C7.4 Introduction to Quantum Information
HT2020 Problem Set 1 solutions

Jordi Mur-Petit*

January 2020

1.1. Pauli matrices

(a) Eigenvalues are ± 1 as the Pauli matrices square to $\mathbb{I}$ (the 2×2 identity matrix).

Eigenvectors: σ_x: $(|0\rangle \pm |1\rangle)/\sqrt{2}$
σ_y: $(|0\rangle \pm i\,|1\rangle)/\sqrt{2}$
σ_x: $|0\rangle\,, \ |1\rangle$

(b) Recalling that $\sigma_j^2 = \mathbb{I}$ and $\{\sigma_j, \sigma_l\} = 2\delta_{jl}\mathbb{I}$, we find

$$\frac{1}{\sqrt{2}}(X+Z)Z\frac{1}{\sqrt{2}}(X+Z) = \frac{1}{2}(XZX + XZ^2 + Z^2X + Z^3) = \frac{1}{2}(-Z + X + X + Z) = X$$
$$\frac{1}{\sqrt{2}}(X+Z)X\frac{1}{\sqrt{2}}(X+Z) = \frac{1}{2}(X^3 + X^2Z + ZX^2 + ZXZ) = \frac{1}{2}(X + Z + Z - X) = Z$$

(c) For any two Pauli matrices, $(\sigma_j|\sigma_l) = \frac{1}{2}\,\mathrm{tr}(\sigma_j\sigma_m) = \delta_{jm}$. Then,

$$(\sigma_k|A) = \frac{1}{2}\,\mathrm{tr}(\sigma_k A) = \frac{1}{2}\,\mathrm{tr}\left(\sum_{m=1}^{3}\sigma_k a_m \sigma_m\right) = \sum_{m=1}^{3} a_m \frac{1}{2}\,\mathrm{tr}\left(\sigma_k\sigma_m\right) = \sum_{m=1}^{3} a_m\delta_{km} = a_k\,.$$

For the adjoint $A^\dagger$ we have $A^\dagger = \sum_{m=1}^{3} a_m^* \sigma_m$. Hence, for an Hermitian A, it follows that $a_k^* = (\sigma_k|A^\dagger) \overset{A\text{ is Hermitian}}{=} (\sigma_k|A) = a_k$. Hence, a_k is real.

1.2. Mutually unbiased bases

Simple check using the eigenvectors of $\sigma_x, \sigma_y, \sigma_z$ determined in Q.1.1.(a). For instance, take as $\{e_j\}$ the eigenvectors of σ_x: $|\pm x\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$, and as $|f_j\rangle$ those of σ_z: $\{|0\rangle\,, |1\rangle\}$. Then:

$$\langle e_1|f_1\rangle = \frac{1}{\sqrt{2}}(\langle 0| + \langle 1|)\,|0\rangle = \frac{1}{\sqrt{2}} \qquad \langle e_1|f_2\rangle = \frac{1}{\sqrt{2}}(\langle 0| + \langle 1|)\,|1\rangle = \frac{1}{\sqrt{2}}$$
$$\langle e_2|f_1\rangle = \frac{1}{\sqrt{2}}(\langle 0| - \langle 1|)\,|0\rangle = \frac{1}{\sqrt{2}} \qquad \langle e_2|f_2\rangle = \frac{1}{\sqrt{2}}(\langle 0| - \langle 1|)\,|1\rangle = -\frac{1}{\sqrt{2}}$$

Hence, $|\langle e_j|f_k\rangle|^2 = 1/2$ as desired.

1.3. Values of σ_x and σ_y of a qubit

Alice prepares the qubit in one of the eigenstates of σ_x, hence she knows the outcome if Bob chooses to measure on σ_x. When she gets the qubit back, she measures it in the σ_y basis, which tells her Bob's outcome if he had chosen to measure σ_y.

*I would like to thank all current and previous Class Tutors and TAs of this paper their help in compiling these solutions, in particular Dr R Pisarczyk and Dr M Lubasch.

