INTRODUCTION TO QUANTUM INFORMATION SCIENCE

Problem Sheet 1
Hilary Term

ARTUR EKERT & ZHENYU CAI

Questions Label: A - Bookwork B - Standard C - Challenging/Optional

1.1.A **Omnipresent Wolfgang Pauli and his ubiquitous matrices.** The three Pauli matrices $\sigma_1 \equiv \sigma_x \equiv X$, $\sigma_2 \equiv \sigma_y \equiv Y$, and $\sigma_3 \equiv \sigma_z \equiv Z$, here supplemented by the identity matrix $\sigma_0 \equiv \mathbb{1}$, are written in the standard basis $\{|0\rangle, |1\rangle\}$ as

$$\mathbb{1} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \qquad X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \qquad Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \qquad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

BIT FLIP PHASE FLIP

The Pauli matrices are unitary as well as Hermitian. They square to the identity

$$X^2 = Y^2 = Z^2 = \mathbb{1}.$$

They anticommute

$$XY + YX = 0,$$
$$XZ + ZX = 0,$$
$$YZ + ZY = 0,$$

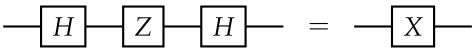
and satisfy

$$XY = iZ,$$
$$YZ = iX,$$
$$ZX = iY.$$

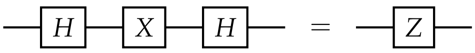
Their trace is zero and their determinant is -1.

(1) Find eigenvalues and eigenvectors of the three Pauli matrices.

(2) The two Pauli gates, X and Z, are often referred to as the bit flip and the phase flip respectively; we will use this terminology later on, when we discuss quantum error correction. Show that the Hadamard gate $H = \frac{1}{\sqrt{2}}(X + Z)$ turns phase flips into bit flips, $HZH = X$,



and bit flips into phase flips $HXH = Z$,



(3) Given that any 2×2 complex matrix A can be written in the basis of the identity plus the three Pauli matrices as:

$$A = a_0\mathbb{1} + \vec{a} \cdot \vec{\sigma} \equiv a_0\mathbb{1} + a_x\sigma_x + a_y\sigma_y + a_z\sigma_z,$$

show that the coefficients a_k are given by the inner products $a_k = (\sigma_k|A) = \frac{1}{2}\operatorname{Tr}\sigma_k A$. If A is Hermitian then these coefficients are real numbers. Why?

The set of complex $N \times N$ matrices form a Hilbert space with the inner product $(A|B) = \frac{1}{N}\operatorname{Tr} A^\dagger B$. This inner product is often called the *Hilbert-Schmidt product*.

Here vector $\vec{a}$ has components a_x, a_y, a_z and $\vec{\sigma} = (\sigma_x, \sigma_y, \sigma_z)$.

Solution:

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

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

(2) Recalling that $\sigma_j^2 = \mathbb{1}$ and $\{\sigma_j, \sigma_l\} = 2\delta_{jl}\mathbb{1}$, we find

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

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

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

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.A **Pauli group.** The three Pauli matrices and the identity form a group under multiplication for when we multiply two Pauli matrices we get another Pauli matrix... well, almost. Explain why the full one-qubit Pauli group $\mathcal{P}_1$ has 16 elements:

$$\pm\mathbb{1}, \pm X, \pm Y, \pm Z, \pm i\mathbb{1}, \pm iX, \pm iY, \pm iZ.$$

Show that $\langle i\mathbb{1}, X, Z\rangle$ is a generating set of this group.

Solution: Can be easily verified using

$$XY = -YX = iZ$$
$$YZ = -ZY = iX$$
$$ZX = -XZ = iY.$$

How does $\langle i\mathbb{1}, X, Z\rangle$ generates the full single-qubit Pauli group? If we multiply X and Z, we will get Y modulo phase. Now taking $i\mathbb{1}$ to different powers will give us all the phase factors $\pm i\mathbb{1}$ and $\pm\mathbb{1}$ to be added in front of the X, Y, Z, which give us the full group.

