Quantum Information Theory
Exercise sheet 5

Lecture: Prof. Dr. Otfried Gühne Exercise: Costantino Budroni
Lecture: Tuesday, 10-12, Room D 120
Exercise: Monday, 15-17, Room B 107

12. Quantum money

Stephen Wiesner has proposed the following idea for banknotes that are impossible to copy: Each banknote contains N qubits, which maintain their quantum states unchanged indefinitely. It also has a classical serial number printed on it. When the banknote is manufactured, two N-bit strings are chosen randomly and the qubits are prepared according to the BB84 scheme, using one bit string to determine the bases and the other bit string to determine the basis states. The bank keeps a secret record of the serial numbers and the random bit strings. When a banknote is returned to the bank, the qubits are measured in the bases used for the preparation. It is only accepted if all measurement results agree with the states in which the qubits were prepared.

(a) Is a genuine banknote still valid after the bank's inspection?

(b) A counterfeiter tries to copy a banknote by measuring its qubits in randomly chosen bases and making new banknotes with their qubits prepared according to the measurement results. What is the probability that a new banknote's qubits are in the correct states? What is the probability that a new banknote passes the bank's inspection?

(c) Suppose now that the measurement results the banknote has to reproduce during the inspection are known to the counterfeiter (but the basis string is not). What is the counterfeiter's best strategy to copy the banknote? How do the results of (b) change?

13. Depolarizing channel

We consider a qubit subjected to the following error model: With probability $1-p$, nothing happens to the qubit, and with probability p one of the following errors occurs with equal probability:

- bit flip: $|0\rangle \mapsto |1\rangle$, $|1\rangle \mapsto |0\rangle$, i. e. $|\psi\rangle \mapsto \sigma_x|\psi\rangle$,
- phase flip: $|0\rangle \mapsto |0\rangle$, $|1\rangle \mapsto -|1\rangle$, i. e. $|\psi\rangle \mapsto \sigma_z|\psi\rangle$,
- bit and phase flip: $|0\rangle \mapsto \mathrm{i}|1\rangle$, $|1\rangle \mapsto -\mathrm{i}|0\rangle$, i. e. $|\psi\rangle \mapsto \sigma_y|\psi\rangle$.

We can describe this by the following unitary evolution in the Hilbert space of the qubit and the environment:

$$|\psi\rangle \otimes |0\rangle_E \mapsto \sqrt{1-p}|\psi\rangle \otimes |0\rangle_E + \sqrt{\frac{p}{3}} \sum_i \sigma_i |\psi\rangle \otimes |i\rangle_E.$$

(a) Compute the Bloch vector representation of a general pure state after the evolution.

(b) If the qubits transmitted in the BB84 protocol are subjected to this error model, what is the fraction of errors in the sifted key? Is there a maximum error probability p we can tolerate?