1.4. Tensor products of Pauli operators

(A) *Show that $X \otimes X$ and $Z \otimes Z$ commute.*

$$(X \otimes X)(Z \otimes Z) = (XZ) \otimes (XZ) = (-ZX) \otimes (-ZX) = (ZX) \otimes (ZX) = (Z \otimes Z)(X \otimes X)\,.$$

The common eigenstates are the Bell states:

$$\begin{aligned}
(X \otimes X)\frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle) &= \frac{1}{\sqrt{2}}(|11\rangle \pm |00\rangle) = (\pm 1)\frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle)\,;\\
(X \otimes X)\frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle) &= \frac{1}{\sqrt{2}}(|10\rangle \pm |01\rangle) = (\pm 1)\frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle)\,;\\
(Z \otimes Z)\frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle) &= \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle) = (+1)\frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle)\,;\\
(Z \otimes Z)\frac{1}{\sqrt{2}}(-|01\rangle \mp |10\rangle) &= \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle) = (-1)\frac{1}{\sqrt{2}}(-|01\rangle \mp |10\rangle)\,.
\end{aligned}$$

(B) *n-qubit Pauli operators.* We will use $U = \lambda P_1 \otimes \dots \otimes P_n$ throughout this section, with $\lambda = \pm 1$ and $P_j \in \{X, Y, Z, \mathbb{I}\}$ $(j = 1, \dots, n)$.

(a) Unitarity: $U^\dagger U = \mathbb{I}$:

$$\begin{aligned}
U^\dagger U &= (\lambda P_1 \otimes \dots \otimes P_n)^\dagger (\lambda P_1 \otimes \dots \otimes P_n)\\
&= |\lambda|^2 P_1^\dagger P_1 \otimes \dots P_n^\dagger P_n = (+1)\mathbb{I} \otimes \dots \otimes \mathbb{I} = \mathbb{I}_{2n}\,. \quad \blacksquare
\end{aligned}$$

Hermiticity: $U^\dagger = (\lambda P_1 \otimes \dots \otimes P_n)^\dagger = \lambda^*\, P_1^\dagger \otimes \dots \otimes P_n^\dagger = \lambda P_1 \otimes \dots \otimes P_n = U$, where we used that $\lambda^* = \lambda$ for $\lambda \in \{\pm 1\}$ and that $P_j^\dagger = P_j$ for all $P_j \in \{X, Y, Z, \mathbb{I}\}$. $\blacksquare$

(b) "All pairs of n-qubit Pauli operators either commute or anticommute":
Take two elements P, Q of the set $\{X, Y, Z, \mathbb{I}\}$. Then one of two things will happen:

* If $P = Q$ or one of them is the identity, then $PQ = QP$ (they commute).
* Otherwise, it must be that P and Q are two different Pauli matrices, in which case $PQ = -QP$ (they anticommute).

We can thus generally write $PQ = \eta QP$, with $\eta = \pm 1$ depending on whether P, Q commute $(+1)$ or anticommute (-1).
Now take $U_P = \lambda_P P_1 \otimes \dots \otimes P_n$ and $U_Q = \lambda_Q Q_1 \otimes \dots \otimes Q_n$ with $\lambda_{P,Q} \in \{\pm 1\}$ and $P_j, Q_j \in \{X, Y, Z, \mathbb{I}\}$ $(j = 1, \dots, n)$. Then, introducing $\eta_j = \pm 1$ through $P_j Q_j = \eta_j Q_j P_j$,

$$U_P U_Q = \lambda_P \lambda_Q\, P_1 Q_1 \otimes \dots \otimes P_n Q_n = \lambda_Q \lambda_P\, \eta_1 Q_1 P_1 \otimes \dots \otimes \eta_n Q_n P_n = \left(\prod_{j=1}^{n} \eta_j\right) U_Q U_P\,.$$

It follows that $U_P U_Q = \pm U_Q U_P$, i.e., U_P and U_Q either commute or anticommute. $\blacksquare$
Whether U_P and U_Q commute or anticommute is determined by how many of the η_j equal -1: if there is an *odd* number of anticommuting pairs (P_j, Q_j), then $\prod_{j=1}^{n} \eta_j = -1$ and U_P and U_Q anticommute; otherwise they commute.

(d) Self-inverse, i.e., involution operators: $U^2 = \mathbb{I}$:
Given that P_j^2 for $P_j \in \{X, Y, Z, \mathbb{I}\}$ and $\lambda = \pm 1$,

$$U^2 = \lambda^2\, P_1^2 \otimes \dots \otimes P_n^2 = (+1)\, \mathbb{I} \otimes \dots \otimes \mathbb{I} = \mathbb{I}_{2n}\,. \quad \blacksquare$$

(c) Eigenvalues: It follows immediately from (d) that the eigenvalues must be ± 1. This can also be seen from the fact that the eigenvalues of any P_j are ± 1, hence the eigenvalue of a tensor product of P_j will be the product of eigenvalues, which will equal ± 1.

