EE 605: Error Correcting Codes
Instructor: Saravanan Vijayakumaran
Indian Institute of Technology Bombay

Quiz 2 : 20 points October 16, 2014

1. (5 points) Let a binary cyclic code C have generator polynomial $g(X)$. If C is used for error detection, prove the following.
   (a) If $X + 1$ is a factor of $g(X)$, all odd weight error patterns are detected.
   (b) If an error pattern $e(X)$ is detectable, then its ith cyclic shift $e^{(i)}(X)$ is also detectable.
2. (5 points) Find all subgroups of $\mathbb{Z}_{30} = \{0, 1, 2, \dots, 29\}$ which is a group under modulo 30 addition. For each subgroup, list its generators.
3. (5 points) Let F_q be a finite field with q elements.
   (a) For any $\beta \in F_q^*$, consider the sequence $\beta, \beta^2, \beta^3, \beta^4, \dots$. Show that the first element to repeat in this sequence is β, i.e. there exists a positive integer n such that $\beta^i \neq \beta^j$ for $1 \leq i < j \leq n - 1$ and $\beta^n = \beta$.
   (b) Using the above result, show that all the elements in F_q are roots of the polynomial $x^q - x$.
4. (5 points) Let $\mathbb{F}_3$ be the finite field with three elements. Let $\mathbb{F}_3[x]$ be the set of polynomials with coefficients in $\mathbb{F}_3$.
   (a) Find the prime polynomials of degree 1 and degree 2 in $\mathbb{F}_3[x]$.
   (b) Let $g(x)$ be a degree 2 prime polynomial found in the previous part. Let $R_{\mathbb{F}_3,2}$ be the set of remainders when polynomials in $\mathbb{F}_3[x]$ are divided by $g(x)$. $R_{\mathbb{F}_3,2}$ is a field under addition and multiplication modulo $g(x)$. Find the multiplicative inverses of all the non-zero elements in $R_{\mathbb{F}_3,2}$.