Quantum Computing

Korben Rusek

6-1-2018

2 Linear Algebra

Lemma 2.1. Let A be a non-singular linear operator. If all the eigenvalues of A are ± 1 then $A^2 = I$

Proof. Since A is non-singular and normal with eigenvalues ± 1 then we can write $A = \sum \lambda_i |i\rangle \langle i|$ with $|i\rangle$ spanning the vector space. Then we have

$$\begin{aligned}
A^2 &= \left(\sum_i \lambda_i |i\rangle \langle i|\right)\left(\sum_j \lambda_j |j\rangle \langle j|\right) \\
&= \sum_i \sum_j \lambda_i |i\rangle \langle i| \lambda_j |j\rangle \langle j| \\
&= \sum_i \sum_j \lambda_i \lambda_j |i\rangle \langle i|j\rangle \langle j| \\
&= \sum_i \sum_j \lambda_i \lambda_j |i\rangle \delta_{i,j} \langle j| \\
&= \sum_i \sum_j \lambda_i \lambda_j \delta_{i,j} |i\rangle \langle j| \\
&= \sum_i \lambda_i^2 |i\rangle \langle i| \\
&= \sum_i |i\rangle \langle i| \\
&= I
\end{aligned}$$

□

Lemma 2.2. Let $A = \sum_x |x\rangle \langle x| - \sum_y |y\rangle \langle y|$, where $\{|x\rangle, |y\rangle\}_{x,y}$ form an orthonormal basis. Then

$$f(\theta A) = \frac{f(\theta) + f(-\theta)}{2} I + \frac{f(\theta) - f(-\theta)}{2} A.$$

Proof. We can write $A = \sum_x |x\rangle\langle x| - \sum_y |y\rangle\langle y|$. Let $X = \sum_x |x\rangle\langle x|$ and $Y = \sum_y |y\rangle\langle y|$. That means that $I = X + Y$ and $A = X - Y$. Then we have

$$\begin{aligned}
f(\theta)A &= \sum_x f(\theta)|x\rangle\langle x| + \sum_y f(-\theta)|y\rangle\langle y| \\
&= f(\theta)\sum_x |x\rangle\langle x| + f(-\theta)\sum_y |y\rangle\langle y| \\
&= f(\theta)X + f(-\theta)Y \\
&= \frac{f(\theta)}{2}X + \frac{f(\theta)}{2}Y + \frac{f(\theta)}{2}X - \frac{f(\theta)}{2}Y + \frac{f(-\theta)}{2}Y + \frac{f(-\theta)}{2}Y + \frac{f(-\theta)}{2}X - \frac{f(-\theta)}{2}X \\
&= \frac{f(\theta)}{2}(X+Y) + \frac{f(-\theta)}{2}(X+Y) + \frac{f(\theta)}{2}(X-Y) - \frac{f(-\theta)}{2}(X-Y) \\
&= \frac{f(\theta)+f(-\theta)}{2}I + \frac{f(\theta)-f(-\theta)}{2}A
\end{aligned}$$

□

Exercise 2.44. Suppose that A is invertible and that $\{A, B\} = [A, B] = 0$. Show that B is 0.

Proof. $[A, B] = 0$ tells us that $AB = BA$ and $\{A, B\} = 0$ tells us that $AB = -BA$. Therefore we know that $BA = -BA$. Now multiplying on the right side by A^{-1}, we get $B = -B$. Thus $-2B = 0$ which implies that $B = 0$. □

Exercise 2.45. Show that $[A, B]^\dagger = [B^\dagger, A^\dagger]$.

Proof.

$$\begin{aligned}
[A, B]^\dagger &= (AB - BA)^\dagger \\
&= B^\dagger A^\dagger - A^\dagger B^\dagger \\
&= [B^\dagger, A^\dagger].
\end{aligned}$$

□

Exercise 2.46. Show that $[A, B] = -[B, A]$.

Proof.

$$\begin{aligned}
[A, B] &= AB - BA \\
&= -(BA - AB) \\
&= -[B, A]
\end{aligned}$$

□

Exercise 2.47. Suppose that A and B are Hermitian. Show that $i[A, B]$ is Hermitian.