1.3.A **Get stabilized.** We say that a unitary S stabilizes $|\psi\rangle$ if $S|\psi\rangle = |\psi\rangle$.

We will use stabilizers to define vectors and vectors subspaces. Right now it may look like an unnecessary complication, but bear with us...

(1) Show that the set of stabilizers of $|\psi\rangle$ forms a group (known as the stabiliser group).

(2) Which states are stabilized by the Pauli matrices X, Y, Z and which by $-X$, $-Y$ and $-Z$? Which states are stabilized by the identity $\mathbb{1}$ and which by $-\mathbb{1}$?

(3) What are the stabilizer groups of the computational basis states, $|0\rangle$ and $|1\rangle$?

Solution:

(1) Denoting the set of elements that stabilise the state $|\psi\rangle$ as $\mathbb{S}$:

$$\mathbb{S} = \{S \in \mathbb{U} \quad | \quad S|\psi\rangle = |\psi\rangle\}$$

where $\mathbb{U}$ is the unitary group. To show that $\mathbb{S}$ forms a group under matrix multiplication, we look at the following.

- Associativity: Matrix multiplication is associative.
- Identity: We have $\mathbb{1}|\psi\rangle = |\psi\rangle$. Hence, $\mathbb{1} \in \mathbb{S}$.
- Inverse: For all $S \in \mathbb{S}$, we have $S^{-1}|\psi\rangle = S^{-1}S|\psi\rangle = |\psi\rangle$. Hence, $S \in \mathbb{S} \Rightarrow S^{-1} \in \mathbb{S}$.

- Closure: For all $S, S' \in \mathbb{S}$, we have $SS' |\psi\rangle = S |\psi\rangle = |\psi\rangle$. Hence, $S, S' \in \mathbb{S} \Rightarrow SS' \in \mathbb{S}$.

(2) Using the notations in Q1.1(1), the stabilised states of different operators are:

$$X: \ |+\rangle, \ -X: \ |-\rangle$$
$$Y: \ |+i\rangle, \ -Y: \ |-i\rangle$$
$$Z: \ |0\rangle, \ -Z: \ |1\rangle$$
$$\mathbb{1}: \ \text{all states}, \ -\mathbb{1}: \text{no states}$$

(3) The stabilizer groups of the computational basis states, if restricting only to Pauli operators, are:

$$|0\rangle: \ \{\mathbb{1}, Z\} \qquad |1\rangle: \ \{\mathbb{1}, -Z\}.$$

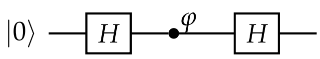
More generally if we allow for any unitary operators, we have:

$$|0\rangle: \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix} \qquad |1\rangle: \begin{pmatrix} e^{i\theta} & 0 \\ 0 & 1 \end{pmatrix}.$$

for any angle θ.

1.4.A **The golden circuit.** Here is a single qubit interference represented by the Hadamard – phase shift – Hadamard circuit. What is the role of the first Hadamard gate, the phase shift gate and the second Hadamard gate?

This exercise is important. It really is. Honestly, if you do not understand this circuit you will not get much out of this course.



Step through the execution of this circuit and write down the state of the qubit at each stage of the computation. Comment on a special case of $\varphi = \pi$.

Solution: See Sec. 2.4 of the online book.

1.5.B **Just Hadamard and Phase.** You are given an unlimited supply of the Hadamard and the phase gates

$$\mathrm{H} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \quad \mathrm{S} = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}.$$

How would you implement $S^\dagger$ and the three Pauli gates?

