum_{i,j} a_i^* b_j \langle Uv_i|Uv_j\rangle = \sum_{i,j} a_i^* b_j \delta_{ij} = \sum_i a_i^* b_i = \langle a|b\rangle$$
This identity $\langle a| U^\dagger U |b\rangle = \langle a| I |b\rangle$ for all $|a\rangle, |b\rangle$ implies $U^\dagger U = I$. Therefore, U is unitary.

3. **Transformation of Any Basis:** By Lemma 2.1, we have already established that if U is unitary, it transforms *any* orthonormal basis into another orthonormal basis. Thus, the property holds universally.

□

6 Elementary Quantum Gates

6.1 Single Qubit Gates

- **Hadamard (H):**
  - **Matrix:** $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$
  - **Action on Computational Basis:**
    - $H|0\rangle = |+\rangle$
    - $H|1\rangle = |-\rangle$
  - **Action on Hadamard Basis:**
    - $H|+\rangle = |0\rangle$
    - $H|-\rangle = |1\rangle$
  - **Property:** $H^\dagger = H$ (Self-adjoint).

- **Pauli-X (Bit Flip):**

  - **Matrix:** $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
  - **Action:**
    * $X|0\rangle = |1\rangle$
    * $X|1\rangle = |0\rangle$

- **Pauli-Z (Phase Flip):**
  - **Matrix:** $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$
  - **Action on Computational Basis:**
    * $Z|0\rangle = |0\rangle$
    * $Z|1\rangle = -|1\rangle$
  - **Action on Hadamard Basis:** (Acts as bit flip in Hadamard basis)
    * $Z|+\rangle = |-\rangle$
    * $Z|-\rangle = |+\rangle$

- **Pauli-Y:**
  - **Matrix:** $Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$
  - **Relation:** $Y = iXZ$
  - **Action:**
    * $Y|0\rangle = i|1\rangle$
    * $Y|1\rangle = -i|0\rangle$

- **Phase Gate (R_φ):**
  - **Matrix:** $R_\varphi = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\varphi} \end{pmatrix}$
  - **Action:**
    * $R_\varphi|0\rangle = |0\rangle$
    * $R_\varphi|1\rangle = e^{i\varphi}|1\rangle$
  - **Note:** The Z gate is a special case where $Z = R_\pi$.

6.2 Multi-Qubit Gates

- **CNOT (Controlled-NOT):**
  - A 2-qubit gate with a control qubit and a target qubit.
  - **Matrix Representation:**

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

  - **Operational Mapping:**
    * $\text{CNOT}|0\rangle|b\rangle = |0\rangle|b\rangle$
    * $\text{CNOT}|1\rangle|b\rangle = |1\rangle|1 \oplus b\rangle$
  - **Qubit Roles:**
    * First qubit $\rightarrow$ Control qubit
    * Second qubit $\rightarrow$ Target qubit

- **CCNOT (Toffoli Gate):**
  - A 3-qubit gate where the third qubit (target) is flipped if and only if the first two qubits (controls) are both in the $|1\rangle$ state.
  - **Matrix Representation:**

$$\text{CCNOT} = \left(\begin{array}{c|cc} I_{6\times 6} & \multicolumn{2}{c}{0} \\ \hline 0 & 0 & 1 \\ & 1 & 0 \end{array}\right)$$

  - **Logic:**
    - $|x, y, z\rangle \to |x, y, z \oplus (x \wedge y)\rangle$

7 Exercises

1. **Conditional Unitary Construction:** Construct a matrix for a $2n$ qubit state that applies unitary U to the last n qubits only when the first n qubits are all 1.
2. **Universal Logic:** Construct classical AND, OR, and NOT gates using only the Toffoli gate.