(e) *Do the given 10-qubit Pauli operators commute or anticommute?* Building on part (b), we have three $\eta_j = -1$ $(j = 2, 7, 10)$: they must anticommute.

1.5. Two-qubit operations

Note:

- If not explicitly given, a matrix element is zero.
- Recall the standard notation $|0\rangle = \begin{pmatrix}1\\0\end{pmatrix}$, $|1\rangle = \begin{pmatrix}0\\1\end{pmatrix}$.

$$\mathbb{I} \otimes H = \begin{pmatrix}1 & 0\\0 & 1\end{pmatrix} \otimes \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\1 & -1\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1 & & \\ 1 & -1 & & \\ & & 1 & 1\\ & & 1 & -1\end{pmatrix};$$

$$H \otimes \mathbb{I} = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\1 & -1\end{pmatrix} \otimes \begin{pmatrix}1 & 0\\0 & 1\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 0 & 1 & 0\\ 0 & 1 & 0 & 1\\ 1 & 0 & -1 & 0\\ 0 & 1 & 0 & -1\end{pmatrix};$$

$$H \otimes H = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\1 & -1\end{pmatrix} \otimes \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\1 & -1\end{pmatrix} = \frac{1}{2}\begin{pmatrix}1 & 1 & 1 & 1\\ 1 & -1 & 1 & -1\\ 1 & 1 & -1 & -1\\ 1 & -1 & -1 & 1\end{pmatrix};$$

$$P(\alpha) \otimes P(\beta) = \begin{pmatrix}1 & 0\\0 & e^{i\alpha}\end{pmatrix} \otimes \begin{pmatrix}1 & 0\\0 & e^{i\beta}\end{pmatrix} = \begin{pmatrix}1 & & & \\ & e^{i\beta} & & \\ & & e^{i\alpha} & \\ & & & e^{i\alpha+i\beta}\end{pmatrix};$$

$$S = \begin{pmatrix}1 & 0 \quad 0 & 0\\ 0 & \multirow{2}{*}{$\sqrt{NOT}$} & 0\\ 0 & & 0\\ 0 & 0 \quad 0 & 1\end{pmatrix} = \begin{pmatrix}1 & & & \\ & \frac{1+i}{2} & \frac{1-i}{2} & \\ & \frac{1-i}{2} & \frac{1+i}{2} & \\ & & & 1\end{pmatrix};$$

$$CNOT = \begin{pmatrix}1 & 0 & & \\ 0 & 1 & & \\ & & 0 & 1\\ & & 1 & 0\end{pmatrix}.$$

1.6. Hamiltonian for two independent systems

Let us denote for generality N_j the dimension of the Hilbert space of subsystem $\mathcal{S}_j$ $(j = 1, 2)$. As the two subsystems are independent, the evolution of the composite system follows from the tensor product of the two evolution operators:

$$\begin{aligned}\mathcal{U}_1 \otimes \mathcal{U}_2 &= (\mathbb{I}_{N_1} - iH_1 dt) \otimes (\mathbb{I}_{N_2} - iH_2 dt)\\ &= \mathbb{I}_{N_1} \otimes \mathbb{I}_{N_2} - i\,(H_1 \otimes \mathbb{I}_{N_2})\,dt - i\,(\mathbb{I}_{N_1} \otimes H_2)\,dt + O(dt^2)\\ &= \mathbb{I}_{N_1+N_2} - i\,(H_1 \otimes \mathbb{I}_{N_2} + \mathbb{I}_{N_1} \otimes H_2)\,dt + O(dt^2)\\ &\equiv \mathcal{U}_{\text{tot}} \stackrel{!}{=} \mathbb{I}_{N_1+N_2} - iH_{\text{tot}}dt\end{aligned}$$

Hence, the overall Hamiltonian —i.e., the generator of the evolution of the composite system— is $H_{\text{tot}} \equiv H_1 \otimes \mathbb{I}_{N_2} + \mathbb{I}_{N_1} \otimes H_2$.

