ECEN 604 - Channel Coding for Communication

Avinash Vem
ECE,Texas A&M University.

November 17, 2015

Number Theory and Algebra: Essentials

1 Motivation

Until this point we have dealt with *binary codes*. That simplified our job in many ways. For example knowing the error locations in the received vectors is sufficient to decode the transmitted code word. However there are many important non binary codes in which case we need to know both the error locations and the value of the error in those locations for a successful decoding. But we don't have theory to construct and analyze non-binary codes. In the cyclic codes section we have seen that the generator polynomial $g(x)$ should divide the polynomial $x^n - 1$. For large block lengths i.e. for large values of n we need efficient tools for factorizing $x^n - 1$. We have also seen that the cyclic structure of codes reduce the amount of storage required for performing syndrome decoding. Maybe by exploiting additional algebraic structures we can develop better codes with efficient decoding.

So in the subsequent lectures we are going to develop the required mathematical tools to address these issues. Most of this material is contained in [1].

2 Preliminaries of Number Theory

Definition 1. An integer b is **divisible** by a nonzero integer a if there exists an integer c such that $b = ac$. We denote this as $a|b$ and read it as a divides b. We denote this as $a|b$ and read it as a divides b. Similarly for polynomials $a(x), b(x) \in F[x]$, where F is a field, we say $b(x)$ is **divisible** by $a(x)$ if there exists $c(x) \in F[x]$ such that $b(x) = a(x)c(x)$. Similarly we denote $a(x)|b(x)$.

Theorem 2 (Division Algorithm). *For any integers a and b with $a > 0$, $\exists$ unique integers q and r such that*

$$b = q + ar,$$

where $0 \leqslant r < a$. For polynomials, for $a(x)$ and $b(x)$ in $F[x]$, F a field, there is a unique representation

$$b(x) = q(x)a(x) + r(x),$$

where $deg(r(x)) < deg(a(x))$.

Definition 3. The **greatest common divisor** (g.c.d) of two integers $a, b \in \mathbb{Z}_+$ is the largest $k \in \mathbb{Z}_+$ such that $k|a$ and $k|b$. The same definition applies for polynomials

2.1 Euclidean Algorithm

Given $a_1, a_2 \in \mathbb{Z}_+$ and $a_1 > a_2$ W.L.O.G. compute the sequence of integers a_i until $a_m = 0$ where the sequence is given by

$$a_{n+2} = \mathrm{R}_{a_{n+1}}[a_n].$$

Note that $\mathrm{R}_{a_{n+1}}[a_n]$ is the remainder when a_n is divided by a_{n+1}. Then the g.c.d of a_1, a_2, denoted as (a_1, a_2), is given by a_{m-1}.

Theorem 4. *If $g = (a, b)$ then $\exists$ integers s and t such that $g = (a, b) = as + bt$. Similarly if $g(x) = (a(x), b(x))$ then $\exists$ polynomials $s(x)$ and $t(x)$ such that $g(x) = a(x)s(x) + b(x)t(x)$.*

3 Fields

The basic difference between a field and a ring is that a field should have a multiplicative identity and a multiplicative inverse for each element where as in a ring that's not necessary. For being complete, we define it here.

Definition 5 (Field)**.** A field F is a set of elements with two binary operations $+$ and $\times$ where

- $(F, +)$ forms an Abelian group.
- $(F\backslash\{0\}, \times)$ forms a **commutative** group under multiplication.
- The operations $+$ and $\times$ distribute.

Definition 6. In a ring R if $a, b \in R$ and $a, b \neq 0$ but $ab = 0$ then a and b are said to be zero divisors.

Theorem 7. *The ring $(\mathbb{Z}_p, +, \times)$ is a field if and only if p is a prime.*

Lemma 8. *In a ring $\mathbb{Z}_n$, the zero divisors are precisely those elements that are not relatively prime to n.*

Proof. Let $a \neq 0 \in \mathbb{Z}_n$ is not relatively prime to n. We will show that a is a zero divisor. Let $d \neq 1$ be the g.c.d of n and a: $d = (n, a)$. Therefore $a(n/d) = (a/d)n$ is equal to zero in $\mathbb{Z}_n$. Thus we have an element $b := n/d \in \mathbb{Z}_n$ where $ab = 0$ in $\mathbb{Z}_n$ thus proving a is a zero divisor in $\mathbb{Z}_n$.

Now suppose that let c is relatively prime to n and it's a zero divisor in $\mathbb{Z}_n \implies cd = kn$ for some $d \in \mathbb{Z}_n$ and $k \in \mathbb{Z}$. This implies n divides cd but there is no common factor between n and c therefore n divides d. This results in $d \equiv 0$ in $\mathbb{Z}_n$, a contradiction. □

Proof of Theorem 7. We have already shown that if p is not a prime then there exists zero divisors and hence $\mathbb{Z}_p$ is not a field. Now we will show that $\mathbb{Z}_p$ is indeed a field for p prime.

