EE 605: Error Correcting Codes

Instructor: Saravanan Vijayakumaran
Indian Institute of Technology Bombay
Autumn 2010

Solutions to Assignment 3 — Prepared by Sravan Kumar Jatavath

1. Suppose $F_q = \{0, \beta_1, \beta_2, \ldots, \beta_{q-1}\}$. We know that

$$x^q - x = x \prod_{i=1}^{q-1} (x - \beta_i) \Rightarrow x^{q-1} - 1 = \prod_{i=1}^{q-1} (x - \beta_i)$$

Let -1 be the additive inverse of the multiplicative identity 1 of F_q. Then using the distributive property we can prove that $-\beta_i = (-1)\beta_i$ for all i. Now equating the constant terms on both sides of the above equation we get

$$-1 = (-1)^{q-1} \prod_{i=1}^{q-1} \beta_i \Rightarrow \prod_{i=1}^{q-1} \beta_i = (-1)^{q-2}.$$

Equating the coefficients of x^{q-2} on both sides of the first equation we get

$$0 = -(\sum_{i=1}^{q-1} \beta_i) \Rightarrow \sum_{i=1}^{q-1} \beta_i = 0$$

2. Consider the irreducible polynomial $x^3 + x + 1 \in \mathbb{F}_2[x]$. The set of remainders $R_{\mathbb{F}_2,3}$ with the operations of addition and multiplication modulo $x^3 + x + 1$ form a field of $2^3 = 8$ elements. The set $R_{\mathbb{F}_2,3}$ consists of the elements $\{0, 1, x, x + 1, x^2, x^2 + 1, x^2 + x, x^2 + x + 1\}$.

3. Determine all the primitive elements of F_7 and F_{17}.

   The primitive element of a field is the non-zero element whose powers generate all the non-zero elements of the field. A field of 7 element is isomorphic to $\{0, 1, 2, 3, 4, 5, 6\}$. The candidates for the primitive element are the non-zero elements $F_7^* = \{1, 2, 3, 4, 5, 6\}$. For any element $a \in F_7^*$, consider the multiplicative subgroup generated by it: $S(a) = \{1, a, a^2, \ldots, a^{n-1}\}$. The number of elements in $S(a)$ is equal to the order n of a. By Lagrange's theorem, n divides 6. So the possible orders of a non-zero element in F_7 are 1, 2, 3 and 6. If an element is primitive, then it needs to have order $|F_7^*| = 6$.

   The element 1 has order 1 so it is not primitive. Since $6^2 = 1 \bmod 7$, 6 has order 2. None of $\{2, 3, 4, 5\}$ are equal to 1 mod7 when they are squared. Since $2^3 = 8 = 1 \bmod 7$ and $4^3 = 64 = 1 \bmod 7$, 2 and 4 have order 3. Both 3 and 5 are not equal to 1 mod7 when they are cubed. So they have to have order 6 and are primitive elements.

   Similarly, the possible orders of non-zero elements in F_{17} are 1, 2, 4, 8 and 16. Eliminating those non-zero elements which have orders 1, 2, 4 or 8 we get the primitive elements as $\{3, 5, 6, 7, 10, 11, 12, 14\}$.

4. The prime polynomials of degree 1 in $F_2[x]$ are $\{x, x+1\}$. Of the degree 2 polynomials in $F_2[x]$, $\{x^2, x^2+1, x^2+x, x^2+x+1\}$, only x^2+x+1 is prime because the other three either have an even number of terms (which results in $x+1$ being a factor) or have x as a factor. The non-prime polynomials of degree 3 must have a degree 1 factor which is either x or $x+1$. So the polynomials of degree 3 with a non-zero constant term and an odd number of terms are prime: $\{x^3+x+1, x^3+x^2+1\}$.

   We claim that a non-prime polynomial of degree 5 has either x, $x+1$ or x^2+x+1 as a factor. If not, all its prime factors are degree 3 or higher. Two such factors cannot add up to degree 5. So if we eliminate all the polynomials of degree 5 which have x, $x+1$ or x^2+x+1 as a factor, the remaining are the prime polynomials of degree 5. If we choose only those degree 5 polynomials whose constant term is non-zero, we eliminate degree 5 polynomials which have x as a factor. If we choose only those degree 5 polynomials which have an odd number of terms, we eliminate degree 5 polynomials which have $x+1$ as a factor. The degree 5 polynomials which have an odd number of terms, a non-zero constant term and x^2+x+1 as a factor are $(x^2+x+1)(x^3+x+1) = x^5+x^4+1$ and $(x^2+x+1)(x^3+x^2+1) = x^5+x+1$. The remaining degree 5 polynomials with non-zero constant term and odd number of terms are prime.

5. **One direction:** Suppose $\gcd(q-1, k) = 1$. Let $\beta \in F_q$. If $\beta = 0$, then it is the kth power of 0 itself. Suppose $\beta \neq 0$, then $\beta^{q-1} = 1$. By Bezout's identity, $1 = a(q-1)+bk$ for some integers $a, b \in \mathbb{Z}$. Then we have

   $$\beta = \beta^1 = \beta^{a(q-1)+bk} = [\beta^{q-1}]^a[\beta^b]^k = [\beta^b]^k$$

   Since $\beta^b \in F_q$, we have proved that every element in F_q is a kth power of some other element in F_q.

   Other direction: Suppose every element in F_q is the kth power of some other element in F_q. Let α be the primitive element of F_q. Then$\alpha^{q-1} = 1$ and $\alpha^i \neq 1$ for $i = 1, 2, \ldots, q-2$. By our assumption $\alpha = \beta^k$ for some element $\beta \in F_q$. Also $\beta^{q-1} = 1$ since β is a non-zero element in a field of q elements.

   Suppose $\gcd(q-1, k) = d \neq 1$. Then $\frac{q-1}{d}$ is a positive integer less than $q-1$. Note that $\frac{k}{d}$ is also a positive integer less than k. Now we get

   $$\alpha^{\frac{q-1}{d}} = (\beta^k)^{\frac{q-1}{d}} = (\beta^{q-1})^{\frac{k}{d}} = 1^{\frac{k}{d}} = 1$$

   which is a contradiction since $\frac{q-1}{d} < q-1$ and α is a primitive element. So $\gcd(q-1, k) = 1$.