Solution: Similar to how H gates enable the transformation between X and Z:

$$HXH = Z, \qquad HZH = X,$$

S gates enable the transformation between X and Y:

$$SXS^\dagger = Y, \qquad S^\dagger YS = X.$$

We can compile $S^\dagger$ and Z simply using S:

$$S^\dagger = S^3, \qquad Z = S^2$$

Then we can transform Z into X and Y using H and S:

$$X = HZH = HS^2H, \qquad Y = SXS^\dagger = SHS^2HS^3.$$

Note that there are also other ways for compilation that is correct up to the global phases, e.g.

$$Y = iXZ = iHS^2HS^2.$$

1.6.B **You know Wolfgang Pauli, now meet William Clifford.** Clifford group on a single qubit, Cl_1, is the group of unitaries generated by the Hadamard and S gates: $Cl_1 = \langle \mathrm{H}, \mathrm{S} \rangle$.

Clifford normalizes Pauli. If this makes no sense to you, please look up centralizers and normalizers.

(1) Show that, under conjugation, Clifford gates $\mathrm{C} \in Cl_1$ map Pauli operators to Pauli operators: $CPC^\dagger = P'$ (modulo phase factors), where P and P' are two Pauli operators. In other words, the Clifford group is defined as the group of unitaries that normalize the Pauli group.

(2) Explain why any circuit composed only of the single qubit Clifford gates maps the set of Pauli eigenstates to the set of Pauli eigenstates.

Solution:

(1) Using the results in Question 1.5, adding onto the fact that $HYH = -Y$ and $SZS^\dagger = Z$, we can see that conjugation using H and S will simply transform one Pauli operator into another Pauli operator modulo phase.

Since H and S are the generators of the Clifford group, any Clifford operators can be written as a product of H and S. Hence, conjugating a Pauli operator using a Clifford operator can be viewed as multiple rounds of conjugations using H and S, which will only map one Pauli operator into another Pauli at every round and end up with a Pauli operator at the end (modulo phase).

(2) Given a state $|\psi\rangle$ is the ± 1-eigenstate of the Pauli operator P, we have

$$P |\psi\rangle = \pm |\psi\rangle . \tag{1}$$

Given a Clifford gate C that will transform the Pauli operator P into another Pauli operator P', we have:

$$CPC^\dagger = P' \quad \Rightarrow \quad CP = P'C.$$

Applying C to Eq. (1), we have

$$CP|\psi\rangle = \pm C|\psi\rangle$$
$$P'C|\psi\rangle = \pm C|\psi\rangle$$

i.e. $C|\psi\rangle$ is the eigenstate of the Pauli operator P'.

1.7.B **Tensor products of Pauli operators.** A 2-qubit Pauli operator is a tensor product of any two Pauli operators $(\mathbb{1}, X, Y, Z)$ with pre-factor $+1$ or -1. Using the properties of single-qubit Pauli-operator in **Question 1.1** show that all 2-qubit Pauli operators have the following properties

Given some operators U_i, V_i and some scalars λ_i, we know the following properties of the tensor products of operators:
$(U_1 \otimes U_2)^\dagger = U_1^\dagger \otimes U_2^\dagger$
$\lambda_1 U_1 \otimes \lambda_2 U_2 = (\lambda_1 \lambda_2)(U_1 \otimes U_2)$
$(U_1 \otimes U_2)(V_1 \otimes V_2) = U_1 V_1 \otimes U_2 V_2$

(1) They are both unitary and Hermitian.

(2) They are self-inverse and have eigenvalues ± 1.

(3) Any two operators either commute or anticommute.

Similar arguments can be extended to n-qubit Pauli operator. Now consider the following two 10-qubit Pauli operators

$$X \otimes X \otimes \mathbb{1} \otimes Z \otimes \mathbb{1} \otimes Y \otimes Z \otimes \mathbb{1} \otimes Z \otimes Z$$
$$X \otimes Y \otimes X \otimes \mathbb{1} \otimes \mathbb{1} \otimes Y \otimes X \otimes \mathbb{1} \otimes Z \otimes X$$

(4) Do they commute or anticommute? There is a simple rule that allows to answer this question immediately, without any algebra. Can you see it?

Solution: We will use $U = \lambda P_1 \otimes P_2$ throughout this section, with $\lambda = \pm 1$ and $P_1, P_2 \in \{\mathbb{1}, X, Y, Z\}$.

