Quantum Computing

Korben Rusek

6-1-2018

1 Linear Algebra

1.3 The Pauli matrices

$$\sigma_0 = I$$

$$\sigma_1 = \sigma_x = X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

$$\sigma_2 = \sigma_y = Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$$

$$\sigma_3 = \sigma_z = Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

1.6 Adjoints and Hermitian operators

Definition 1.1 (Hermitian)**.** An operator A is Hermitian if $A = A^\dagger$.

Theorem 1.2. Two eigenvectors of a Hermitian operator with different eigenvalues are orthogonal.

Definition 1.3. A matrix is normal if $AA^\dagger = A^\dagger A$.

Theorem 1.4. A normal matrix is Hermitian iff it has real eigenvalues.

Definition 1.5 (Unitary)**.** A matrix U is unitary if $U^\dagger U = I$.

Definition 1.6 (Positive and Positive definite)**.** A positive operator A is defined to be an operator such that for any vector $\left|v\right\rangle$, $(\left|v\right\rangle, A\left|v\right\rangle)$ is a real, non-negative number. If $(\left|v\right\rangle, A\left|v\right\rangle) > 0$ then A is positive definite.

1.7 Tensor products

1.8 Operator functions

1.9 The commutator and anti-commutator

Definition 1.7 (Commutator)**.** The *commutator* between two operators A and B is defined to be

$$[A,B] = AB - BA.$$

If $[A,B]=0$ then we say that A commutes with B.

Definition 1.8 (Anti-commutator)**.** The *anti-commutator* between to operators A and B is defined to be

$$\{A,B\} = AB + BA.$$

If $\{A,B\}=0$ then we say that A anti-commutes with B.

Definition 1.9 (Simultaneously Diagonalizable)**.** Hermitian operators A and B are said to be *simultaneously diagonalizable* if there exist some orthonormal set of vectors $\langle i|$ such that $A = \sum a_i |i\rangle \langle i|$ and $B = \sum b_i |i\rangle \langle i|$.

Theorem 1.10 (Simultaneous diagonalization theorem)**.** Suppose A and B are Hermitian operators. Then $[A,B]=0$ iff A and B are simultaneously diagonalizable.

Here are some facts

$$[X,Y] = 2iZ; [Y,Z] = 2iX; [Z,X] = 2iY$$
$$[A,B]^\dagger = [B^\dagger, A^\dagger]$$

Theorem 1.11. Suppose A and B are Hermitian. Then $i[A,B]$ is also Hermitian.

1.10 The polar and singular value decompositions

Theorem 1.12 (Polar decompositions)**.** Let A be a linear operator on a vector space V. Then there exists unitary U and positive operators J and K such that

$$A = UJ = KU,$$

where the unique positive operators J and K satisfying these equations are $J = \sqrt{A^\dagger A}$ and $K = \sqrt{AA^\dagger}$. Moreover, if A is invertible then U is unique.

Theorem 1.13 (Singular value decomposition)**.** Let A be a square matrix. Then there exist unitary matrices U and V, and a diagonal matrix D with non-negative entries such that

$$A = UDV.$$

The diagonal elements of D are known as the *singular values* of A.

2 The postulates of quantum mechanics

2.1 State Space

Postulate 2.1. Associated to any isolated physical system is a complex vector space with inner product (that is, a Hilbert space) known as the *state space* of the system. The system is completely described by its *state vector*, which is a unit vector in the system's state space.

2.2 Evolution

Postulate 2.2. The evolution of a *closed* quantum system is described by a *unitary transformation.* That is, the state $|\phi\rangle$ of the system at time t_1 is related to the state $|\phi'\rangle$ of the system at time t_2 by a unitary operator U which depends only on the times t_1 and t_2,

$$|\phi'\rangle = U|\phi\rangle .$$

The X Pauli matrix is often referred to as the not gate or the *bit flip* gate. It will send $|0\rangle$ to $|1\rangle$ and $|1\rangle$ to $|0\rangle$.

The Z Pauli matrix is called the *phase flip* gate. It leaves $|0\rangle$ invariant but sends $|1\rangle$ to $-|1\rangle$.

Definition 2.1 (Hadamard Gate)**.** An interesting unitary operator is the *Hadamard gate.* This had the matrix representation

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

Postulate 2.2 (Revised)**.** The time evolution of the state of a closed quantum system is described by the *Schrödinger equation*,

$$i\hbar\frac{d|\phi\rangle}{dt} = H|\phi\rangle .$$

In this equation, $\hbar$ is a physical constant known as *Planck's constant* whose value must be experimentally determined. The exact value is not important to us. In practice, it is common to absorb the factor $\hbar$ into H, effectively setting $\hbar = 1$. H is a fixed Hermitian operator known as the *Hamiltonian* of the closed system.

