Imperial College London

NOTES

IMPERIAL COLLEGE LONDON

DEPARTMENT OF COMPUTING

Quantum Information

Author:
Chen Huang

Email:
chen.huang23@imperial.ac.uk

Date: October 23, 2023

Contents

1 Elements of Quantum Mechanics and Quantum Information

1.1 Tools I from Quantum Mechanics

1.1.1 States and Operators

The harmonic oscillator

$$\hat{H} = \hbar\omega \left(\hat{a}^\dagger \hat{a} + \frac{1}{2} \right) \tag{1}$$

where the unit of $\hbar = 1$ has been applied and the zero-point energy $\omega/2$ has been ignored. With the common relations

$$\hat{a} \left| n \right\rangle = \sqrt{n} \left| n-1 \right\rangle, \qquad \hat{a}^\dagger \left| n \right\rangle = \sqrt{n+1} \left| n+1 \right\rangle \tag{2}$$

one can evaluate everything with any knowledge of the wave functions $\psi(x)$ in real space or any other representation.

We can express the operator a as

$$\hat{a} = \sum_{m,n=0}^{\infty} \left| m \right\rangle \left\langle m \right| \hat{a} \left| n \right\rangle \left\langle n \right| = \sum_{n=0}^{\infty} \sqrt{n+1} \left| n \right\rangle \left\langle n \right| \tag{3}$$

Similarly, we can express any operator for any quantum mechanical system as

$$\hat{A} = \sum_{i,j} \left\langle i \right| \hat{A} \left| j \right\rangle \left| i \right\rangle \left\langle j \right| \tag{4}$$

For a two-dimensional system, *i.e.* a qubit, the corresponding space of operators is in 2×2 matrix, and a common basis is given by the identity $\mathbb{1}$ and the three Pauli matrices.

$$\hat{\sigma}_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \hat{\sigma}_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \hat{\sigma}_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad \mathbb{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \tag{5}$$

that implies the **commutator** and **anti-commutator** relation

$$[\hat{\sigma}_\alpha, \hat{\sigma}_\beta] = 2i\varepsilon_{\alpha\beta\gamma}\hat{\sigma}_\gamma, \qquad \{\hat{\sigma}_\alpha, \hat{\sigma}_\beta\} = 0 \tag{6}$$

1.1.2 Dynamics

The Schrödinger equation is written as $(\hbar = 1)$

$$i\frac{\mathrm{d}}{\mathrm{d}t} \left| \Psi(t) \right\rangle = \hat{H} \left| \Psi(t) \right\rangle \tag{7}$$

with a time-independent Hamiltonian, one obtains that

$$\left| \Psi(t) \right\rangle = \hat{U}(t, t_0) \left| \Psi(t_0) \right\rangle = \mathrm{e}^{-i\hat{H}(t-t_0)} \left| \Psi(t_0) \right\rangle \tag{8}$$

One may express this also in terms of the *time-evolution operator* or *propagator*

$$\hat{U}(t,t_0) = \mathrm{e}^{-i\hat{H}(t-t_0)} \tag{9}$$

which has several key properties:

- **The propagator $\hat{U}$ and $\hat{H}$ commute, and have the same eigenstates.** With the spectral decomposition $\hat{H} = \sum_j \omega_j |\Psi_j\rangle \langle\Psi_j|$, one obtains

$$\hat{U} = \hat{U} \sum_j |\Psi_j\rangle \langle\Psi_j| = \sum_j \mathrm{e}^{-i\omega_j(t-t_0)} |\Psi_j\rangle \langle\Psi_j| \tag{10}$$

- **The propagator is unitary**, *i.e.*

$$\hat{U}(t,t_0)\hat{U}^\dagger(t,t_0) = \hat{U}(t,t_0)^\dagger \hat{U}(t,t_0) = \mathbb{I} \tag{11}$$

  which guarantees conservation of norm of $|\Psi(t)\rangle$, and thus normalisation.

- **The propagator (as operator) satisfies the Schrödinger equation.** The basis states evolve as $|\Psi_j(t)\rangle = \hat{U}(t,t_0)|\Psi_j(t_0)\rangle$. That is, we can write the propagator as

$$\hat{U}(t,t_0) = \hat{U}(t,t_0) \sum_j |\Psi_j(t_0)\rangle \langle\Psi_j(t_0)| = \sum_j |\Psi_j(t)\rangle \langle\Psi_j(t_0)| \tag{12}$$

  We thus obtain

$$i\frac{\mathrm{d}}{\mathrm{d}t}\hat{U}(t,t_0) = \sum_j i\frac{\mathrm{d}}{\mathrm{d}t} |\Psi_j(t)\rangle \langle\Psi_j(t_0)| = \sum_j \hat{H} |\Psi_j(t)\rangle \langle\Psi_j(t_0)| = \hat{H}\hat{U}(t,t_0) \tag{13}$$

In quantum information, one often uses the term ‘quantum gate’ or simply ‘gate’ instead of propagator.