(1) Remember that we have seen in Question 1.1 that all single-qubit Pauli operators are unitary $P^\dagger P = \mathbb{1}$ and Hermitian $P^\dagger = P$. Using this and the fact that $\lambda = \pm 1$, we can now looking at two-qubit Pauli operators on the following properties:

Unitarity:

$$U^\dagger U = (\lambda P_1 \otimes P_2)^\dagger (\lambda P_1 \otimes P_2) = |\lambda|^2 \left(P_1^\dagger P_1\right) \otimes \left(P_2^\dagger P_2\right) = \mathbb{1} \otimes \mathbb{1}$$

Hermiticity:

$$U^\dagger = (\lambda P_1 \otimes P_2)^\dagger = \lambda^* P_1^\dagger \otimes P_2^\dagger = \lambda P_1 \otimes P_2 = U.$$

(2) Self-inverse, i.e., involution operators: $U^2 = \mathbb{1}$, follows directly from unitarity and Hermiticity.

Eigenvalues: follows immediately from self-inverse that the eigenvalues must be ± 1.

(3) Take two elements P, Q of the set $\{\mathbb{1}, X, Y, Z\}$. Then one of two things will happen:

- If $P = Q$ or one of them is the identity $\mathbb{1}$, 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 two different 2-qubit Pauli operators $U_P = \lambda_P P_1 \otimes P_2$ and $U_Q = \lambda_Q Q_1 \otimes Q_2$ and study their commutation relationship, we have:

$$\begin{aligned} U_P U_Q &= \lambda_P \lambda_Q (P_1 Q_1) \otimes (P_2 Q_2) = \lambda_Q \lambda_P (\eta_1 Q_1 P_1) \otimes (\eta_2 Q_2 P_2) \\ &= \eta_1 \eta_2 \lambda_Q \lambda_P (Q_1 P_1) \otimes (Q_2 P_2) = \eta_1 \eta_2 U_Q U_P. \end{aligned}$$

It follows that $U_P U_Q = \pm U_Q U_P$, i.e. U_P and U_Q either commute or anticommute.

Whether U_P and U_Q commute or anticommute is determined by how many η_j equal -1:

- Odd number of η_j equal to -1, i.e. an *odd* number of anticommuting pairs $(P_j, Q_j) \quad \Rightarrow \quad \eta_1 \eta_2 = -1 \quad \Rightarrow \quad U_P$ and U_Q anticommute.
- Otherwise, U_P and U_Q commute

Similar arguments can be applied to n-qubit Pauli operators as suggested in the question with $\eta_1 \eta_2$ replaced by $\prod_j \eta_j$.

(4) *Do the given 10-qubit Pauli operators commute or anticommute?* Building on the last question, we have three $\eta_j = -1$ $(j = 2, 7, 10)$, i.e. an *odd* number of single-qubit Pauli pairs anti-commute, hence the two 10-qubit Pauli operators anticommute.

1.8.B **Unitary evolution vs Hamiltonian for independent subsystems.** If subsystem $\mathcal{S}_1$ undergoes a unitary transformation U_1 and subsystem $\mathcal{S}_2$ undergoes a transformation U_2, then the overall unitary evolution is described by the operator $U_1 \otimes U_2$. Now, suppose that both subsystems evolve continuously in time and are characterised by the Hamiltonians H_1 and H_2. What is the overall Hamiltonian?

Hint: Over an infinitely small time interval dt, the subsystems evolve by $U_1 = \mathbb{1} - iH_1 dt$ and $U_2 = \mathbb{1} - iH_2 dt$, respectively.

