Homework 6

Let

$$P_1 = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle) \cdot \frac{1}{\sqrt{2}}(\langle 0| - i\langle 1|) \text{ and } P_2 = \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle) \cdot \frac{1}{\sqrt{2}}(\langle 0| + i\langle 1|).$$

1. Check that the above matrices are projection operators.

2. Check that the above matrices can be used for organizing a von Neumann measurement.

3. Find the classical and quantum outputs of the measurements of a qubit in

1. state $|0\rangle$,
2. state $|1\rangle$.

4. Find the classical and quantum outputs of the measurement of a qubit in

1. state $\frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle)$;
2. state $\frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle)$.

For problems 3 and 4, please present results in the following form:

State $|v\rangle = ...$

Quantum outputs	**Classical outputs**	**Probability**
Write here q. out	Write here cl. out	Prob. of this event

5. We will use the following notations and assumptions.

1. Basis 0, bit 0, means that Alice sends quantum state $|0\rangle$.
2. Basis 0, bit 1, means that Alice sends quantum state $|1\rangle$.
3. Basis 1, bit 0, means that Alice sends quantum state $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$.
4. Basis 1, bit 1, means that Alice sends quantum state $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$.
5. Making measurement in basis B_0 means to use $P_0 = |0\rangle\langle 0|$ and $P_1 = |1\rangle\langle 1|$.
6. Making measurement in basis B_1 means to use $P_0 = |+\rangle\langle +|$ and $P_1 = |-\rangle\langle -|$.

Let Alice choose the following bases and bits for sending qubits to Bob:

time instance:	t_1	t_2	t_3	t_4	t_5	t_6	t_7	t_8	t_9	t_{10}
basis:	B_0	B_1	B_1	B_0	B_1	B_0	B_1	B_0	B_0	B_1
bit:	0	1	0	1	1	1	0	0	0	0

Let now Bob use the following bases for conducting measurements

time instance:	t_1	t_2	t_3	t_4	t_5	t_6	t_7	t_8	t_9	t_{10}
basis:	B_0	B_0	B_0	B_0	B_1	B_1	B_1	B_0	B_0	B_1

Further Alice and Bob follow the protocol BB84 (which we discussed in the class).

Find the secret key obtained by Alice and Bob.

6. For the same settings (bases and bits used by Alice and bases used by Bob) let us assume that Eve intercepts the first 5 qubits sent by Alice. Eve measures these qubits using bases

time instances:	t_1	t_2	t_3	t_4	t_5
basis:	B_1	B_1	B_1	B_1	B_1

and sends the qubits (after measurements) further to Bob.

Find possible classical outputs and the corresponding probabilities of the first 5 measurements conducted by Bob.