1.1.3 Measurement

Formally, a measurement is described in terms of projectors. Choose $\{|0\rangle, |1\rangle\}$ as the measurement basis, and the projectors are $\hat{P}_0 = |0\rangle\langle 0|$ and $\hat{P}_1 = |1\rangle\langle 1|$. The state reduction

$$\hat{P}_0 |\psi\rangle = \hat{P}_0(\alpha|0\rangle + \beta|1\rangle) = \alpha|0\rangle \tag{14}$$

$$\hat{P}_1 |\psi\rangle = \hat{P}_1(\alpha|0\rangle + \beta|1\rangle) = \beta|1\rangle \tag{15}$$

with probability

$$p_0 = \langle\psi|\hat{P}_0|\psi\rangle = |\alpha|^2, \quad p_1 = \langle\psi|\hat{P}_1|\psi\rangle = |\beta|^2 \tag{16}$$

The condition

$$\sum_i p_i = \langle\psi| \sum_i \hat{P}_i |\psi\rangle = 1 \tag{17}$$

must be required.

1.2 Quantum Key Distribution - BB84

Quantum Key Distribution (QKD) permits to share string of random numbers. One of the QKD protocol is *BB84*, which invented by Charles Bennett and Giles Brassard in 1984. Alice uses one qubit and prepares randomly one of the four states

$$|\mathrm{H}\rangle = |0\rangle\,, \quad |\mathrm{V}\rangle = |1\rangle\,, \quad |\mathrm{D}\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \quad |\mathrm{A}\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \tag{18}$$

1. **Sending**: Alice randomly selects a string of bits and a string of basis ($+$ or $\times$) of equal length.
$$+ \rightarrow \{|\mathrm{H}\rangle\,, |\mathrm{V}\rangle\}, \qquad \times \rightarrow \{|\mathrm{D}\rangle\,, |\mathrm{A}\rangle\}$$
Then she transmits a photon for each bit with the corresponding polarization to Bob.

2. **Receiving**: Bob randomly chooses a basis for each photon to measure its polarization. If Bob selects the same basis as Alice for a particular photon, he will correctly find the bit Alice wanted to share as he measured the same polarization. If he doesn't guess correctly, he will get a random bit.

3. **Compare**: Bob tells Alice the bases he used to measure each photon. Alice informs Bob of the bases he guessed correctly to measure the encoded bits. After that, Alice and Bob remove the encoded and measured bits on different bases. Now, Alice and Bob have an identical bit-string, the s**hifted key**.

Alice's random bits	1	0	0	1	1	0	1	0	0	1
Alice's encoding basis	$+$	$\times$	$\times$	$+$	$\times$	$+$	$+$	$+$	$+$	$+$
Photons Alice sends	V	D	D	V	A	H	V	H	H	V
Random measurement basis	$+$	$+$	$\times$	$+$	$+$	$\times$	$+$	$+$	$+$	$\times$
Bits as received by Bob	V	V	D	V	H	A	V	H	H	D
Reveal the sequence of their basis	✓		✓	✓			✓	✓	✓	
Shifted Key	1		0	1			1	0	0	

Table 1: BB84 protocol

1.3 No-Cloning Theorem

Let's assume we have a qubit in a given state $|\Psi\rangle$ (but we don't know the state) and a second qubit in the $|0\rangle$ state. We would like to find a gate such that

$$\hat{U}\,|\Psi\rangle\,|0\rangle = |\Psi\rangle\,|\Psi\rangle \tag{19}$$

for any state $|\Psi\rangle$, so we have

$$\hat{U}\,|0\rangle\,|0\rangle = |0\rangle\,|0\rangle \tag{20}$$

$$\hat{U}\,|1\rangle\,|0\rangle = |1\rangle\,|1\rangle \tag{21}$$

For a general state $|\Psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$, this implies that

$$\hat{U}\,(\alpha\,|0\rangle + \beta\,|1\rangle)\,|0\rangle = \alpha\,|0\rangle\,|0\rangle + \beta\,|1\rangle\,|1\rangle \tag{22}$$

whereas we would have wanted to obtain

$$(\alpha\,|0\rangle + \beta\,|1\rangle)\,(\alpha\,|0\rangle + \beta\,|1\rangle) = \alpha^2\,|0\rangle\,|0\rangle + \alpha\beta(|0\rangle\,|1\rangle + |1\rangle\,|0\rangle) + \beta^2\,|1\rangle\,|1\rangle \tag{23}$$

In the above example, the cloning process works if either α or β vanishes; that is, it works for the two orthogonal basis states for which it is defined.