Solution: As the two subsystems are independent, the evolution of the composite system follows from the tensor product of the two evolution operators:

$$\begin{aligned}\mathcal{U}_{\text{tot}} = \mathcal{U}_1 \otimes \mathcal{U}_2 &= (\mathbb{1}_1 - iH_1 dt) \otimes (\mathbb{1}_2 - iH_2 dt) \\ &= \mathbb{1}_1 \otimes \mathbb{1}_2 - i\,(H_1 \otimes \mathbb{1}_2)\,dt - i\,(\mathbb{1}_1 \otimes H_2)\,dt + O(dt^2) \\ &= \mathbb{1}_1 \otimes \mathbb{1}_2 - i\,(H_1 \otimes \mathbb{1}_2 + \mathbb{1}_1 \otimes H_2)\,dt + O(dt^2)\end{aligned}$$

Compare against $\mathcal{U}_{\text{tot}} = \mathbb{1}_{\text{tot}} - iH_{\text{tot}}dt$, we see that the overall Hamiltonian —i.e., the generator of the evolution of the composite system— is

$$H_{\text{tot}} \equiv H_1 \otimes \mathbb{1}_2 + \mathbb{1}_1 \otimes H_2$$

More generally, if we have two operators A and B commute with each other: $[A, B] = 0$, then we have:

$$e^A e^B = e^{A+B}.$$

Search for Baker–Campbell–Hausdorff formula for the general case when A and B might not commute.

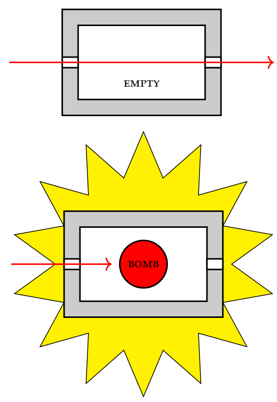
With $A = i(H_1 \otimes \mathbb{1}_2)t$ and $B = i(\mathbb{1}_1 \otimes H_2)t$, we then have:

$$\underbrace{e^{i(H_1 \otimes \mathbb{1}_2)t}}_{\mathcal{U}_1 \otimes \mathbb{1}_2} \underbrace{e^{i(\mathbb{1}_1 \otimes H_2)t}}_{\mathbb{1}_1 \otimes \mathcal{U}_2} = \underbrace{e^{i(H_1 \otimes \mathbb{1}_2 + \mathbb{1}_1 \otimes H_2)t}}_{\mathcal{U}_{\text{tot}} = \mathcal{U}_1 \otimes \mathcal{U}_2}$$

We can see that the Hamiltonian for the evolution operator $\mathcal{U}_{\text{tot}}$ is simply $H_{\text{tot}} = H_1 \otimes \mathbb{1}_2 + \mathbb{1}_1 \otimes H_2$.

1.9.B **The Quantum Bomb Tester.** You have been drafted by the government to help in the demining effort in a former war-zone. In particular, retreating forces have left very sensitive bombs in some of the sealed rooms. The bombs are configured such that if even one photon of light is absorbed by the fuse (i.e. if someone looks into the room), the bomb will go off. Each room has an input and output port which can be hooked up to external devices. An empty room will let light go from the input to the output ports unaffected, whilst a room with a bomb will explode if light is shone into the input port and the bomb absorbs even just one photon.

This is a slightly modified version of a bomb testing problem described by Avshalom Elitzur and Lev Vaidman in *Quantum-mechanical interaction-free measurement*, Found. Phys. **47**, 987-997 (1993).



Your task is to find a way of determining whether a room has a bomb in it without blowing it up, so that specialised (limited and expensive) equipment can be devoted to defusing that particular room. You would like to know with certainty whether a particular room had a bomb in it.

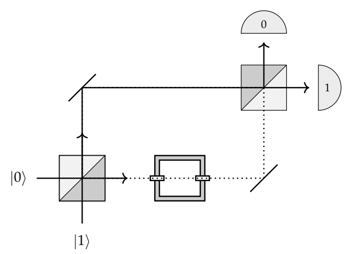
(1) To start with, consider the setup (see the margin) where the input and output ports are hooked up in the lower arm of a Mach-Zehnder interferometer (with symmetric beam splitters).

  (a) Assume an empty room. Send a photon to input port $|0\rangle$. Which detector, at the output port, will register the photon?

  (b) Now assume that the room does contain a bomb. Again, send a photon to input port $|0\rangle$. Which detector will register the photon and with which probability?