1.7. Basic entanglement

We start by decomposing $|\psi\rangle$ by pulling out the first qubit:

$$|\psi\rangle = a\,|00\rangle + b\,|01\rangle + c\,|10\rangle + d\,|11\rangle = |0\rangle\,(a\,|0\rangle + b\,|1\rangle) + |1\rangle\,(c\,|0\rangle + d\,|1\rangle)$$

The state ψ will be separable when the state of the second qubit on the two brackets is the same, i.e., if and only if $(a\,|0\rangle + b\,|1\rangle) \propto (c\,|0\rangle + d\,|1\rangle)$. This condition is equivalent to

$$\frac{a}{b} = \frac{c}{d} \Rightarrow ad - bc = 0 \quad \blacksquare$$

For the particular case that $|\psi\rangle = \frac{1}{2}\left(|00\rangle + |01\rangle + |10\rangle + (-1)^k\,|11\rangle\right)$, we have $a = b = c = 1/2$, $d = (-1)^k/2$, hence

$$ad - bc = \frac{1}{4}\left((-1)^k - 1\right) = \begin{cases} 0, & k = 0 \;\Rightarrow\; \text{separable} \\ -1/2, & k = 1 \;\Rightarrow\; \text{entangled} \end{cases}$$

The separable state is ($k = 0$):

$$|\psi\rangle = \frac{1}{2}\left(|00\rangle + |01\rangle + |10\rangle + |11\rangle\right) = \frac{1}{2}\left[|0\rangle\left(|0\rangle + |1\rangle\right) + |1\rangle\left(|0\rangle + |1\rangle\right)\right] \equiv \frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + |1\rangle}{\sqrt{2}}\,.$$

1.8. Partial measurement

We factor out the first qubit to get:

$$|\psi\rangle = |0\rangle\left[\frac{i}{2}\,|00\rangle + \frac{12+5i}{26}\,|01\rangle\right] + |1\rangle\left[-\frac{1}{2}\,|01\rangle + \frac{3}{10}\,|10\rangle - \frac{2i}{5}\,|11\rangle\right] \equiv |0\rangle\,|u_0\rangle + |1\rangle\,|u_1\rangle\,.$$

The probability of seeing outcome 1 upon measuring the first qubit equals $\langle u_1|u_1\rangle = \frac{1}{4} + \frac{9}{100} + \frac{4}{25} = \frac{1}{2}$. In that case, the state of the 3-qubit system after the measurement is $|1\rangle\,(\sqrt{2}\,|u_1\rangle) = |1\rangle\left[-\frac{1}{\sqrt{2}}\,|01\rangle + \frac{3\sqrt{2}}{10}\,|10\rangle - \frac{2\sqrt{2}i}{5}\,|11\rangle\right]$. This follows from the measurement postulate of quantum mechanics, and from the requirement that the state vector be normalized.

1.9. Quantum bomb tester

(1) (i) As shown in the lecture notes, the beam splitter transition matrix is

$$B = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix}\,,$$

and for the interferometer we get

$$B^2 = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}\,.$$

If there is no bomb in the Mach-Zehnder interferometer and you input a photon in the $|0\rangle$ arm, then it comes out, definitely, in the $|1\rangle$ arm. Physically the photon can travel from the $|0\rangle$ input to the $|1\rangle$ output via two equivalent paths (two transmissions and one mirror reflection), and hence the corresponding amplitudes interfere constructively. On the other hand, the pathways leading to detector D0 differ by a phase shift of π, and hence they interfere destructively.

(ii) If there is a bomb in one of the arms of the interferometer, then this acts like a measuring device, causing us to know which arm the photon has travelled through. With 50% probability the bomb will explode. The rest of the time, the photon impinges on the second beam splitter and is detected in either detector with 50% probability. The probability to detect the photon at D0 (D1) is thus given by 1/4.

(iii) If we get a photon in the $|0\rangle$ arm, we know for certain that

- the bomb did not explode since we detect the photon;

* the bomb must be in the room because otherwise the photon would have come out in the $|1\rangle$ arm.

Observing a photon at D0 thus allows us to detect the bomb without exploding it!

Now let us construct the following iterative scheme. After we send the input photon in arm $|0\rangle$, there are three possible outcomes:

* The bomb explodes and the scheme terminates.
* The photon is detected at D0 and the scheme terminates with success.
* The photon is detected at D1.