Proof. Suppose that $A = A^\dagger$ and $B = B^\dagger$. Then we have

$$\begin{aligned}(i[A,B])^\dagger &= -i[B^\dagger, A^\dagger] \\ &= -i[B,A] = i[A,B].\end{aligned}$$

Therefore $i[A,B]$ is Hermitian. □

Lemma 2.3. Let A be a diagonalizable matrix. Write $A = \sum_i \lambda_i |i\rangle$. Then $\sqrt{A^\dagger A} = \sum_i |\lambda_i| |i\rangle \langle i|$.

Proof. The proof is pretty straight forward. We start with

$$\begin{aligned}A^\dagger A &= \left(\sum_i \lambda_i^* |i\rangle \langle i|\right)\left(\sum_i \lambda_i |i\rangle \langle i|\right) \\ &= \sum_i |\lambda_i|^2 |i\rangle \langle i|.\end{aligned}$$

Therefore $\sqrt{A^\dagger A} = \sum_i |\lambda_i| |i\rangle \langle i|$. □

Exercise 2.48. What is the polar decomposition of a positive matrix, P? Of a unitary matrix, U? or a Hermitian matrix, H?

Positive matrix. By the above lemma, for a positive matrix, P, $\sqrt{P^\dagger P} = P$. Therefore we have IP or PI as the polar decompositions. □

Unitary matrix. Suppose V is unitary. By the above lemma $\sqrt{V^\dagger V} = I$. Therefore $V = VI = IV$ is the polar decomposition. □

Hermitian matrix. Suppose that H is Hermitian. Write $H = \sum_i \lambda_i |i\rangle \langle i|$. Then $J = \sum_i |\lambda_i| |i\rangle \langle i|$. Let a_i be defined as $\lambda_i/|\lambda_i|$ when $\lambda_i \neq 0$ and 1 when $\lambda_i = 0$. Then $U = \sum_i v_i |i\rangle \langle i|$. □

Exercise 2.49. Express the polar decomposition of a normal matrix in the outer product representation.

Proof. The solution is similar to what we see in the Hermitian version of the above exercise. J has eigenvalues that are the absolute value of the eigenvalues of H. U would have eigenvalues that are the unit vectors of the eigenvalues of H (or 1 when eigenvalues are 0). □

Exercise 2.50. Find the left and right polar decompositions of the matrix

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

Proof. It is easy to see that the eigenvalues of P is 1 repeated. Therefore P is positive. Therefore $U = I$ and $J = K = P$. □

Definition 2.4. We define H to be the Hadamard matrix.

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

Exercise 2.51. Verify that th Hadamard gate H is unitary.

Proof.

$$H^2 = \frac{1}{2}\begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix} = I.$$

It is clear that $H^\dagger = H$. Thus $H \dagger H = I$ and H is unitary. □

Exercise 2.52. Verify that $H^2 = I$.

Proof. This was shown in the previous exercise. □

Exercise 2.53. What are the eigenvalues and eigenvectors of H?

Proof. To find the eigenvalues of H we solve the polynomial equation

$$\begin{aligned} 0 &= (1-\lambda)(-1-\lambda) - 1 \\ &= (\lambda - 1)(\lambda + 1) - 1 \\ &= \lambda^2 - 2. \end{aligned}$$

Thus our eigenvalues are $\lambda = \pm\sqrt{2}$. To find the eigenvectors we solve the system:

$$\begin{aligned} x + y &= \frac{\lambda}{\sqrt{2}}x \\ x - y &= \frac{\lambda}{\sqrt{2}}y \end{aligned}$$

Since $(0, 1)$ is clearly not an eigenvector we can assume that $x = 1$. For $\lambda = 1$ we have $y = \frac{1-\sqrt{2}}{\sqrt{2}}$. For $\lambda = -1$ we get $y = \frac{-1+\sqrt{2}}{\sqrt{2}}$. Therefore we have the eigenvectors $(\sqrt{2}, 1 - \sqrt{2})$ and $(\sqrt{2}, \sqrt{2} - 1)$ with eigenvalues 1 and -1 respectively. □

Exercise 2.54. Suppose A and B are commuting Hermitian operators. Prove that $exp(A)exp(B) = exp(A + B)$.