2.3 Quantum measurement

We introduce Postulate 3 in order to describe the effects that measurement have on a system.

Postulate 2.3. Quantum measurements are described by a collection $\{M_m\}$ of *measurement operators.* These are operators acing on the state space of the system being measured. The index m refers to the measurement outcomes that may occur in the experiment. If the state of the quantum system is $|\phi\rangle$ immediately before the measurement then the probability that result m occurs is given by

$$p(m) = \langle\phi| M_m^\dagger M_m |\phi\rangle ,$$

and the state of the system after the measurement is

$$\frac{M_m|\phi\rangle}{\sqrt{\langle\phi| M_m^\dagger M_m |\phi\rangle}}.$$

The measurement operators satisfy the *completeness equation*,

$$\sum_m M_m^\dagger M_m = I.$$

The completeness equation expresses the fact that probabilities sum to one:

$$I = \sum p(m) = \sum \langle\phi| M_m^\dagger M_m |\phi\rangle .$$

We can use this understanding to illustrate measurement of a single qubit in the computational basis. We have two measurement operators, $M_0 = |0\rangle\langle 0|$ and $M_1 = |1\rangle\langle 1|$. Of course each is Hermitian as we have real eigenvalues on computational basis elements. We see that $M_0^\dagger M_0 = M_0^2 = M_0$ and similarly $M_1^\dagger M_1 = M_1^2 = M_1$. Thus the completeness relation is obeyed, $I = M_0^\dagger M_0 + M_1^\dagger M_1$. Then the probability of obtaining the measurement outcome 0 is

$$p(0) = \langle\psi| M_0^\dagger M_0 |\psi\rangle = \langle\psi| M_0 |\psi\rangle = |a|^2.$$

Similarly $p(1) = |b|^2$. The state after measurement is therefore

$$\begin{aligned} \frac{M_0|\psi\rangle}{|a|} &= \frac{a}{|a|}|0\rangle \\ \frac{M_1|\psi\rangle}{|b|} &= \frac{b}{|b|}|1\rangle . \end{aligned}$$

Later we will see that modulus one multipliers like $\frac{a}{|a|}$ can effectively be ignored so we can consider the post-measurement states as $|0\rangle$ and $|1\rangle$.

2.4 Distinguishing quantum states

2.5 Projective measurements

Definition 2.2 (Projective measurements)**.** A projectiv measurement is described by an *observable*, M, a Hermitian operator on the state space of the system being observed. The observable has a spectral decomposition,

$$M = \sum_m m P_m,$$

where P_m is the projector onto the eigenspace of M is eigenvalue m. The possible outcomes of the easurement correspond to the eigenvalues, m of the observable. Upon measuring the state $|\psi\rangle$, the probability of getting result m is given by

$$p(m) = \langle\psi| P_m |\psi\rangle .$$

Given that the outcome of m occursed, the state of the quantum system immediately after the measurement is

$$\frac{P_m|\psi\rangle}{\sqrt{p(m)}}.$$

Projective measurements can be viewed as a special case of Postulate 3. We have the added restriction that the measurement operators M_m are orthoganal projectors. That is M_m are Hermitian and $M_m M_{m'} = \delta_{m,m'} M_m$ and $\sum M_m^\dagger M_m = I$.

Projective measurements have many nice properties. For example, the average value of the measurment is

$$\begin{aligned} E(M) &= \sum_m m p(m) \\ &= \sum_m m \langle\psi| P_m |\psi\rangle \\ &= \langle\psi| \left(\sum_m m P_m\right) |\psi\rangle \\ &= \langle\psi| M |\psi\rangle . \end{aligned}$$

The average value of an observable M is often written $\langle M\rangle = \langle\psi| M |\psi\rangle$. This gives us a formula for standard deviation as

$$\begin{aligned} [\Delta(M)]^2 &= \langle (M - \langle M\rangle)^2\rangle \\ &= \langle M^2\rangle - \langle M\rangle^2 . \end{aligned}$$

Theorem 2.3 (Heisenberg uncertainty principle, Box 2.4, page 89)**.** Suppose C and D are two observables. Then we have the Heisenberg uncertainty principle,

$$\Delta(C)\Delta(D) \geq \frac{|\langle\psi| [C, D] |\psi\rangle|}{2}.$$

A very common misconception about the uncertainty principle is that measuring an observable C to some 'accuracy' $\Delta(C)$ causes the value of D to be 'disturbed' by an amount $\Delta(D)$ in such a way that some sort of inequality like the above inequality is satisified.

