CSE 392: Matrix and Tensor Algorithms for Data Spring 2024

Lecture 25 — April 17

Instructor: Shashanka Ubaru *Scribe: Paulina Hoyos*

Introduction to Quantum Computing

Qubits and Quantum States

A bit is a fundamental unit of information used in classical computation and digital communication; it can take on exactly one value in $\{0, 1\}$. The state of a register of q classical bits, can be represented by a binary string in $\{0, 1\}^q$. This is a q-dimensional space, and we see that the dimension of the state space grows linearly with the number of bits. Moreover, the state of each classical bit can be set independently of the state of the other classical bits in the register.

Qubits are the quantum counterpart of bits. They are represented using Dirac's bra-ket notation.

Definition. Given a complex Hilbert space $\mathcal{H}$, $|\psi\rangle \in \mathcal{H}$ denotes a column vector, and $\langle\psi| \in \mathcal{H}^*$ denotes a row vector in the dual space of $\mathcal{H}$ that is the conjugate transpose of $|\psi\rangle$, that is, $\langle\psi| = |\psi\rangle^*$.

The column vector $|\psi\rangle$ is called a ket, while the row vector $\langle\psi|$ is called a bra. Hence, the expression $\langle\psi|\phi\rangle$ represents an inner product and is called a bra-ket.

Definition. The state of a quantum bit (quibit) is a unit vector $|\psi\rangle$ in $\mathbb{C}^2$.

In bra-ket notation, the standard basis for $\mathbb{C}^2$ is given by

$$|0\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \quad |1\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}.$$

The basis elements $|0\rangle$ and $|1\rangle$ correspond to the classical bits 0 and 1, respectively.

The state of a qubit $|\psi\rangle$ can be represented as

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

where $\alpha, \beta \in \mathbb{C}$ satisfy $|\alpha|^2 + |\beta|^2 = 1$ and indicate the amplitudes of the states $|0\rangle$ and $|1\rangle$, respectively.

The state space of a single qubit can be represented geometrically using the Bloch sphere: a unit 2-sphere with antipodal points corresponding to a pair of mutually orthogonal state vectors. The north and south poles are typically chosen to correspond to the standard basis vectors $|0\rangle$ and $|1\rangle$. Points on the surface of the sphere correspond to the pure states of the system, whereas interior points correspond to the mixed states (aka density matrices). The most general pure state $\psi\rangle \in \mathbb{C}^2$ is written as

$$|\psi\rangle = e^{i\gamma}\left(\cos(\theta/2)|0\rangle + \sin(\theta/2)e^{i\phi}\right).$$

Definition. The state of q qubits is a unit vector in $(\mathbb{C}^2)^{\otimes q} = \underbrace{\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2}_{q \text{ times}}$.

The standard basis for $(\mathbb{C}^2)^{\otimes q}$, which has 2^q elements, is denoted by $|j\rangle$ for $j \in \{0,1\}^q$. If we let j_k denote the kth digit of the binary string j, then $|j\rangle$ has a one in position $\sum_{k=1}^{1} j_k 2^{q-k} + 1$ and 0 elsewhere.

Example 1. The basis elements of $(\mathbb{C}^2)^{\otimes 2} = \mathbb{C}^2 \otimes \mathbb{C}^2$ are

$$|00\rangle = |0\rangle \otimes |0\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \quad |01\rangle = |0\rangle \otimes |1\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix},$$

$$|10\rangle = |1\rangle \otimes |0\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \quad |11\rangle = |1\rangle \otimes |1\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}.$$

The state of q qubits can be represented as

$$|\psi\rangle = \sum_{j=0}^{2^q-1} \alpha_j |j\rangle,$$

where $\alpha_j \in \mathbb{C}$ and $\sum_{j=0}^{2^q-1} |\alpha_j|^2 = 1$.

Definition. We say that q quibits are in a basis state if their corresponding state $|\psi\rangle = \sum_{j=0}^{2^q-1} \alpha_j |j\rangle$ is such that exists an index k for which $\alpha_k = 1$ while $\alpha_j = 0$ for all $j \neq k$. Otherwise, we say that the qubits are in a superposition state.

