Lecture notes on Quantum Computing

Chapter 1 Mathematical Background

Vector states of a quantum system with n physical states are represented by unique vectors in $\mathbf{C}^n$, the set of $n \times 1$ column vectors[1] For example, a photon has vertical or horizontal polarization upon measurement. So, the quantum state of a photon is represented as a unit vector in $\mathbf{C}^2$. Furthermore, the theory is better explained using density matrices (positive definite matrices with trace one) to represent quantum states. Thus, we present some basic notation and results on vector and matrices in this chapter.

Here are the notation of number systems: $\mathbf{N} \subseteq \mathbf{Z} \subseteq \mathbf{Q} \subseteq \mathbf{R} \subseteq \mathbf{C}$.

1 Basics of Vectors

The set $\mathbf{C}^n$ of $n \times 1$ complex vectors form a vector space. Here is the formal definition.

Definition A complex vector space V has two operations:

the addition of two vectors x and y in V yielding $x + y$, and

the scalar multiplication of a complex scalar μ and a vector $x \in V$ yielding $\mu x \in V$

such that

1) $(x + y) + z = x + (y + z)$ and $x + y = y + x$ for all $x, y, z \in V$,

2) there is a zero vector $0 \in V$ such that $x + 0 = x$ for any $x \in V$,

3) for every $x \in V$, there is y such that $x + y = 0$,

4) $1x = x$ for any $x \in V$,

5) for any $\mu_1, \mu_2 \in \mathbf{C}$ and $x \in V$, we have $(\mu_1\mu_2)x = \mu_1(\mu_2 x)$, $(\mu_1 + \mu_2)x = \mu_1 x + \mu_2 x$,

6) for any $\mu \in \mathbf{C}$ and $x, y \in V$, we have $\mu(x + y) = \mu x + \mu y$,

Exercise Let $x = \begin{pmatrix} 1+i \\ 2 \end{pmatrix}$, $y = \begin{pmatrix} 3 \\ -2i \end{pmatrix}$ and $\mu = 1 + i$. Evaluate $\mu x + y$,

Operations and properties

Definition A linear functional f on a complex vector space V is a function $f : V \to \mathbf{C}$ such that $f(\mu x + y) = \mu f(x) + f(y)$ for all $x, y \in V$ and $\mu \in \mathbf{C}$. The set V^* of all linear functional on V form a linear space under the operations $f + g$ and μf such that $(f + g)(x) = f(x) + g(x)$ and $(\mu f)(x) = \mu f(x)$ for all $x \in V$ and $\mu \in \mathbf{C}$.

Denote by $e_1, \dots, e_n$ the standard unit vectors of $\mathbf{C}^n$, i.e., e_i has 1 at the ith position, and 0 elsewhere. The dual space of $\mathbf{C}^n$, denoted by $(\mathbf{C}^n)^* = \mathbf{C}^{n*}$ can be viewed as the vector space of $1 \times n$ complex row vectors such that every linear functional f on $\mathbf{C}^n$ corresponds to $1 \times n$ vector $v_f = (f(e_1), \dots, f(e_n))$ such that

$$f(x) = x \qquad \text{for all } x \in \mathbf{C}^n.$$

[1] Beginners always ask why we need to use complex vectors. The short answer is: only complex vectors can be used to provide a good model for quantum systems, and explain the observed phenomena.

In physics, one uses the **Dirac** notation so that the **ket** vector is:

$$|x\rangle = (x_1, \dots, x_n)^t = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in \mathbf{C}^n,$$

and the **bra** vector is:

$$\langle x| = (\bar{x}_1, \dots, \bar{x}_n) = (x_1^*, \dots, x_n^*) \in \mathbf{C}^{n*},$$

which is the dual vector of $|x\rangle$. The **norm** (**length**) of $|x\rangle$ is

$$\|x\| = \langle x|x\rangle^{1/2} = \{(\bar{x}_1, \dots, \bar{x}_n)(x_1, \dots, x_n)^t\}^{1/2} = \left\{\sum_{j=1}^{n} |x_j|^2\right\}^{1/2}.$$

(a) For $|x\rangle \in \mathbf{C}^n$, denote by $|x\rangle^t$ its transpose, $|\overline{x}\rangle = |x\rangle^*$ its conjugate, $|x\rangle^\dagger$ its conjugate transpose $|x\rangle^\dagger = \langle x|$.

