Lecture notes on Quantum Computing

Chapter 1 Mathematical Background Basic notation: $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$.

§1.1 Vector spaces

- $\mathbb{C}^n$ is the set of complex $n \times 1$ column vectors.
- $\mathbb{C}^n$ is a vector space under scalar multiplication and addition.
- We use the Dirac notation, bra-vector $\langle x|$ and ket-vector $|x\rangle$.

Terminology zero vector, (additive) inverse of a vector, complex and real vector spaces.

§1.2 Linear independent vectors and basis

- A set of vectors $\{|u_1\rangle, \ldots, |u_m\rangle\} \subseteq \mathbb{C}^n$ is linearly dependent if there are $a_1, \ldots, a_m \in \mathbb{C}$ not all zero such that $a_1|u_1\rangle + \cdots + a_m|u_m\rangle = |0\rangle$. Else, the set is linear independent. (How to check?)

- A set of vectors A set of vectors $\{|u_1\rangle, \ldots, |u_m\rangle\} \subseteq \mathbb{C}^n$ is generating if for every $|v\rangle \in \mathbb{C}^n$ there are $a_1, \ldots, a_m \in \mathbb{C}$ not all zero such that $|v\rangle = a_1|u_1\rangle + \cdots + a_m|u_m\rangle$. (How to check?)

- A linearly independent generating set for $\mathbb{C}^n$ is a basis. The number of vectors in it must be n, known as the dimension of $\mathbb{C}^n$.

§1.3 Linear functions and dual vector spaces

- A function $f : \mathbb{C}^n \to \mathbb{C}$ is a linear functional if $f(|u\rangle + |v\rangle) = f(|u\rangle) + f(|v\rangle)$ and $f(a|u\rangle) = af(|u\rangle)$ for all $a \in IC, |u\rangle, |v\rangle \in \mathbb{C}^n$.
- The set of functional on $\mathbb{C}^n$ form a vector space $\mathbb{C}^{n*}$, known as the dual space of $\mathbb{C}^n$.
- Each linear functional can be defined by $f(|u\rangle) = \langle v|u\rangle$ for some $|v\rangle \in \mathbb{C}^n$. Thus, $\mathbb{C}^{n*}$ can be viewed as the space of complex row vectors.

Inner product and length of vectors

- Define the inner product of $|u\rangle, |v\rangle \in \mathbb{C}^n$ by $\langle u|v\rangle = \bar{u}_1 v_1 + \cdots + \bar{u}_n v_n = u_1^* v_1 + \cdots + u_n^* v_n \in \mathbb{C}$.
- Then $\langle u|v\rangle = \langle v|u\rangle^*$, $\langle u|c_1 v + c_2 w\rangle = c_1\langle u|v\rangle + c_2\langle u|w\rangle$ for any $c_1, c_2 \in \mathbb{C}$, $|u\rangle, |v\rangle, |w\rangle \in \mathbb{C}^n$.
- Also, $\langle u, u\rangle = \sum_{j=1}^n |u_j|^2 \geq 0$, where the equality holds if and only if $|u\rangle = |0\rangle$.
- Define $\|u\| = \sqrt{\langle u|u\rangle}$ as the length or norm of $|u\rangle$.
- Two vectors $|u\rangle, |v\rangle \in \mathbb{C}^n$ are orthogonal if $\langle u, v\rangle = 0$.

§1.4 Orthonormal basis and the Gram-Schmidt process

- Express a vector as a linear combination of orthonormal basis $\{|e_1\rangle, \ldots, |e_n\rangle\}$.
- The set $\{P_j = |e_j\rangle\langle e_j| : j = 1, \ldots, n\}$ form a complete set of projection operators/matrices.
- Gram-Schmidt orthogonalization/orthonormalization.

§1.5 Linear operators and Matrices

- A function $T : \mathbb{C}^n \to \mathbb{C}^n$ is linear if $T(|u\rangle + |v\rangle) = T(|u\rangle) + T(|v\rangle)$ and $T(c|u\rangle) = cT(|u\rangle)$ for all $c \in \mathbb{C}, |u\rangle, |v\rangle \in \mathbb{C}^n$.
- Every linear function on $\mathbb{C}^n$ has the form $T(|v\rangle) = A|v\rangle$ for an $n \times n$ matrix $A = (A_{ij})$.
- Let A be a matrix. We can define the transpose A^t, the conjugate A^* or sometimes $\bar{A}$, and the Hermitian conjugate $A^\dagger = (\bar{A})^t$.
- A square matrix A is Hermitian if $A = A^\dagger$; A is unitary if $A^\dagger A = I_n$; A is normal if $A^\dagger A = AA^\dagger$.

