C&O 781 Topics in Quantum Information
Quantum Information Theory, Error-correction, and Cryptography
University of Waterloo
Fall 2006

Instructors: Debbie Leung and Ashwin Nayak
Assignment 2
Due: Nov. 10, 2006

Total: 40 marks.

Question 1. [5 marks] Count the number of distinct n-qubit subspaces of dimension 2^k that are stabilized by some subgroup of the Pauli group, where $0 \leq k \leq n$.

Question 2. [5 marks] Exercise 10.27, Page 452, Nielsen and Chuang.

Question 3. [3 marks] Exercise 10.67, Page 488, Nielsen and Chuang.

Question 4. [7 marks] Exercise 10.69-70, Page 491, Nielsen and Chuang.

Question 5. [10 marks] All symbols are as defined in class (or as in Nielsen and Chuang). Consider the 5-qubit code with stabilizer generated by $IXZZX$, $XIXZZ$, $ZXIXZ$, $ZZXIX$.

1. State one choice for each of $\bar{X}, \bar{Z}$ that is fault tolerant (the choice should admit a solution for the rest of the question). (1 mark)
2. How can CNOT, P, and H be performed fault-tolerantly? State complete schemes as circuits. (3 marks for the general method, 2 marks for each correct solution.)

Question 6. [5 marks] Recall that an ideal strong coin flipping protocol is a communication protocol between two parties A, B that start without any input and produce one output each $c_A, c_B \in \{0, 1, \text{abort}\}$ such that:

1. If A and B are honest (follow the protocol), then for any bit $b \in \{0, 1\}$,
$$\Pr(c_A = c_B = b) \quad = \quad \frac{1}{2}.$$
2. Moreover, if only A is dishonest, then for any bit $b \in \{0, 1\}$,
$$\Pr(c_B = b) \quad \leq \quad \frac{1}{2}.$$
Similarly, if only B is dishonest, he cannot force any particular outcome on A's side, with probability more than 1/2.

Prove that ideal strong coin flipping is impossible, even with quantum communication.

Question 7. [5 marks] Let $\mathcal{H}$ be a finite dimensional Hilbert space. Prove that for any density matrices $\rho_0, \rho_1 \in \mathrm{L}(\mathcal{H})$,

$$\max_{\sigma \in \mathrm{L}(\mathcal{H})} \left(\mathrm{F}(\rho_0, \sigma) + \mathrm{F}(\sigma, \rho_1) \right) \quad \leq \quad 1 + \sqrt{\mathrm{F}(\rho_0, \rho_1)} \, .$$