The correct interpretation is that if we prepare a large number of quantum systems in identical states, $|\psi\rangle$, and then perform measurements of C on some of those systems and of D on others, the the standard deviation $\Delta(C)$ of the C results times the standard deviation $\Delta(D)$ of the D results will satisfy the above inequality.

2.6 POVM measurements

Definition 2.4 (POVM elements)**.** Suppose a measurement is described by the measurement operators M_m. The probability of a measurement m is given by $p(m) = \langle\psi| M_m^\dagger M_m |\psi\rangle$. Then we define the elements $E_m = M_m^\dagger M_m$. From Postulate 3 and linear algebra we see that E_m are positive operators and $\sum_m E_m = I$ and $p(m) = \langle\psi| E_m |\psi\rangle$. This set of operators E_m is sufficient to determine the probabilities of different measurement outcomes. The individual operators E_m are known as the *POVM elements* associated with the measurement. The complete set $\{E_m\}$ is known as a *POVM*.

A simple example of a POVM is a projective measurement, where the elements are disjoint projections and $\sum P_m = I$. In this case, and only this case the POVM elements are the same as the measurement operators themselves.

We defined a POVM in terms of an preexisting set of measurement operators. A worthwhile observation follows. Suppose that $\{E_m\}$ is some arbitrary set of positive operators such that $\sum_m E_m = I$. Then there is a set of measurement operators M_m defining a measurement described by the POVM $\{E_m\}$. We can define $M_m = \sqrt{E_m}$. We see that $\sum_m M_m^\dagger M_m = \sum_m E_m = I$, and therefore the set $\{M_m\}$ describes a measurement with POVM $\{E_m\}$. For this reason the following definition of POVM is often used:

Definition 2.5 (POVM)**.** We define a *POVM* to be any set of operators $\{E_m\}$ such that

a each operator E_m is positive

b the completeness relation $\sum_m E_m = I$ is obeyed.

As in other places, the completeness relation expresses the fact that probabilities sum to one. We reiterate the fact that

$$p(m) = \langle\psi|\, E_m \,|\psi\rangle\,.$$

This gives rise to a worthwhile example regarding distinguising quantum states that are not orthognonal. Suppose Alice gives Bob a qubit prepared in either $|\psi_1\rangle = |0\rangle$ or $|\psi_2\rangle = |+\rangle$. Since these two states are not orthogonal it is not possible to distinguish them with without error. However it is possible to perform a measurement that sometimes is able to correctly identify the states, but never makes an error. (This is in some ways related to an BPP style algorithm.) Consider the POVM containing three elements:

$$\begin{aligned} E_1 &= \frac{\sqrt{2}}{1+\sqrt{2}}\,|1\rangle\,\langle 1| \\ E_2 &= \frac{\sqrt{2}}{1+\sqrt{2}}\,|-\rangle\,\langle -| \\ E_3 &= I - E_1 - E_2. \end{aligned}$$

It is straight forward to verify that the completeness relation is satisfied and that we have positive operators. On top of that we have

$$\begin{aligned} \langle\psi_1|\, E_1 \,|\psi_1\rangle &= \langle 0|\, E_1 \,|0\rangle = 0 \\ \langle\psi_1|\, E_2 \,|\psi_1\rangle &= \langle 0|\, E_2 \,|0\rangle > 0 \\ \langle\psi_2|\, E_1 \,|\psi_2\rangle &= \langle +|\, E_1 \,|+\rangle > 0 \\ \langle\psi_2|\, E_2 \,|\psi_2\rangle &= \langle +|\, E_2 \,|+\rangle = 0. \end{aligned}$$

Therefore, if Bob gets the measurement outcome E_1 we know he was given $\bar{+}$ whereas if Bob gets the outcome E_2 we know he was given $\bar{0}$. On the other had if Bob was given the outcome E_3 then we do not know what state he was given. Therefore though Bob cannot perfectly distinguish the two states, but he can do better than nothing.

We can also see problems C1 and C2 from the MS quantum computation for further examples.

2.7 Phase

2.8 Composite systems

Postulate 4 describes how to mathematicaly describe the composition of smaller systems.

Postulate 2.4. The state space of a composite physical system is the tensor product of the component physical systems. Moreover, if we have systems numbered 1 through n and system i is prepared in the state $|\psi_i\rangle$, then the joint state of the total system is $|\psi_1\rangle \otimes \cdots \otimes |\psi_n\rangle$.