§1.7 Pauli matrices $\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $\sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$, $\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ and their properties

- The Jordan product $\{\sigma_u, \sigma_v\} = \sigma_u\sigma_v + \sigma_v\sigma_u = 2\delta_{uv}I_2$, where δ_{uv} is the Kronecker symbol.
- The Lie product $[\sigma_u, \sigma_v] = \sigma_u\sigma_v - \sigma_v\sigma_u = 2i\xi_{uv}\sigma_w$ where $\xi_{uv} = 1$ if $(u, v) = (x, y), (y, z), (z, x)$ and $\xi_{uv} = -1$ if $(u, v) = (y, x), (z, y), (x, z)$.

§1.6 & 1.8 Eigenvalues

Let A be an $n \times n$ complex matrix. Then $\lambda \in \mathbb{C}$ is an eigenvalue of A if there is a nonzero eigenvector $|\lambda\rangle$ such that $A|\lambda\rangle = \lambda|\lambda\rangle$.

- The matrix A always has complex eigenvalues because $\det(tI - A) = 0$ always has a solution λ so that $(\lambda I - A)|\lambda\rangle = |0\rangle$ has non-trivial solution.
- There is a unitary matrix U such that $U^\dagger AU = T$ is in upper triangular form. Moreover, $\det(tI - A) = \det(tI - T) = (t - T_{11}) \cdots (t - T_{nn})$.
- The matrix A is normal if and only if T is diagonal; the matrix A is unitary if and only if T is a diagonal matrix so that the diagonal entries have moduli 1; the matrix A is Hermitian if and only if T is a real diagonal matrices.

Proof of the Schur Triangularization Lemma. Suppose $A \in M_n$. We show that there a unitary $U \in M_n$ such that $U^\dagger AU = T$ is in upper triangular form. We prove the result by induction on n. If $n = 1$, the result is trivial. Suppose the result holds for matrices in M_{n-1}. Let $A \in M_n$. Solve $\det(tI - A) = 0$ to get a solution λ.There is a nonzero vector $|\lambda\rangle$ such that $A|\lambda\rangle = \lambda|\lambda\rangle$. We may replace $|\lambda\rangle$ by $|\lambda\rangle/\||\lambda\rangle\|$ and assume that $|\lambda\rangle$ has unit length, and we can let $U_1 \in M_n$ be unitary with $|\lambda\rangle$ as the first column. Then $AU_1 = [A|x_1\rangle \cdots A|x_n\rangle] = [\lambda|x_1\rangle A|x_2\rangle \cdots A|x_n\rangle]$ if U_1 has columns $|x_1\rangle = |\lambda\rangle, |x_2\rangle, \ldots, |x_n\rangle$. Because $\langle x_1|A|x_1\rangle = \lambda$, and $\langle x_j|A|x_1\rangle = 0$ for $j = 2, \ldots, n$, we see that $U^\dagger AU = \begin{pmatrix} \lambda_1 & * \\ 0 & A_1 \end{pmatrix}$. By induction assumption there is a unitary $U_2 \in M_{n-1}$ such that $U_2^\dagger A_1 U_2 = T_1$ in upper triangular form. Let $U = U_1 \begin{pmatrix} 1 & 0 \\ 0 & U_2 \end{pmatrix} \in M_n$. Then $U^\dagger U = I_n$ so that U is unitary, and $U^\dagger AU = \begin{pmatrix} 1 & 0 \\ 0 & U_2^\dagger \end{pmatrix} \begin{pmatrix} \lambda_1 & * \\ 0 & A_1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & U_2 \end{pmatrix} = \begin{pmatrix} \lambda & * \\ 0 & T_1 \end{pmatrix}$ is upper triangular form. □

Proof of the consequences for normal, unitary, Hermitian matrices. Let $U^\dagger AU = T$. Suppose A is normal, i.e., $A^\dagger A = AA^\dagger$. Then

$$T^\dagger T = (U^\dagger AU)^\dagger (U^\dagger AU) = (U^\dagger A^\dagger U)(U^\dagger AU) = U^\dagger A^\dagger AU = U^\dagger AA^\dagger U = TT^\dagger.$$

Now, the $(1,1)$ entry of $T^\dagger T$ is $|T_{11}|^2$ and the $(1,1)$ entry of $TT^\dagger$ is $|T_{11}|^2 + \cdots + |T_{1n}|^2$. So, $T_{12} = \cdots = T_{1n} = 0$. Now, consider the $(2,2), \ldots, (n,n)$ entries, we see that only the diagonal entries of T can be nonzero. So, T is a diagonal matrix. Conversely, if $U^\dagger AU = T$ is in diagonal form, then $A = UTU^\dagger$ so that $A^\dagger A = U^\dagger T^\dagger UU^\dagger TU = U^\dagger T^\dagger TU$ and $AA^t = U^\dagger TT^\dagger U$. Note that for a diagonal matrix T, we have $TT^\dagger = T^\dagger T$ is a diagonal matrix with diagonal entries $|T_{11}|^2, \ldots, |T_{nn}|^2$. So, $A^\dagger A = AA^\dagger$.