1.4 Tools II from Quantum Mechanics

1.4.1 Bell's Inequality

Assume that Alice has two cards A_0, A_1 having their value either $+1$ or -1 and Bob has his cards B_0 and B_1 also having their values $+1$ or -1. If all the cards bear the value $+1$, i.e. $A_0 = A_1 = B_0 = B_1 = 1$, then

$$A_0B_0 + A_0B_1 + A_1B_0 - A_1B_1 = 2 \tag{24}$$

The average

$$\boxed{\langle A_0B_0\rangle + \langle A_0B_1\rangle + \langle A_1B_0\rangle - \langle A_1B_1\rangle \leq 2} \tag{25}$$

This is called *Bell's inequality* which is obtained for **classical** physics based on local realism.
However, we can prove that a quantum-mechanically correlated state can violate Bell's inequality. Let us assume the singlet state,

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \tag{26}$$

and the observables $\hat{A}_0 = \hat{\sigma}_z$, $\hat{A}_1 = \hat{\sigma}_x$, $\hat{B}_0 = -\frac{1}{\sqrt{2}}(\hat{\sigma}_x + \hat{\sigma}_z)$, $\hat{B}_1 = \frac{1}{\sqrt{2}}(\hat{\sigma}_x - \hat{\sigma}_z)$. Then we find that

$$\begin{aligned}\langle \hat{A}_0 \otimes \hat{B}_0\rangle &= \langle\psi|\,\hat{A}_0 \otimes \hat{B}_0\,|\psi\rangle \\ &= -\frac{1}{2\sqrt{2}}(\langle 01| - \langle 10|)\hat{\sigma}_z \otimes (\hat{\sigma}_x + \hat{\sigma}_z)(|01\rangle - |10\rangle) \\ &= -\frac{1}{2\sqrt{2}}(\langle 01| - \langle 10|)\,(|00\rangle - |01\rangle + |11\rangle + |10\rangle) = \frac{1}{\sqrt{2}}\end{aligned} \tag{27}$$

Similarly, we can find

$$\langle \hat{A}_0 \otimes \hat{B}_0\rangle = \langle \hat{A}_0 \otimes \hat{B}_1\rangle = \langle \hat{A}_1 \otimes \hat{B}_0\rangle = -\langle \hat{A}_1 \otimes \hat{B}_1\rangle = \frac{1}{\sqrt{2}} \tag{28}$$

and the Bell's expectation value is

$$\langle \hat{A}_0 \otimes \hat{B}_0\rangle + \langle \hat{A}_0 \otimes \hat{B}_1\rangle + \langle \hat{A}_1 \otimes \hat{B}_0\rangle - \langle \hat{A}_1 \otimes \hat{B}_1\rangle = 2\sqrt{2} \tag{29}$$

which clearly **violates** Bell's inequality.

1.4.2 Partial Trace

The trace of the operator $\hat{A}$ reads

$$\operatorname{tr} \hat{A} = \sum_i \langle i| \hat{A} |i\rangle \tag{30}$$

for any orthonormal basis $\{|i\rangle\}$. For an operator $\hat{A} \otimes \hat{B}$ (on $\mathcal{H}_a \otimes \mathcal{H}_b$) we can define the partial traces

$$\hat{A} \operatorname{tr}_b \hat{B} = \operatorname{tr}_b \left(\hat{A} \otimes \hat{B} \right) \tag{31}$$

$$\hat{B} \operatorname{tr}_a \hat{A} = \operatorname{tr}_a \left(\hat{A} \otimes \hat{B} \right) \tag{32}$$

The partial trace naturally appears in expressions of the form $\operatorname{tr}\left(\left(\hat{A} \otimes \mathbb{I} \right) \hat{C} \right)$, where $\hat{A}$ acts on $\mathcal{H}_a$, $\mathbb{I}$ acts on $\mathcal{H}_b$ and $\mathbb{C}$ acts on $\mathcal{H}_a \otimes \mathcal{H}_b$.

$$\begin{aligned}
\operatorname{tr}\left(\left(\hat{A} \otimes \mathbb{I} \right) \hat{C} \right) &= \sum_{ij} \langle i|_a \otimes \langle j|_b \left(\left(\hat{A} \otimes \mathbb{I} \right) \hat{C} \right) |i\rangle_a \otimes |j\rangle_b \\
&= \sum_{ij} \left(\langle i|_a \hat{A} \right) \otimes \langle j|_b \hat{C} \left(|i\rangle_a \otimes |j\rangle_b \right) \\
&= \sum_i \langle i|_a \hat{A} \left(\sum_j \langle j|_b \hat{C} |j\rangle_b \right) |i\rangle_a \\
&= \operatorname{tr}_a \left(\hat{A} \operatorname{tr}_b \hat{C} \right)
\end{aligned} \tag{33}$$