EE 605: Error Correcting Codes

Instructor: Saravanan Vijayakumaran
Indian Institute of Technology Bombay
Autumn 2010

Assignment 1 : **36 points** **Due date**: August 10, 2010

Each of the following exercises is worth 3 points. Every nontrivial step in a proof should be accompanied by justification.

1. Consider a binary symmetric channel (BSC) with crossover probability p. Suppose N bits are transmitted over it.

    (a) What is the probability that *exactly* one error is observed in the received bits?

    (b) What is the probability that *at least* one error is observed in the received bits?

    (c) What is the probability that *at most* one error is observed in the received bits?

2. Suppose that a sequence of N bits is passed through a cascade of two BSCs with crossover probabilities p_1 and p_2, respectively.

    (a) What is the probability that *exactly* k errors are observed in the received bits?

    (b) What is the probability that *at least* k errors are observed in the received bits?

    (c) What is the probability that *at most* k errors are observed in the received bits?

    Assume $k \leq N$.

3. Suppose a binary source generates bits which are equally likely to be 0 or 1. Suppose the source output is encoded by a 3-repetition code before transmission over a cascade of two BSCs with crossover probabilities p_1 and p_2, respectively. What is the optimal decoding rule for this scenario?

4. Suppose a binary source generates bits which are equally likely to be 0 or 1. Suppose the source output is passed through three BSCs in parallel with crossover probabilities p_1, p_2, and p_3, respectively. This is illustrated in Figure 1.

    (a) What is the optimal decoding rule for this scenario when $p_1 = p_2 = p_3$?

    (b) What is the optimal decoding rule for this scenario when $p_1 > p_2 > p_3$?

5. Determine which of the following binary operations are associative.

    (a) The operation $\star$ on $\mathbb{Z}$ defined by $a \star b = a - b$.

    (b) The operation $\star$ on $\mathbb{R}$ defined by $a \star b = a + b + ab$.

    (c) The operation $\star$ on $\mathbb{Q}$ defined by $a \star b = \frac{a+b}{5}$.

    (d) The operation $\star$ on $\mathbb{Z} \times \mathbb{Z}$ defined by $(a, b) \star (c, d) = (ad + bc, bd)$.

    (e) The operation $\star$ on $\mathbb{Q} - \{0\}$ defined by $a \star b = \frac{a}{b}$.

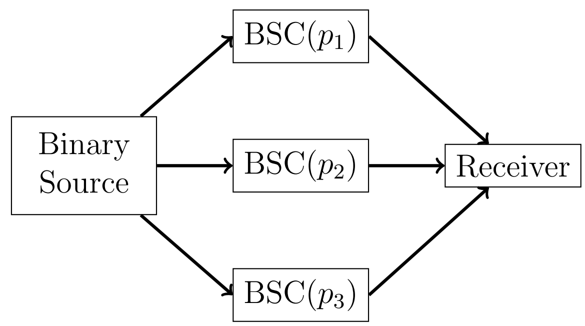

Figure 1: Bits through three parallel BSCs

6. Determine which of the binary operations described in the previous exercise are commutative.

7. Determine which of the following sets are groups under addition.

   (a) The set of rational numbers (including 0) in lowest terms whose denominators are odd.

   (b) The set of rational numbers (including 0) in lowest terms whose denominators are even.

   (c) The set of rational numbers of absolute value less than 1.

   (d) The set of rational numbers of absolute value greater than or equal to 1 together with zero.

8. Let $G = \{z \in \mathbb{C} | z^n = 1 \text{ for some } n \in \mathbb{Z}^+\}$.

   (a) Prove that G is a group under multiplication.

   (b) Prove that G is not a group under addition.

9. Let $G = \{a + b\sqrt{2} \in \mathbb{R} | a, b \in \mathbb{Q}\}$.

   (a) Prove that G is a group under addition.

   (b) Prove that the nonzero elements of G form a group under multiplication.

10. Let G be a group. Prove that if $x^2 = 1$ for all $x \in G$ then G is abelian.

11. Prove that $A \times B$ is an abelian group if and only if both A and B are abelian groups.

12. Let m be a positive integer. If m is not a prime, prove that the set $\{1, 2, 3, \ldots, m-1\}$ is not a group under modulo-m multiplication.