Now, if A is unitary, then A is normal and $T = U^\dagger AU$ is diagonal, and is unitary. So, $T^\dagger T = I_n$ implies $|T_{jj}|^2 = 1$ for all j. Conversely, if $A = U^\dagger TU$ such that T is diagonal with all diagonal entries satisfying $|T_{jj}| = 1$, then $A^\dagger A = UT^\dagger U^\dagger UTU^\dagger = UT^\dagger TU^\dagger = UU^\dagger = I_n$.

Finally, suppose A is Hermitian, then $A = A^\dagger$ so that the diagonal matrix T satisfies $T^\dagger = UA^\dagger U^\dagger = UAU^\dagger = T$ So, T is Hermitian and all the diagonal entries of T are real. Conversely, if T is a real diagonal matrix, then $T = T^\dagger$ so that $A^\dagger = U^\dagger T^\dagger U = U^\dagger TU = A$. □

§1.9 Spectral decomposition

- Suppose A is normal and $A = UDU^\dagger$, where D has diagonal entries $\lambda_1, \ldots, \lambda_n$ and U has orthonormal columns $|\lambda_1\rangle, \ldots, |\lambda_n\rangle$. Then $A = \lambda_1|\lambda_1\rangle\langle\lambda_1| + \cdots + \lambda_n|\lambda_n\rangle\langle\lambda_n|$ so that

$$A^k = \sum_{j=1}^{n} \lambda_j^k |\lambda_j\rangle\langle\lambda_j| \qquad \text{and} \qquad e^A = \sum_{k=0}^{\infty} \frac{1}{k!} A^k = \sum_{j=1}^{n} e^{\lambda_j} |\lambda_j\rangle\langle\lambda_j|.$$

- Also, $A = \sum_\alpha \alpha P_\alpha$, where $P_\alpha = \sum_{\lambda_j = \alpha} |\lambda_j\rangle\langle\lambda_j|$. Then $A^k = \sum_\alpha \alpha^k P_\alpha$ and $e^A = \sum_\alpha e^\alpha P_\alpha$.

Proof. Because $A|\lambda_j\rangle = \lambda_j|\lambda_j\rangle$ for $j = 1, \ldots, n$, we have $AU = UD$ so that

$$A = UDU^\dagger = \sum_{j=1}^{n} \lambda_j |\lambda_j\rangle\langle\lambda_j|.$$

Now,

$$A^k = \underbrace{UDU^\dagger \cdots UDU^\dagger}_{k} = UD^kU^\dagger = \sum_{j=1}^{n} \lambda_j^k |\lambda_j\rangle\langle\lambda_j|,$$

and

$$e^A = \sum_{k=0}^{\infty} \frac{1}{k!} A^k = \sum_{k=0}^{\infty} \frac{1}{k!} \sum_{j=1}^{n} \lambda_j^k |\lambda_j\rangle\langle\lambda_j| = \sum_{j=1}^{n} e^{\lambda_j} |\lambda_j\rangle\langle\lambda_j|.$$

§1.9 Singular value decomposition (SVD)

Theorem *Every square matrix A can be written as $A = UDV^\dagger$, where U, V are unitary and $D = \operatorname{diag}(s_1, \ldots, s_n)$ with $s_1 \geq \cdots \geq s_n \geq 0$.*

Proof. Proof by induction on the size of A. Clearly, the result holds for $n = 1$. Assume that the result is true for matrices of size less than n with $n \geq 2$. Choose unitary U, V such that $S = U_1^\dagger A V_1$ has largest $(1,1)$ entry with largest real part S_{11}. First, we have $S_{11} \geq 0$, else replace V by $e^{it}V$ for some suitable e^{it}. Next, we claim that $S_{1j} = 0$ for $j = 2, \ldots, n$. If not, we can replace V_1 by $V_1 R$ where R is obtained from I_n by changing the 2×2 submatrix in rows and columns $1, j$ by $\frac{1}{\sqrt{S_{11}^2 + |S_{1j}|^2}} \begin{pmatrix} S_{11} & S_{1j} \\ \bar{S}_{1j} & -S_{11} \end{pmatrix}$. Then $U_1^\dagger A V_2 R$ has $(1,1)$ entry equal to $\sqrt{S_{11}^2 + |S_{1j}|^2} > S_{11}$, which is a contradiction. Similarly, we can show that $S_{j1} = 0$ for all $j = 2, \ldots, n$. Thus, $S = \begin{pmatrix} 1 & 0 \\ 0 & \hat{S} \end{pmatrix}$. By induction assumption, there are unitary U_2, V_2 such that $U_2^\dagger \hat{S} V_2 = \operatorname{diag}(s_2, \ldots, s_n)$.