Note that q qubits are in a (standard) basis state if and only if its state can be represented as the tensor product of q single qubits, each of which is in a basis state.

Superposition is one of the unique key features of quantum computers. There is no classical equivalent to superposition as q classical bits are always in a basis state, i.e., the q bits will always correspond exactly to one of the 2^q binary strings representing the numbers 0, . . . , 2^{q-1}.

Definition. A quantum state $|\psi\rangle \in (\mathbb{C}^2)^{\otimes q}$ is a product state if there exist q single qubit quantum states $|\psi_i\rangle \in \mathbb{C}^2$, $i = 1, \ldots, q$, such that $|\psi\rangle = |\psi_1\rangle \otimes \cdots \otimes |\psi_q\rangle$. Otherwise, it is an entangled state.

Quantum Gates

Classical logic gates are the fundamental building blocks of computation and information processing tasks. Examples of classical gates include:

1. NOT
2. AND

3. OR
4. XOR
5. NAND

Similarly to classical logical gate, a quantum logic gate is a mean to manipulate the state of a qubit or a set of qubits in such a way that it does not break the basic properties of a quantum state.

Definition. Any operation applied by a quantum computer with q qubits, also called a gate, is a unitary matrix U in $\mathbb{C}^{2^q \times 2^q}$.

Recall that a matrix U is unitary if $U^*U = UU^* = I$. Unitary matrices are norm-preserving: given a unitary matrix U and a vector x, $||Ux|| = ||x||$. Thus, for a q-qubit system, the quantum state is a unit vector $|\psi\rangle \in (\mathbb{C}^2)^{\otimes q}$, a quantum operation is a unitary matrix $U \in \mathbb{C}^{2^q \times 2^q}$, and the application of U onto the state $|\psi\rangle$ is the unit vector $U|\psi\rangle$. This leads to the following central properties:

1. Quantum operations are linear.
2. Quantum operations are reversible

While these properties may initially seem to be extremely restrictive, [Deutsch, 1985] shows that a universal quantum computer is Turing-complete, implying that it can simulate any Turing-computable function, given sufficient time and memory.

Note that the classical model of computation is typically not reversible, as memory can be erased. However, [Bennett, 1973] shows that computations can be made reversible by means of a reasonable amount of extra space.

Single Qubit Gates

Definition. The Pauli matrices are the following 2×2 complex matrices:

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix},$$
$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \quad I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

These matrices form a basis for $\mathbb{C}^{2\times 2}$. They are Hermitian and satisfy the relation $XYZ = iI$. The identity matrix I is sometimes omitted from the list.

The Pauli matrices perform the following transformations on the basis elements $|0\rangle$ and $|1\rangle$ of a single qubit:

1. The X gate maps $|0\rangle$ to $|1\rangle$ and $|1\rangle$ to $|0\rangle$. This is called a bit flip.
2. The Z gate leaves $|0\rangle$ unchanged and maps $|1\rangle$ to $-|1\rangle$. This is called a phase flip.
3. The Y gate performs both a bit flip and a phase flip.

4. The identity operator I performs an idle operation on a single qubit.

Definition. The Hadamard gate is the matrix

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

It exchanges the Z and X gates. The Hadamard matrix maps basis states $0\rangle$ and $|1\rangle$ to equally-weighted superposition states and vice-versa:

$$|0\rangle \xrightarrow{H} |+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}, \quad |+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \xrightarrow{H} |0\rangle,$$
$$|1\rangle \xrightarrow{H} |-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}, \quad |-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}} \xrightarrow{H} |1\rangle.$$

Multi-Qubit Gates

An important class of multi-qubit operations is given by the controlled gates, which act on 2 or more qubit and where one or more qubits act as a control for some operation

Definition. The controlled NOT (CNOT) gate acts on 2 qubits, performing the NOT operation on the target qubit only when the control qubit is $|1\rangle$, and otherwise leaving the target qubit unchanged. It is given by the matrix

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

Quantum Measurements

In a classical computer we can simply read the state of the bits at the end of a computation, but in a quantum computer we do not have direct, unrestricted access to the quantum state. This implies that we can't determine the state of a quantum system by means of a measurement; instead, partial information regarding the quantum state can be gathered through a measurement gate.