Proof. We can write $A = \sum_i a_i |i\rangle \langle i|$ and $B = \sum_i b_i |i\rangle \langle i|$ for some orthonormal basis $|i\rangle$. Then we have

$$exp(A) = \sum_i e^{a_i} keti \langle i| ,$$

$$exp(B) = \sum_i e^{b_i} keti \langle i| ,$$

and so

$$\begin{aligned} exp(A)exp(B) &= \sum_i e^{a_i} e^{b_i} keti \langle i| \\ &= \sum_i e^{a_i + b_i} keti \langle i| \\ &= exp(A + B). \end{aligned}$$

□

Definition 2.5.

$$U(t_1, t_2) = exp\left[\frac{-iH(t_2 - t_1)}{\hbar}\right].$$

Exercise 2.55. Prove that $U(t_1, t_2)$ is unitary.

Proof. This is simple as $exp(x)$ is non-zero, so U is unitary. □

Exercise 2.56. Use spectral decomposition to show that $K = -i\log(U)$ is Hermitian for any unitary U, and thus $U = \exp(iK)$ for some Hermitian K.

Proof. Let U be unitary. Then we can write $U = \sum \alpha_\phi |\phi\rangle \langle\phi|$ for some orthonormal basis $\langle\phi|$ and $\alpha_\phi \neq 0$. That means that $K = \sum -i\log(\alpha_\phi) |\phi\rangle \langle\phi|$. Since U is unitary then $\alpha_\phi = e^{i\theta_\phi}$ for some real θ_ϕ. Therefore we can simplify K to

$$K = \sum -i(i\theta_p hi) |\phi\rangle \langle\phi| = \sum \theta_\phi |\phi\rangle \langle\phi|.$$

Now sime θ_ϕ is real then K is Hermitian. Therefore any unitary operator is $\exp(iK)$ for some Hermitian K. □

Exercise 2.58. Suppose we prepare a quantum system in an eigenstate $|\psi\rangle$ of some observable M, with corresponding eigenvalue m. What is the average observed value of M, and the standard deviation?

Proof. The average observed value of M is given by $E(M) = \langle\psi| M |\psi\rangle$. Then we have

$$\begin{aligned} E(M) &= \langle\psi| M |\psi\rangle \\ &= m \langle\psi|\rangle \psi \\ &= m. \end{aligned}$$

The standard deviation squared is given by

$$[\Delta(M)]^2 = \langle M^2\rangle - \langle M\langle^2.$$

We already saw that $\langle M\rangle = m$. And so we have

$$\begin{aligned} \langle M^2\rangle &= \langle\psi| M^2 |\psi\rangle \\ &= \langle\psi| mM |\psi\rangle \\ &= m^2 \langle\psi|\psi\rangle \\ &= m^2. \end{aligned}$$

Therefore the standard deviation is 0. □

Exercise 2.59. Suppose we have a qubit in the state $|0\rangle$, and we measure the observable X. What is the average value of X? What is the standard deviation of X?

Proof. The average value is given by $\langle 0| X |0\rangle = \langle 0|1\rangle = 0$.

The standard deviation squared is

$$\langle 0| X^2 |0\rangle = \langle 0|0\rangle = 1.$$

□

Exercise 2.60. Show that $v \cdot \sigma$ has eigenvalues ± 1 and that the projectors onto the correspnding eigenspaces are given by $P_\pm = (I \pm v \cdot \sigma)/2$.

Proof. We have already seen that $v \cdot \sigma$ has eigenvalues ± 1. It is easy to verify that the eigenvectors of $v \cdot \sigma$ are

$$e_\pm = \begin{bmatrix} 1 \pm c \\ a \pm bi \end{bmatrix}.$$

Furthermore $P \pm e_\pm = e_\pm$. Therefore $P_\pm$ are the projectors. □

Exercise 2.61. Calculate the probability of obtaining $+1$ for a measurement of $v \cdot \sigma$, given that the state prior to measurement is $|0\rangle$. What is the state of the system after the measurement?

Proof. The value $p(+1)$ is given by $\langle 0| P_+ |0\rangle$. This gives $\frac{1}{2} \left\langle 0 \middle| \begin{bmatrix} 1+c \\ a+bi \end{bmatrix} \right\rangle = \frac{1+c}{2}$.

After measurement the state of the system is

$$\frac{P_+ |0\rangle}{\sqrt{p(+1)}} = \begin{bmatrix} 1+c \\ a+bi \end{bmatrix} \sqrt{\frac{2}{1+c}}$$

□

Exercise 2.62. Show that any measurement where the measurement operators and the POVM elements coincide is a projective measurement.