Let $V = V_1 \begin{pmatrix} 1 & \\ & V_2 \end{pmatrix}$ and $U = U_1 \begin{pmatrix} 1 & \\ & U_2 \end{pmatrix}$. Then $U^\dagger A V = \operatorname{diag}(s_1, \ldots, s_n)$. □

Note $s_1, \ldots, s_n$ are the singular values of A and equal the nonnegative square roots of the eigenvalues of $A^\dagger A$ or / and $AA^\dagger$.

The matrix A has rank k if and only if it has k nonzero singular values.

In practice, write $A^\dagger A = V D^2 V^\dagger$ so that the columns of the unitary matrix V, $|v_1\rangle, \ldots, |v_n\rangle$, are the right singular vectors. Then $AV = UD$ for some unitary U such that $A = UDV^\dagger$. In particular, if $s_j \neq 0$ then $|u_j\rangle = A|v_j\rangle / s_j$; if A has rank k so that $s_k > 0 = s_{k+1} = \cdots = s_n$ then $|u_{k+1}\rangle, \ldots, |u_n\rangle$ are chosen so that $\{|u_1\rangle, \ldots, |u_n\rangle\}$ is an orthonormal basis.

In Matlab, we use the command $[U, D, V] = \operatorname{svd}(A)$.

§1.10 Tensor product (Kronecker product)

- $A \otimes B = (A_{ij}B)$ satisfies

  (a) $(A \otimes B)(C \otimes D) = (AC) \otimes (BD)$,

  (b) $A \otimes (B + C) = A \otimes B + A \otimes C$, $(A \otimes B)^\dagger = A^\dagger \otimes B^\dagger$, $(A \otimes B)^{-1} = A^{-1} \otimes B^{-1}$.

  (c) $\operatorname{tr}(A \otimes B) = (\operatorname{tr} A)(\operatorname{tr} B)$ and $\det(A \otimes B) = \det(A)^n \det(B)^m$ if $A \in M_m, B \in M_n$.

Proof. (a) Let A be $m \times n$, B be $r \times s$, C be $n \times p$, D be $s \times q$. Then $A \otimes B = (A_{ij}B)$ is $mr \times ns$, and $C \otimes D = (C_{ij}D)$ is $ns \times pq$. Now

$$(A \otimes B)(C \otimes D) = (A_{ij}B)(C_{ij}D) = (f_{rs}BD),$$

where $f_{rs} = \sum_{\ell=1}^{n} A_{r\ell}C_{\ell s} = (AC)_{rs}$. So, $(f_{rs}BD) = AC \otimes BD$.

(b) $A \otimes (B + C) = (A_{ij}(B + C)) = (A_{ij}B) + (A_{ij}C) = A \otimes B + A \otimes C$.

$(A \otimes B)^\dagger = \overline{A \otimes B)^t} = \overline{(A^t \otimes B^t)} = A^\dagger \otimes B^\dagger$.

$(A^{-1} \otimes B^{-1})(A \otimes B) = (A^{-1}A) \otimes (B^{-1}B) = I_m \otimes I_n = I_{mn} \implies A^{-1} \otimes B^{-1} = (A \otimes B)^{-1}$.

(c) Note that $\operatorname{tr}(AB) = \sum_{i=1}^{n} \sum_{j=1}^{n} A_{ij}B_{ji} = \operatorname{tr}(BA)$. Assume that A is $m \times m$ and B is $n \times n$. Let U, V be unitary and S, T be triangular such that $A = USU^\dagger$ and $B = VTV^\dagger$. Then $\operatorname{tr} A = \operatorname{tr} S, \operatorname{tr} B = \operatorname{tr} T$,

$$\operatorname{tr}(A \otimes B) = \operatorname{tr}((U \otimes V)(S \otimes T)(U \otimes V)^\dagger) = \operatorname{tr}(S \otimes T)$$

$$= \sum_{i=1}^{m} S_{ii} \sum_{j=1}^{n} T_{jj} (\sum_{i=1}^{m} S_{ii})(\sum_{j=1}^{n} T_{jj}) = (\operatorname{tr} S)(\operatorname{tr} T) = (\operatorname{tr} A)(\operatorname{tr} B).$$

Also,

$$\det(A \otimes B) = \det((U \otimes V)(S \otimes T)(U \otimes V)^\dagger) = \det(S \otimes T)$$

$$= \prod_{i=1}^{m} {S_{ii}}^n \det(T) = (\det S)^n (\det T)^m = (\det A)^n (\det B)^m.$$