  (c) Design a scheme that allows you – at least part of the time – to decide whether a room has a bomb in it without blowing it up. If you iterate the procedure, what is its overall success rate for the detection of a bomb without blowing it up?

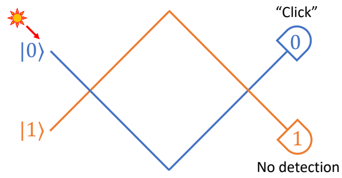
Hint: Consider the setup where the input and output ports are hooked up in one of the arms of a Mach-Zehnder interferometer.



(2) Assume that the two beam splitters in the interferometer are different. Say the first beamsplitter reflects incoming light with probability r and transmits with probability $t = 1 - r$ and the second one transmits with probability r and reflects with probability t. Would the new setup improve the overall success rate of the detection of a bomb without blowing it up?

(3) There exists a scheme, involving many beamsplitters and something called "quantum Zeno effect", such that the success rate for detecting a bomb without blowing it up approaches 100%. Try to work it out or find a solution on internet.

Solution: General set up of the problem:



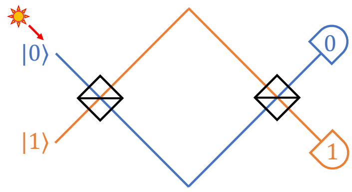
As we can see from the figure on the right, our qubit state is define by the two light paths, with the blue path representing $|0\rangle$ and the orange path representing $|1\rangle$. We will use D0 and D1 to denote the two detectors at the end that measure whether the photon is at the $|0\rangle$ path or $|1\rangle$ path. If we input the photon from the $|0\rangle$ port as shown, the it will stay on the $|0\rangle$ path and get detected at the end by D0.

This is a set-up without any gates in it. Now we are going to add beam-splitters into the set-up which act as gates operating on our quantum state.

(1) (a) **No bombs:**

A 50/50 beam splitter will turn an incoming photon into equal superposition of the transmitted and reflected photon. It matrix representation using our definition of "light path" qubits above is given in the lecture note as

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



Let us consider the case in which there is no bombs, and we add two 50/50 beam splitters into the circuit as shown on the right.

The full circuit with two 50/50 beam-splitters is then:

$$B^2 = iX$$

i.e. it will flip the input.

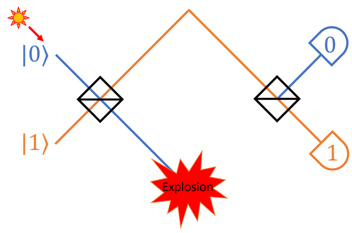
With input state $|0\rangle$, the output state is simply

$$B^2 |0\rangle = iX |0\rangle \equiv |1\rangle$$

Hence, we will measure $|1\rangle$ with 100% probability.

Physically the photon can travel from the $|0\rangle$ input to the D1 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 the D0 differ by a phase shift of π, and hence they interfere destructively.

(b) **With bombs:**



If there is a bomb in one of the arms of the interferometer, it will act like a measuring device, causing us to know which arm the photon has travelled through or not. With 50% probability the photon will pass through and hit the bomb, causing it to explode. The rest of the time, the photon will be reflected on the first beam splitter and go on to hit the second beam splitter, and then be detected in either detector with 50% probability. The probability to detect the photon at D0 (D1) is thus given by 1/4.

(c) If we measure a photon at D0, 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 be measured at D1

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

On the other hand, measuring a photon at D1 can happen in both the cases of no bombs and with bombs. Hence, if we measure a photon at D1, we are uncertain about whether there is a bomb and we will repeat our experiment.

The overall scheme if there is a bomb is given by:

$$\begin{cases} P_{\text{boom}} = \frac{1}{2} & \text{BOOM, terminate} \\ P_{\text{idle}} = \frac{1}{2} & \text{bomb idle} \begin{cases} P_{D0} = \frac{1}{4} & \text{measure } |0\rangle \rightarrow \text{bomb detected, terminate.} \\ P_{D1} = \frac{1}{4} & \text{measure } |1\rangle \rightarrow \text{uncertian, repeat.} \end{cases} \end{cases}$$

At each repeat we have $P_{\text{boom}} = \frac{1}{2}$ probability of setting off the bomb and $P_{D0} = \frac{1}{4}$ probability of detecting the bomb.