We have already seen that $(\mathbb{Z}_p, +)$ is a Abelian group. As for $(\mathbb{Z}_p \backslash \{0\}, \times)$, it is closed, commutative and 1 is the multiplicative identity. For the multiplicative inverse of $a \in \mathbb{Z}_p$, consider the set

$$\mathbb{Z}_p.a = \{1.a, 2.a, \ldots, (p-1).a\}$$

with $p - 1$ elements. All of the elements in the set are distinct because supposing not, $m.a \equiv n.a \mod p$ implying $(m - n).a \equiv 0 \mod p$ and hence a is a zero divisor. Clearly this is a contradiction and hence the set $\mathbb{Z}_p.a$ has $p - 1$ distinct elements belonging to the set $\mathbb{Z}_p \backslash \{0\}$ which has exactly $p - 1$ elements. Thus for some $m \in \{1, 2, \ldots p - 1\}$, $m.a \equiv 1 \mod p$. Hence $(\mathbb{Z}_p, \times)$ is an Abelian group and $(\mathbb{Z}_p, +, \times)$ is a field. □

3.1 Finite Fields or Galois Fields

A field with a finite number of elements is referred to as Galois field in the memory of the great mathematician Èveriste Galois (1811-1832).
We recall that the characteristic is the smallest positive integer k such that $k(1) = 1 + 1 + \ldots + 1 = 0$.

Lemma 9. *The characteristic of a field must be either* 0 *or a finite number.*

On the basis of this lemma, for any finite field GF(q) of characteristic p we can find a set of p elements $\{0, 1, 2 = 2(1), 3 = 3(1), \ldots ..p - 1\}$ which behave as a field. Thus $\mathbb{Z}_p$ for some prime number p is a sub-field of every Galois field.

Theorem 10. *The order q of a every finite field GF(q) must be a power of a prime.*

Theorem 11 (Freshman Exponentiation)**.** *If x and y are elements in a field of characteristic p,*

$$(x + y)^p = x^p + y^p.$$

Let us consider multiplicative questions related to a finite field.

Definition 12. The order of $\beta \in \mathrm{GF}(q)$, denoted as $\mathrm{ord}(\beta)$ is the smallest positive integer n such that $\beta^n = 1$.

Definition 13. An element with order $q - 1$ in $\mathrm{GF}(q)$ is called a **primitive element**.

The primitive element in a finite field plays an important role since it enables us to have a exponential representation for each element in the field and thus making the multiplication operation easy. So it's important for us to consider the questions: 1) Does a Galois field always have a primitive element? 2) How many primitive elements does a Galois field have? Over the next few lemmas we intend to arrive at the result in Theorem. 1 which tells us how many primitive elements are in a Galois field.

Lemma 14. *If $\beta \in GF(q)$ and $\beta \neq 0$ then $ord(\beta)|(q-1)$.*

Hint: Consider the subset $\{\beta, \beta^2, \dots, \beta^{\mathrm{ord}(\beta)} = 1\}$.

Lemma 15. *Let $\beta \in GF(q)$. $\beta^s = 1 \iff ord(\beta)|s$.*

Hint: $\Longleftarrow$ is trivial. For $\Longrightarrow$ suppose that $\mathrm{ord}(\beta) \not| \ s$ then $s = \mathrm{ord}(\beta)m + r$, $0 < r < \mathrm{ord}(\beta)$. Then $\beta^s = \beta^r = 1$ where $r < \mathrm{ord}(\beta)$ from the division algorithm which contradicts the minimality of $\mathrm{ord}(\beta)$.

Lemma 16. *In a finite field, if $ord(\alpha) = t$ and $\beta = \alpha^i$, then*

$$ord(\beta) = \frac{t}{(i,t)}.$$

Definition 17. The **Euler totient** function $\phi(n)$ is the number of positive integers less than n that are relatively prime to n. This is called Euler ϕ function.

$$\phi(n) = n \prod_{p|n} (1 - \frac{1}{p})$$

Lemma 18. *For a Galois field GF(q), if $t|(q-1)$ then there are $\phi(t)$ elements of order t in GF(q) where $\phi(t)$ is the Euler totient function.*

Proof. Let α be an element of order t. Then for any i such that $(i,t) = 1$, $\beta = \alpha^i$ has the same order t from Lemma. 16. From the definition of Euler Totient function there are exactly $\phi(t)$ such elements. To show that elements that are not of the form α^i but are of order t does not exist, consider the set of elements $\{\alpha, \alpha^2, \dots \alpha^t\}$ as solutions to the polynomial. Then show that all these elements are distinct and then use the fact that polynomials of degree t over a field has no more than t roots. □

Note that there are no elements of order t when $t \not| \ (q-1)$ since for any valid order t, it should divide $(q-1)$[see Lemma 14].