Definition. Given a q qubit quantum state $|\psi\rangle = \sum_{j\in\{0,1\}^q} \alpha_j |j\rangle$, a measurement gate on qubit k outputs 0 with probability $\sum_{j\in\{0,1\}^q\colon j_k=0} |\alpha_j|^2$ and 1 with probability $\sum_{j\in\{0,1\}^q\colon j_k=1} |\alpha_j|^2$. If $x \in 0, 1$ is the measured value, then after the measurement the quantum state becomes

$$\sum_{j\in\{0,1\}^q\colon j_k=x} \frac{\alpha_j}{\sqrt{\sum_{j\in\{0,1\}^q\colon j_k=x} |\alpha_j|^2}} |j\rangle,$$

and the original quantum state is no longer recoverable.

In other words, the state of the quantum system after a measurement collapses to a linear combination of only those basis states that are consistent with the outcome x of the measurement, i.e., basis states $|j\rangle$ with $j_k = x$. The coefficients α_j for such basis states are normalized to yield a unit vector.

Quantum computers can also perform measurements on two or more qubits simultaneously.

Definition. A quantum measurement is described by a spanning set of orthogonal subspaces V_j with corresponding projectors Π_j (i.e. $\Pi_j \Pi_l = 0$ when $j \neq k$). If the quantum system is in state $|\psi\rangle$, we get outcome $j \in V_j$ with probability

$$\mathbb{P}(|j) = \langle\psi|\Pi_j^* \Pi_j|\psi\rangle.$$

The posterior state of the quantum system is

$$\frac{\Pi_j|\psi\rangle}{\sqrt{\mathbb{P}(j)}}$$

The measurement operators satisfy the completeness equation:

$$\sum_j \Pi_j^* \Pi_j = I$$

Example 2. The projectors to measure the (single) qubit k of a quantum state are $|0\rangle\langle 0|_k \otimes I_{\overline{k}}$ and $|q\rangle\langle q|_k \otimes I_{\overline{k}}$.

Example 3. A complete quantum measurement of a q qubit is described by an orthonormal basis $|e_j\rangle$ for the state space. If the state of the system is $|\psi\rangle$then we get outcome e_j with probability $Pr(j) = |\langle e_j|\psi\rangle|^2$, and the posterior state is $|e_j\rangle$. If we expand $|\psi\rangle = \sum_i \alpha_i |e_i\rangle$, the amplitude α_j can be found by the inner product $\langle e_j|\psi\rangle = \langle e_i| \sum_i \alpha_i |e_i\rangle = \alpha_j$.

As in the case of a single qubit measurement, the state of the quantum system after a measurement collapses to a linear combination of only those basis states that are consistent with the outcome of the measurement.

We have a principle of uncertainty: measurements disturb the qubit. Following a measurement, the measured qubit becomes classical and the original quantum state is no longer recoverable. From an information theory standpoint, it implies that only a finite amount of classical information is storable in a qubit.

The Quantum Computation Model

In summary, a quantum computer performs 3 basic tasks:

1. A quantum state is contained in a quantum register (a set of q qubits grouped together) and by convention is initialized as $|0\rangle = \underbrace{|0\rangle \otimes |0\rangle}_{q \text{ times}}$.
2. The quantum state evolves by applying unitary operations as indicated by a succession of quantum gates.
3. At the end of the computation, partial information on the state of the quantum register is obtained using a measurement operator.

The input to the quantum computer is a circuit, comprising the instructions as well as the data (unless QRAM is assumed). The input circuits are then combined in an algorithm. The algorithm may be self-contained in the quantum computer, or it may involve an external, classical computing.