In the limit of infinity trials, we will terminate in one of the two outcomes above. The probability of the two terminating options is determined by their relative probability. Hence, the probability of the bomb being successfully detected if it exists is:

$$\frac{P_{D0}}{P_{\text{boom}} + P_{D0}} = \frac{\frac{1}{4}}{\frac{1}{2} + \frac{1}{4}} = \frac{1}{3}.$$

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) Can we do any better with beam splitters beyond the 50/50 type?

More general beam-splitters will have a transmission probability T and a reflection probability $R = 1 - T$ if we measure right after the beam splitter. The matrix form (gate form) of such a general beam splitter is given in Sec. 3.2 of the lecture notes as:

$$B = \sqrt{T}\left(|0\rangle\langle 0| + |1\rangle\langle 1|\right) + i\sqrt{R}\left(|0\rangle\langle 1| + |1\rangle\langle 0|\right) = \begin{pmatrix} \sqrt{T} & i\sqrt{R} \\ i\sqrt{R} & \sqrt{T} \end{pmatrix} \tag{2}$$

Now we will replace the two 50/50 beam-splitters in our set-up with one that has $T = t$ and another that has $T = r = 1 - t$:

$$B_1 = \begin{pmatrix} \sqrt{t} & i\sqrt{r} \\ i\sqrt{r} & \sqrt{t} \end{pmatrix} \quad B_2 = \begin{pmatrix} \sqrt{r} & i\sqrt{t} \\ i\sqrt{t} & \sqrt{r} \end{pmatrix}.$$

In such a case, following similar arguments as before, we then have:

- **No bombs:**

  With input state $|0\rangle$, our circuit is simply

  $$B_1 B_2 |0\rangle = iX|0\rangle \equiv |1\rangle$$

  Hence, we will measure $|1\rangle$ with 100% probability.

- **With bombs:**

The bomb act as a detector that essentially perform a measurement after the first beam-splitter. Overall, we have:

$$\begin{cases} P_{\text{boom}} = t & \text{BOOM, terminate} \\ P_{\text{idle}} = r & \text{bomb idle} \begin{cases} P_{D0} = rt & \text{measure } |0\rangle \to \text{bomb detected, terminate.} \\ P_{D1} = r^2 & \text{measure } |1\rangle \to \text{uncertian, repeat.} \end{cases} \end{cases}$$

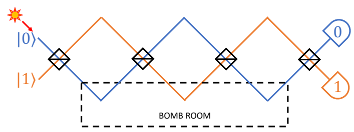
At each repeat we have $P_{\text{boom}} = t$ probability of setting off the bomb and $P_{D0} = rt$ probability of detecting the bomb.

In the limit of infinity trials, we will terminate in one of the two outcomes above. The probability of the two terminating options is determined by their relative probability. Hence, the probability of terminating in the bomb being successfully detected is

$$\frac{P_{D0}}{P_{\text{boom}} + P_{D0}} = \frac{rt}{t + rt} = \frac{r}{1 + r}.$$

To maximise the probability of detecting the bomb, we have $r \to 1$, and $\frac{r}{1+r} \to \frac{1}{2}$. Note that, this also means the probability of termination in each run is infinitesimal and we require infinite trials to terminate. i.e. most of the measurement will end in the 'useless' $|1\rangle$.

(3) In order to further improve our set-up, we will now probe the bomb multiple times rather than just once as shown on the right.



The matrix representation of the beam splitter in Eq. (2) can also be written as:

$$B_\theta = \begin{pmatrix} \cos\theta & i\sin\theta \\ i\sin\theta & \cos\theta \end{pmatrix} = \mathbb{1}\cos\theta + iX\sin\theta = e^{i\theta X}. \tag{3}$$

where $T = \cos^2\theta$ and $R = 1 - T = \sin^2\theta$.