(b) The **inner product** of $|x\rangle, |y\rangle \in \mathbf{C}^n$ is $\langle x|y\rangle = \sum_{j=1}^n \overline{x}_j y_j = \sum_{j=1}^n x_j^* y_j$. We have

$$\langle z|c_1 x + c_2 y\rangle = c_1\langle z|x\rangle + c_2\langle z|y\rangle \quad \text{and} \quad \langle c_1 x + c_2 y|z\rangle = \overline{c}_1\langle x|z\rangle + \overline{c}_2\langle y|z\rangle.$$

Two vectors are **orthogonal** if their inner product is zero.

(c) Given a set of vectors $S = \{|v_1\rangle, \dots, |v_r\rangle\}$ in $\mathbf{C}^n$, we can determine whether it is a **linearly independent set**, a **generating set**, a **basis**, an **orthonormal set**, or an **orthonormal basis**.

All these properties can be checked by considering the $n \times r$ matrix A with columns $|v_1\rangle, \dots, |v_r\rangle$.

c.1) S is linear independent if and only if A has rank r.

c.2) S is a generating set if and only if A has rank n.

c.3) S is a basis if and only if $n = r$ and A has rank n.

c.4) S is an orthonormal set if and only if $S^*S = I_r$.

c.5) S is an orthonormal basis if and only if $n = r$ and $S^*S = I_n$.

(d) If S is linearly independent, one can apply the Gram-Schmidt process to S to get an orthonormal set. If $|e_k\rangle$ is a unit vector, then the projection of a vector $|v\rangle$ in the direction of $|e_k\rangle$ is $|v\rangle - P_k|v\rangle$, where $P = |e_k\rangle\langle e_k|$ is the **projection operator**. The vector $|v\rangle - P_k|v\rangle$ is orthogonal to $|e_k\rangle$.

(e) If $\{|e_1\rangle, \dots, |e_n\rangle\}$ is an orthonormal basis and $P_k = |e_k\rangle\langle e_k|$ for $k = 1, \dots, n$, then

$$\text{(i) } P_k^2 = P_k, \quad \text{(ii) } P_j P_k = 0 \text{ for } j \neq k, \quad \text{(iii) } \textstyle\sum_{k=1}^n P_k = I_n.$$

Example 1 $P_1 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$, $P_2 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$.

Example 2 $P_1 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$, $P_2 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}$.

§2. Basics of Matrices

Pauli matrices:

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Linear maps (transformations/functions) on finite dimensional vector spaces can be identified with matrices, namely, $A : \mathbf{C}^n \to \mathbf{C}^n$ so that $|x\rangle \mapsto A|x\rangle$.

Let $\{|e_1\rangle, \ldots, |e_n\rangle\}$ be the standard basis for $\mathbf{C}^n$. Then

$$A_{ij} = \langle e_i|A|e_j\rangle \quad \text{and} \quad A = \sum_{i,j} A_{ij}|e_i\rangle\langle e_j|.$$

Operations and Properties

Let M_n be the set (vector space/algebra) of $n \times n$ matrices.

(a) One can perform $A + B$, AB and μA for $A, B \in M_n$ and $\mu \in \mathbf{C}$.

(b) One can compute the eigenvalues and eigenvectors of $A \in M_n$.

This can be done by solving the characteristic equation $\det(tI - A) = 0$, and for every zero t solve for nonzero vectors $|x\rangle$ such that $A|x\rangle = t|x\rangle$.

(c) Let $A \in M_n$. Denote by A^t, $\overline{A} = A^*$, and $A^\dagger$, its transpose, conjugate, and the conjugate transpose respectively.

(d) A matrix $A \in M_n$ is Hermitian if $A = A^\dagger$; it is skew-Hermitian if $A = -A^\dagger$; it is normal if $AA^\dagger = A^\dagger A$; it is unitary if $A^\dagger = A^{-1}$. If A is real and $A^t = A^{-1}$, then A is a real orthogonal matrix.

(e) For every $A \in M_n$, there is a unitary U such that U^*AU is in upper triangular form.