Proof. Let M_m be the collection of measurement operators. We will show that $M_m = M_m^\dagger M_m$. Since $M_m = E_n$ for some n, then $M_m^\dagger M_m = E_n^\dagger E_n = E_n = M_m$. This means that M_m is positive. In that case $M_m^\dagger = M_m$ and we have M_m is projective as $M_m^2 = M_m$. □

Exercise 2.63. Suppose a measurement is described by measurement operators, M_m. Show that there exist unitary operators U_m such that $M_m = U_m \sqrt{E_m}$, where E_m is the POVM associated to the measurement.

Proof. Write $M_m = \sum \lambda_i |i\rangle \langle i|$. Then $E_m = M_m^\dagger M_m = \sum |\lambda_i|^2 |i\rangle \langle i|$. Therefore $U_m = \sum_i \frac{\lambda_i}{|\lambda_i|} |i\rangle \langle i|$. □

Exercise 2.64. Suppose Bob is given a quantum state chosen from a set $|\psi_1\rangle, \ldots, |\psi_m\rangle$ of linearly independent states. Construct a POVM $\{E_1, \ldots, E_{m+1}\}$ such that if outcome E_i occurs for $1 \leq i \leq m$ then Bob knows with certainty that he was give the state $|\psi_i\rangle$. (The POVM must be such that $\langle \psi_i| E_i |\psi_i\rangle > 0$ for each i.)

Proof. Let $E_i = |\psi_i\rangle \langle\psi_i|$ for $1 \leq i \leq m$ and $E_{m+1} = I - \sum E_i$. Then for $1 \leq i \leq m$, we have

$$\begin{aligned} \langle\psi_i| E_j |\psi_i\rangle &= \langle\psi_i|\psi_j\rangle \langle psi_j|\psi_i\rangle \\ &= \delta_{i,j}\delta_{i,j}. \end{aligned}$$

Therefore we only get E_i when we also have ψ_i. It's also easy to see that E_{m+1} won't happen for ψ_i. □

Exercise 2.65. Express the states $(\langle 0| + \langle 1|)/\sqrt{2}$ and $(\langle 0| - \langle 1|)/\sqrt{2}$ in a basis in which they are *not* the same up to a relative phase shift.

Proof. These elements are the elements $|+\rangle$ and $|-\rangle$, so in that basis they are not the same up to a relative phase shift. □

Exercise 2.66. Show that the average value of the observable $X_1 Z_2$ for a two qubit system measured in the state $(|00\rangle + |11\rangle)/\sqrt{2}$ is zero.

Proof. Let $\psi = (|00\rangle + |11\rangle)/\sqrt{2}$. We have

$$\begin{aligned} \langle\psi| X_1 Z_2 |\psi\rangle &= \langle\psi| X_1 Z_2 (|00\rangle + |11\rangle)/\sqrt{2} \\ &= \langle\psi| X_1 (|00\rangle - |11\rangle)/\sqrt{2} \\ &= \frac{1}{2}(\langle 00| + \langle 11|)(|10\rangle - |01\rangle) \\ &= 0 \end{aligned}$$

□

Exercise 2.67. Suppose V is a Hilbert space with subspace W. Suppose $U : W \to U$ is a linear operator which preserves inner products, that is, for any $|w_1\rangle$ and $|w_2\rangle$ in W,

$$\langle w_1| U^\dagger U |w_2\rangle = \langle w_1|w_2\rangle .$$

Prove that there exists a unitary operator $U' : V \to V$ which *extends* U. That is, $U'|w\rangle = U|w\rangle$ for all $w \in W$, but U' is defined on the entire space V. Usually we omit the prime symbol and just write U to denote the extension.

Proof. Let the set $\{|w_i\rangle\}$ be an orthonormal basis for W. We extend this set with elements $\{|v_j\rangle\}$ such that $\{|w_i\rangle\} \cup \{|v_j\rangle\}$ forms an orthonormal basis of V.

