Quantum Communication
day 4

June 22, 2022

1 Theory

Quantum Money. Suppose you're a quantum money counterfeiter, trying to forge a banknote in Wiesner's scheme. You're given a qubit that's $|0\rangle$, $|1\rangle$ or $|+\rangle$, $|-,\rangle$ each with equal probability 1/4. You can apply any quantum circuit you like to the qubit to produce a two-qubit state. Then, both of your output qubits will separately be given back to the bank for verification. (I.e., if the original qubit was $|0\rangle$ or $|1\rangle$ then the bank will measure both output qubits in the $\{|0\rangle, |1\rangle\}$ basis and accept if and only if both outcomes match the original qubit, and likewise if the original qubit was $|+\rangle$ or $|-\rangle$ the bank will measure and check in the $\{|+\rangle, |-\rangle\}$ basis.) Your goal is to maximize the probability that the bank accepts both coins.

a) Give a procedure that succeeds with probability at least 5/8 . Your procedure should not involve creating any entangled states.

b) [Open discussion] What do you think might be a possible use-case for Wiesner's quantum money? What are the main drawbacks of its scheme? Why its implementation is very difficult?

2 Practice

Quantum Money. Imagine the following procedure to counterfeit one quantum coin (a qubit). Among 3 qubits, initialize the first two qubits to $|0\rangle$ and let the third qubit be the qubit from the original banknote to be counterfeited. Then apply a 3-qubit unitary transformation. Finally, discard the first qubit and output the state given by the second two qubits.

a) Run the protocol using a random unitary[1] on a quantum computer and compute what is the probability that both the qubits get validated by the bank.

b) [Difficult] it turns out that the optimal choice is a unitary whose effect is the following mapping:

$$|000\rangle \to \frac{\sqrt{3}}{2}|000\rangle + \frac{|110\rangle + |101\rangle + |011\rangle}{\sqrt{12}} \tag{1}$$

$$|001\rangle \to \frac{\sqrt{3}}{2}|111\rangle + \frac{|001\rangle + |010\rangle + |100\rangle}{\sqrt{12}} \tag{2}$$

[1] to implement given unitary with the correct gates check https://qiskit.org/documentation/tutorials/simulators/4_custom_gate_noise.html and to pick a random unitary check https://qiskit.org/documentation/stubs/qiskit.quantum_info.random_unitary.html

Try to run a circuit with this mapping and show that the counterfeiting probability is 3/4.

Bomb-test. Perform the bomb-test on a real QC:

a) for the trivial version (one iteration) and check that the winning probability (i.e. probability of identifying the bomb without dying) is close to 1/4.

b) for N iterations, varying N. Discuss the noise added on every iteration (check the information IBM gives about the QC you are using and try to use different combinations of qubits).