If D1 clicks, we can repeat the procedure. If there is a bomb in the room, we will get a conclusive result eventually — either the bomb explodes or we detect the photon at D0. The probability to get a photon count at D0 at iteration k is $(1/4)^k$, and hence the probability for detecting the bomb without exploding it is

$$\sum_{r=1}^{k} \frac{1}{4^k} = \frac{1/4}{1-1/4}\left(1-\frac{1}{4^k}\right) = \frac{1}{3}\left(1-\frac{1}{4^k}\right) \xrightarrow{k\to\infty} \frac{1}{3}$$

On average, two out of three bombs will explode and one will be detected successfully.

If the room is empty, we always detect the photon at D1 and the scheme does not terminate. The probability for the detection of k successive photons at D1 in the presence of a bomb is $(1/4)^k$. For sufficiently large k we can thus conclude that it is highly unlikely to have a bomb in the room and terminate the iteration.

(2) The unitaries describing the beam splitters as specified in the question read

$$BS1 = \begin{pmatrix} \sqrt{1-r} & i\sqrt{r} \\ i\sqrt{r} & \sqrt{1-r} \end{pmatrix}, \qquad BS2 = \begin{pmatrix} \sqrt{r} & i\sqrt{1-r} \\ i\sqrt{1-r} & \sqrt{r} \end{pmatrix}.$$

The corresponding transfer matrix of the interferometer reads

$$BS2\, BS1 = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

We can thus apply the same logic of our iterative scheme developed in (1), but now with changed probabilities. Let us assume that there is a bomb in the lower arm of the interferometer. The probability to trigger the bomb in each run is $t = 1-r$. The probability to get a photon at D1 is $P_{D1} = (1-r)^2$, and the probability for a photon count at D0 is $P_{D0} = r(1-r)$.

At iteration k, the probability to get a photon at D0 is $P_{D0}(P_{D1})^{k-1}$. This is the probability for allowing us to detect the bomb without blowing it up in iteration k. Summing over all k gives

$$\sum_{k=1}^{\infty} P_{D0}(P_{D1})^{k-1} = P_{D0}\sum_{n=0}^{\infty}(P_{D1})^n = \frac{r(1-r)}{1-r^2} = \frac{r}{1+r} \overset{r\to 1}{\approx} \frac{1}{2}$$

(3) For a beam splitter with transmission probability t the unitary becomes

$$B = \begin{pmatrix} \sqrt{t} & i\sqrt{1-t} \\ i\sqrt{1-t} & \sqrt{t} \end{pmatrix}.$$

Now set $t = \cos^2[\frac{\pi}{2}(1-1/N)]$. We can see that B is a rotation matrix by an angle $\theta = \frac{\pi}{2}(1-1/N)$,

$$B = \exp\left[i\sigma_x\theta\right] = \begin{pmatrix} \cos\theta & i\sin\theta \\ i\sin\theta & \cos\theta \end{pmatrix}.$$

After N iterations, we have

$$B^N = \exp\left[i\sigma_x N\theta\right] = \begin{pmatrix} \cos[\frac{\pi}{2}(N-1)] & i\sin[\frac{\pi}{2}(N-1)] \\ i\sin[\frac{\pi}{2}(N-1)] & \cos[\frac{\pi}{2}(N-1)] \end{pmatrix} .$$

Taking N to be even, we get

$$B^N = -i(-1)^{N/2} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} .$$

This means that if we put N beam splitters together, putting a $|0\rangle$ at the input will return a $|1\rangle$. We have to be careful and go through and check what that means for the output beams (consistently labelling $|0\rangle$ on the output when $|0\rangle$ is input). If one follows it through for an even number of beam splitters, the $|1\rangle$ output is horizontal.

If we keep the same arrangement of beam splitters, but make one arm (say the lower arm) of each section pass through a room with a bomb in it, the probability that we get the output in the vertical arm (the $|0\rangle$ answer) at the end and that the bomb does not explode is simply given by the probability that every mirror reflects:

$$\cos^{2N}\left[\frac{\pi}{2N}\right] .$$

This can clearly be made arbitrarily close to 1 just by making N large. Hence we have a way of distinguishing the two possibilities perfectly without causing the bomb to explode!

Note: *The original idea for the quantum bomb tester goes back to A. C. Elitzur and L. Vaidman, "Quantum Mechanical Interaction-Free Measurements", Found. Phys.* ***23****, 987 (1993) [doi: 10.1007/BF00736012]. The solution in part (3) utilizing the quantum Zeno effect is based on P. Kwiat, H. Weinfurter, T. Herzog, A. Zeilinger, and M. A. Kasevich, "Interaction-Free Measurement", Phys. Rev. Lett.* ***74****, 4763 (1995).*