Proof. By induction on n. When $n = 1$, the result trivially holds. Suppose the result holds for matrices of size at most $n - 1$. For $A \in M_n$, one can solve $\det(tI - A) = 0$ and get a unit vector $|x\rangle$ such that $A|x\rangle = t|x\rangle$. Let $U_1 \in M_n$ with $|x\rangle$ as the first column. Then $U_1^\dagger AU_1 = \begin{pmatrix} t & * \\ 0 & A_1 \end{pmatrix}$. By induction assumption, there is unitary $U_2 \in M_{n-1}$ such that $U_2^\dagger A_2 U_2 = T$ is in triangular form. Let $U = U_1 \begin{pmatrix} 1 & \\ & U_2 \end{pmatrix}$. Then $U^\dagger AU = \begin{pmatrix} t & * \\ 0 & T \end{pmatrix}$ is in triangular form. □

(f) A matrix $A \in M_n$ is normal if and only if $A = U \begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{pmatrix} U^\dagger$ so that

$$A = \lambda_1 |u_1\rangle\langle u_1| + \cdots + \lambda_n |u_n\rangle\langle u_n|.$$

Proof. Suppose $A = UDU^\dagger$ for a diagonal matrix D. Then $AA^\dagger = UDD^\dagger U^\dagger = UD^\dagger DU^\dagger = A^\dagger A$. Conversely, suppose $AA^\dagger = A^\dagger A$, and suppose $U \in M_n$ is unitary such that $UAU^\dagger = T$ is in upper triangular form. Then $TT^\dagger = UAA^\dagger U^\dagger = UA^\dagger AU^\dagger = T^\dagger T$. Comparing the $(1,1)$ entry on both sides, one sees that the first row of T has the form $[t_{11}, 0, \ldots, 0]$. Comparing the $(2,2)$ entry on both sides, one sees that the second row of T has the form $[0, t_{22}, 0, \ldots, 0]$. Repeating this argument, one sees that T is a diagonal matrix. □

(g) Suppose A is normal. For any positive integer m,

$$A^m = \lambda_1^m |u_1\rangle\langle u_1| + \cdots + \lambda_n^m |u_n\rangle\langle u_n|.$$

The formula holds for negative integers m as well if A is invertible.

(h) For every $m \times n$ matrix A, there is unitary $U \in M_m$ and $V \in M_n$ so that $U^\dagger AV = \Sigma$ such that the (j,j) entries of Σ is s_j for $1 \leq j \leq \min\{m,n\}$, where $s_1^2 \geq s_2^2 \geq \cdots$ are the eigenvalues of $A^\dagger A$.

Proof. Suppose $V^\dagger A^\dagger AV = \mathrm{diag}\,(s_1^2, \ldots, s_n^2)$ with $s_1 \geq \cdots \geq s_n \geq 0$. Then the columns of AV form an orthogonal set. Suppose the first k columns of AV are nonzero. Then $k \leq m$. Let $|u_i\rangle$ be the ith column of AV divided by s_i, and let $U \in M_m$ with the first k columns equal to $|u_1\rangle, \ldots, |u_k\rangle$. Then $U^\dagger AV = \Sigma$. □

Tensor products

Let $A = (a_{ij})$ and B be two rectangular matrices. Then their tensor product (Kronecker product) is the matrix

$$A \otimes B = (a_{ij}B).$$

The following property hold for matrices A, B, C, D of appropriate sizes:

- $(A \otimes B)(C \otimes D) = (AC) \otimes (BD)$.
- $A \otimes (B + C) = A \otimes B + A \otimes C, \ (A \otimes B)^\dagger = A^\dagger \otimes B^\dagger, \ (A \otimes B)^{-1} = A^{-1} \otimes B^{-1}$.
- If A, B are square matrices and U, V are unitary matrices such that UAU^* and VBV^* are in upper triangular forms, then $(U \otimes V)(A \otimes B)(U \otimes V)^* = (UAU^*) \otimes (VBV^*)$ is in upper triangular form.
- If A, B are rectangular matrices with singular decomposition $U_1^* AV_1 = \Sigma_1$ and $U_2^* BV_2 = \Sigma_2$, then $(U_1 \otimes U_2)^*(A \otimes B)(V_1 \otimes V_2) = \Sigma_1 \otimes \Sigma_2$ is the singular value decomposition of $A \otimes B$.

Lie products and Jordan products

Let A and B be square matrices of the same size. Then their Lie product (commutator) is $[A, B] = AB - BA$; their Jordan product (anti-comutator) is $\{A, B\} = AB + BA$.

More examples and exercises

References