EE 605: Error Correcting Codes

Instructor: Saravanan Vijayakumaran

Indian Institute of Technology Bombay

Autumn 2010

1. Suppose a binary source generates bits which are equally likely to be 0 or 1. Suppose the source output is encoded by an n-repetition code, before transmission over a time-varying BSC which operates in the following manner. Given that $n = n_1 + n_2$, the time-varying BSC behaves like a regular BSC with crossover probability p_1 for the first n_1 bits which are transmitted through it and it behaves like a regular BSC with crossover probability p_2 for the remaining n_2 bits which are transmitted through it. If n is odd and $p_1 + p_2 = 1$, what is the optimal decoding rule for this scenario?

   [3 points]

2. Consider a set of positive integers $G = \{1, 2, \ldots, p - 1\}$ where p is a prime number.

   (a) Prove that multiplication of two set elements modulo p is a binary operation over G?   [1 point]

   (b) Prove that every element in G has a multiplicative inverse.   [1 point]

3. Prove that every finite field F_q has a prime subfield. If the prime subfield has p elements, prove that
$$\underbrace{\beta + \beta + \cdots + \beta}_{p \text{ times}} = 0$$
   for every $\beta \in F_q$ where 0 is the additive identity of F_q.   [3 points]

4. Prove that a nonzero finite field element β satisfies $\beta^m = 1$ for some positive integer m if and only if m is divisible by the order of β.   [2 points]