Chapter 3 States, measurements and channels

Qubits

- Mathematically, qubit is a vector in $|x\rangle = a|0\rangle + b|1\rangle = \begin{pmatrix} a \\ b \end{pmatrix} \in \mathbf{C}^2$ with $|a|^2 + |b|^2$ realized by physical quantum states such as the vertically and horizontally polarized photons, or spin 1/2 in NMR system.
- Note that measurement will give $|0\rangle$ or $|1\rangle$ even a qubit can assume infinitely many states. The probability for the measurement on $|x\rangle$ yielding $|0\rangle$ is $\langle x|(|0\rangle\langle 0|)|x\rangle = |a|^2$.
- We cannot extract the information $|a|$ and $|b|$ by **making** many identical $|x\rangle$ and measure them because of the no cloning theorem.
- One may consider qutrits in $\mathbf{C}^3$ and qudits in $\mathbf{C}^n$.

Bloch sphere

Let $\sigma = (\sigma_x, \sigma_y, \sigma_z)$. If $|x\rangle = \cos(\theta/2)|0\rangle + e^{i\phi}\sin(\theta/2)|1\rangle = \begin{pmatrix} \cos(\theta/2) \\ e^{i\phi}\sin(\theta/2) \end{pmatrix}$, then

$$\begin{aligned} |x\rangle\langle x| &= \begin{pmatrix} \cos^2(\theta/2) & e^{-i\phi}\sin(\theta/2)\cos(\theta/2) \\ e^{i\phi}\sin(\theta/2)\cos(\theta/2) & \sin^2(\theta/2) \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 1+\cos\theta & e^{-i\phi}\sin\theta \\ e^{i\phi}\sin\theta & 1-\cos\theta \end{pmatrix} \\ &= \frac{1}{2}\begin{pmatrix} 1+\cos\theta & \cos\phi\sin\theta - i\sin\phi\sin\theta \\ \cos\phi\sin\theta + i\sin\phi\sin\theta & 1-\cos\theta \end{pmatrix} \\ &= \frac{1}{2}(\sigma_0 + \sin\theta\cos\phi\sigma_x + \sin\theta\sin\phi\sigma_y + \cos\theta\sigma_z). \end{aligned}$$

If

$$\hat{\mathbf{n}}(\theta,\phi) = (\sin\theta\cos\phi, \sin\theta\sin\phi, \cos\theta)^t,$$

then

$$\hat{\mathbf{n}}(\theta,\phi)\cdot\sigma|x\rangle = (2|x\rangle\langle x| - I_2)|x\rangle = |x\rangle.$$

So, every state vector $|x\rangle$ corresponds to a vector $\hat{\mathbf{n}}(\theta,\phi)$ on the surface of the unit sphere, called the Bloch sphere in this context.

Multi-qubit systems and entangled states

Given n qubits $|x_1\rangle, \ldots, |x_n\rangle$, we can consider the tensor product $|x_1\rangle \otimes \cdots \otimes |x_n\rangle \in \mathbf{C}^N$ with $N = 2^n$. Most state vectors

$$\sum_{i_k=0,1} a_{i_1 \cdots i_n} |x_{i_1}\rangle \otimes \cdots \otimes |x_{i_n}\rangle \in \mathbf{C}^N$$

are entangled state vectors, which are not of the tensor form.

Example The Bell states

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \quad |\Phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle),$$

$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle), \quad |\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

are entangled states and form an orthonormal basis for the two qubit systems.

Example In the 3 qubit system, we have that GHZ state and W state:

$$|GHZ\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle) \quad \text{and} \quad |W\rangle \frac{1}{\sqrt{3}}(|100\rangle + |010\rangle + |001\rangle).$$

Measurements

For each outcome m, construct a measurement operator M_m so that the probability of obtaining outcome m in the state $|x\rangle$ is computed by

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

and the state immediately after the measurement is

$$|m\rangle = \frac{M_m|x\rangle}{\sqrt{p(m)}}.$$

Example Let $M = \{M_0, M_1\}$ with $M_0 = |0\rangle\langle 0|$ and $M_1 = |1\rangle\langle 1|$. Then for $|x\rangle = a|0\rangle + b|1\rangle$ with $a \neq 0$, $p(0) = |a|^2$, $M_0|x\rangle = a|0\rangle/|a|$, which is the same as the vector state $|0\rangle$.