The number of beam-splitters we will use in our set-up is some *even number* N, and all of them will be beam-splitters with $\theta = \frac{\pi}{2N} + \frac{\pi}{2}$.

- **No bombs:**

  Our circuit is simply

  $$B_\theta^N = e^{iN\theta X} = \mathbb{1}\cos(N\theta) + iX\sin(N\theta)$$

  We have

  $$N\theta = \frac{\pi}{2} + N\frac{\pi}{2} = (n + \frac{1}{2})\pi$$

  for some integer n since N is a even number. Hence,

  $$B_\theta^N = \mathbb{1}\cos(N\theta) + iX\sin(N\theta) \propto X$$

  Therefore, like before the whole circuit is simply equivalent to an X gate in the absence of a bomb, so that the light path will interfere and always output $|1\rangle$ when the input is $|0\rangle$.

- **With bombs:**

  Like before, the existence of the bomb will destroy the interference and allow the setup to output $|0\rangle$. To output $|0\rangle$, the photon need to take the no-bomb-room path (*all reflection* for all N beam splitter) before arriving at the last beam-splitter. Hence, the probability of outputting 0 and thus detect the bomb without explosion is:

  $$P_{D0} = R^N = \sin^{2N}(\theta) == \sin^{2N}\left(\frac{\pi}{2N} + \frac{\pi}{2}\right) = \cos^{2N}\left(\frac{\pi}{2N}\right).$$

In the limit of large N it becomes:

$$P_{D0} = \left(1 - \frac{1}{2}\left(\frac{\pi}{2N}\right)^2 + \mathcal{O}(N^{-4})\right)^{2N}$$
$$\approx 1 - \frac{\pi^2}{4N} + \mathcal{O}(N^{-2})$$

which can approach 1 when $N \to \infty$.

Hence, using our set-up with $N \to \infty$, we will always measure $|0\rangle$ when there is a bomb and always measure $|1\rangle$ when there are no bombs. Hence we have a way of distinguishing the two possibilities perfectly without causing the bomb to explode!

At large N, we have $T \to 0$, $R \to 1$. Hence, each measurement by the bomb after the beam-splitter will have very high probability of projecting the photon into the reflected paths. Hence, such constant measurements will keep projecting the photon into reflected path and prevent the photon into drifting into the transmitted path that set off the bomb, thus it is related to Zeno effect.

Additional insights:

Okay, the maths checks out, but it still seems a bit counter-intuitive that we have detected the bomb without hitting it with a photon. How exactly do we manage it? Let us look back at the set-up in the cases of no bombs and with bombs:

- **No bombs:** All beam splitters will take the incoming light beam and take it into a *superposition* of the transmitted and reflected beams, i.e. *the entire system without bombs is quantum mechanical* such that the interference between the two light paths can happen and *always output 1*.
- **With bombs:** All beam splitters are followed by detectors (including the bomb) which will destroy their quantum mechanical property, and turn each of them into a device that inserts a mirror with some probability (reflection) and do nothing otherwise (transmission). Such a device is completely classical, and hence *the entire system with bombs is classical*. In this classical set-up we can *sometimes measure 0* through multiple reflection.

We are NOT trying to directly detect the bomb by hitting it with photon. The *mere presence of the bomb without any photon hitting it will already turn the whole system from entirely quantum to entirely classical.*

Hence, our set-up is for detecting whether the system (the beam splitter inside) is quantum or classical, which will in turn inform us about whether there is a bomb or not.

More generally, the bomb is just a detector, our question turns into, can we know that whether there is a detector present without setting off the detector? The answer is yes, and the way we do this is making use of the fact that *a detector will destroy interference by its mere presence even without interacting with the particle*. Hence, we can map the question of whether there is a detector or not to whether we have observe a interference pattern or not. This is very much in the same spirit as the double slit experiment.

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).*