On elements v_j we define U' such that $U'|v_j\rangle = |v_j\rangle$. Then we can linearly extend it to finite linear combinations of elements of $\{|w_i\rangle\} \cup \{|v_j\rangle\}$. It is straight forward to see that we still have inner products preserved. □

Exercise 2.68. Define

$$|\psi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}.$$

Prove that $\psi \neq |a\rangle |b\rangle$ for all single qubit states $|a\rangle$ and $|b\rangle$.

Proof. Define $|a\rangle = a_0 |0\rangle + a_1 |1\rangle$ and $|b\rangle = b_0 |0\rangle + b_1 |1\rangle$. Then we have

$$\begin{aligned} |a\rangle |b\rangle &= (a_0 |0\rangle + a_1 |1\rangle)(b_0 |0\rangle + b_1 |1\rangle) \\ &= a_0 b_0 |00\rangle + a_0 b_1 |01\rangle + a_1 b_0 |01\rangle + a_1 b_1 |11\rangle . \end{aligned}$$

To have $|\psi\rangle = |a\rangle |b\rangle$ we need to have $a_0 b_0 = 1$ and $a_1 b_1 = 1$. This means that we need $a_0, a_1, b_0, b_1 \neq 0$. But we also have to have $a_0 b_1 = 0$ and $a_1 b_0 = 0$. This is impossible because none of the values can be 0. □

Exercise 2.69. Verify that the Bell basis forms an orthonormal basis for the two qubit state space.

Proof. This is straight forward as the only elements from the Bell states that have shared elements have a single element with an opposite sign. □

Exercise 2.70. Suppose that E is any positive operator acting on Alice's qubit. Show that $|\psi\rangle E \otimes I |\psi\rangle$ takes the same value when $|\psi\rangle$ is any of the four Bell states. Suppose an malevolent third party, Eve, intercepts Alice's qubit on the way to Bob in the superdence coding protocol. Can Eve infer anything about which of the four possible bit strings 00, 01, 10, 11 Alice is trying to send? If so, how, or if not, why not?

Proof. □

Exercise 2.71. Let ρ be a density operator. Show that $\mathrm{tr}(\rho^2) \geq 1$, with equality if and only if ρ is a pure state.

Proof. Let $\rho = \sum p_i |\psi_i\rangle \langle\psi_i|$ be a density operator. Then

$$\begin{aligned} \rho^2 &= (\sum_i p_i |\psi_i\rangle \langle\psi_i|)(\sum_j p_j |\psi_j\rangle \langle\psi_j|) \\ &= \sum_i \sum_j p_i p_j |\psi_i\rangle \langle\psi_i|\psi_j\rangle \langle\psi_j| \\ &= \sum_i \sum_j p_i p_j |\psi_i\rangle \delta_{i,j} \langle\psi_j| \\ &= \sum_i p_i^2 |\psi_i\rangle \langle\psi_i| \end{aligned}$$

Now since $p_i > 0$ and $\sum p_i = 1$ then $\sum p_i^2 \leq 1$. Now if any $p_i \neq 1$ then $\sum p_i^2 < 1$. That is, that means that ρ is not pure. On the other hand if ρ is pure than $p_i = 1$ for one p_i and we have $\mathrm{tr}(\rho^2) = 1$ □

Exercise 2.72 (Bloch sphere for mixed states)**.** The Block sphere picture for states of a single qubit was introduced in section 1.2. This description has an important generalization to mixed states as follows.

1. Show that an arbitrary density matrix for a mized state qubit may be written as

$$\rho = \frac{I + r \cdot v}{2},$$

   where r is a real three-dimensional vector such that $||r|| \leq 1$. This vector is known as the *Bloch vector* for the state ρ.

2. What is the Bloch vector representaiton for the state $\rho = I/2$?

3. Show that a state ρ is pure if and only if $||r|| = 1$.

4. Show that for pure states the description of the Bloch vector we have given coincises with that in Section 1.2.

Exercise 2.73. Let ρ be a density operator. A *minimal ensemble* for ρ is an ensemble $\{p_i, |\psi_i\rangle\}$ containing a number of elements equal to the rank of ρ. Let $|\psi\rangle$ be any state in the support of ρ. Show that there is a minimal ensemble for ρ that contains $|\psi\rangle$, and moreover that in any such ensemble $|\psi\rangle$ must appear with probability

$$p_i = \frac{1}{\langle\psi_i| \rho^{-1} |\psi_i\rangle},$$

where ρ^{-1} is defined to be the inverse of ρ.