In general, suppose an observable M is given with measurement operators M_m. Then setting $P_i = M_i^\dagger M_i$, we require that $\sum_m P_m = I_n$.

If there are many copy of a state $|x\rangle$, then the expected value of M is

$$E(M) = \langle M \rangle = \sum_m mp(m) = \sum_m m\langle x|P_m|x\rangle = \langle x|M|x\rangle.$$

Here M can be identified with $\sum_m mP_m$.

The standard derivation is

$$\Delta(M) = \sqrt{\langle (M - \langle M\rangle)^2} = \sqrt{\langle M^2\rangle - \langle M\rangle^2}.$$

The variance (square of standard deviation) is

$$\langle (M - \langle M\rangle)^2\rangle = \langle x|M^2|x\rangle - \langle x|M|x\rangle^2.$$

Example One can do measurement of the first qubit for a state vector in a n qubit system. For instance,

$$|x\rangle = a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle, \quad |a|^2 + |b|^2 + |c|^2 + |d|^2 = 1.$$

We measure the first qubit with respect to the basis $\{|0\rangle, |1\rangle\}$. Set

$$|x\rangle = |0\rangle(a|0\rangle + b|1\rangle) + |1\rangle(c|0\rangle + d|1\rangle) = u|0\rangle((a/u)|0\rangle + (b/u)|1\rangle) + v|1\rangle((c/v)|0\rangle + (d/v)|1\rangle),$$

where $u = \sqrt{|a|^2 + |b|^2}$ and $v = \sqrt{|c|^2 + |d|^2}$. Now,

$$M_0 = |0\rangle\langle 0| \otimes I_2, \quad M_1 = |1\rangle\langle 1| \otimes I_2.$$

Applying M_0 and M_1, we obtain 0 with probability $\langle x|M_0|x\rangle = u^2$ and 1 with probability v^2; the state $|x\rangle$ collapses to $|0\rangle\otimes((a/u)|0\rangle+(b/u)|1\rangle)$ and $|1\rangle\otimes((c/v)|0\rangle+(d/v)|1\rangle)$, respectively, upon measurement.

Einstein-Podolsky-Rosen (EPR) Paradox

Consider the EPR state

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle).$$

Alice gets the first particle and Bob gets the second one. When Alice measures, Bob's particle will change instantaneously to $|01\rangle$ or $|10\rangle$ according to the measuring outcome of Alice.

Note that information is not sent. Alice cannot control her measurement and hence the reading of Bob! So, it does not violate the special theory of relativity. (It is impossible that information travels faster than light!)

3.2 Quantum Key Distribution (BB84 protocol)

Alice wants to send n bits to Bob securely. Eve is the notorious eavesdropper.

Alice and Bob will choose two randomly chosen systems:

(1) $0 \mapsto |e_1\rangle,\ \ 1 \mapsto |e_2\rangle$.

(2) $0 \mapsto (|e_1\rangle + |e_2\rangle)/\sqrt{2},\ \ 1 \mapsto (|e_1\rangle - |e_2\rangle)/\sqrt{2}$.

- Alice send $4n$ bits to Bob, each using the two systems randomly.
- Announce the types of systems; discard about $2n$ bits with wrong channel match.

  Probability for Alice and Bob use the same system: (1)(1), (2)(2), vs. (1)(2), (2)(1).
- Alice tells Bob n of two remaining bits to test whether they have not been tempered.

  Alice, Eve, Bob use channels

(1)(1)(1)	(1)(1)(2)	(1)(2)(1)	(1)(2)(2)	(2)(1)(1)	(2)(1)(2)	(2)(2)(1)	(2)(2)(2)
Y	N	Y	N	N	Y	N	Y
G	*	$\pm$ G	*	*	$\pm$ G	*	G

- If not, use the remaining n bits as the private key. Otherwise, repeat the process.