Theorem 1. There are $\phi(q-1)$ primitive elements in $\mathrm{GF}(q)$.

Example 19. For example consider GF(7). One can verify that only the elements 3 and 5 in GF(7) are of order 6. From the above theorem there are $\phi(7-1) = 2$ primitive elements.

Because primitive elements exist, the non zero elements of a field GF(q) can always be written as powers of a primitive element. Let α is a primitive element in GF(q) and let $\beta = \alpha^i$ be another primitive element i.e., $(i, q-1) = 1$. Despite the fact that there are two different representations for GF(q) i.e, $\{0, 1, \alpha, \alpha^2, \ldots, \alpha^{q-2}\}$ and $\{0, 1, \beta, \beta^2, \ldots, \beta^{q-2}\}$ these two are not two different fields. Therefore $\langle\alpha\rangle$ is isomorphic to $\langle\beta\rangle$. We can thus talk of **the** Galois field with q elements.

Theorem 20. *Every element of the field GF(q) satisfies the equation $x^q - x = 0$. Furthermore they constitute the entire set of the roots for this degree q equation.*

Corollary 21. *Every element in the field GF(q) satisfies the equation*

$$x^{q^n} - x = 0$$

for every $n \geqslant 0$.

4 Irreducible and Primitive polynomials

Definition 22. A polynomial $g(x) \in \mathrm{GF}(q)[x]$ is said to be **irreducible** over GF(q)[x] if it cannot be factored into polynomials of lower degree in the same field.

Example 23. $f(x) = x^2 + x + 1$ is irreducible over GF(2)[x] but $f(x) = x^2 + x + 1 = (x+2)^2$ is not irreducible (or factorizable) over GF(3)[x].

As we have seen in the example in the class, any irreducible polynomial can be used to construct an extension field but the computation in the field is easier if a primitive polynomial is used whose definition and properties we will see shortly.

Theorem 24. *Let p be prime. An irreducible mth-degree polynomial $f(x) \in GF(p)[x]$ divides $x^{p^m-1} - 1$.*

Proof. Let GF(q)[x] = GF(p^m) be constructed using the irreducible polynomial $f(x)$ where α denotes the root of the polynomial $f(x) : f(\alpha) = 0$. By Theorem 20 $\alpha^{p^m-1} = 1$ which implies

$$x^{p^m-1} - 1 = p(x)q(x) + r(x)$$

where deg($r(x)$)<deg($p(x)$). Substituting α gives $r(\alpha) = 0$. But as we have seen in the example that the elements in the field are represented as polynomials in α of degree $\leqslant m-1$. Thus $r(x)$ is the zero polynomial. □

In the above proof by using the result in Corollary 21 that $\alpha^{q^n} - 1 = \alpha$ rather than $\alpha^q = 1$ for all $\alpha \in \mathrm{GF}(q)$ we obtain the following result.

Theorem 25. *If $f(x) \in GF(q)[x]$ is an irreducible polynomial of degree m, then*

$$f(x) \mid (x^{q^k} - x)$$

for any k such that $m \mid k$.

Definition 26. An irreducible polynomial $p(x) \in \mathrm{GF}(p)[x]$ of degree m is said to be a **primitive polynomial** if the smallest integer n for which $p(x)$ divides $x^n - 1$ is $n = p^m - 1$.

Let's assume we constructed $\mathrm{GF}(p^m)$ using the irreducible polynomial $p(x)$ and let α be the root of $p(x)$ in $\mathrm{GF}(p^m)$. We know $\alpha^{p^m-1} = 1$. If the polynomial $p(x)$ is not primitive then there exists $n < p^m - 1$ such that $p(x)|x^n - 1$ which implies $\alpha^n = 1$. This would mean the order of α is less than $p^m - 1$ and hence α is not a primitive element. This is intuition behind the Definition 26 of primitive polynomial. In fact we have a stringer relation between primitive polynomials and primitive elements in a Galois Field.

Theorem 27. *The roots of an mth degree primitive polynomial $p(x) \in GF(p)[x]$ are primitive elements in $GF(p^m)$.*

We will skip the proof of this theorem since it requires a result from subsequent section.

Lets' recollect that all the elements of the field can be **generated as powers of the roots of primitive polynomial.**

5 Conjugate Elements and Minimal Polynomials

Even when we are working over a higher field, say $\mathrm{GF}(q^m)$, it is desirable that we have the generator polynomial over the base field $\mathrm{GF}(q)$. In this section we see how do we obtain polynomials that have coefficients in base field but the roots in a larger field. This is analogous to the polynomial $x^2 + 1$ being from $\mathbb{R}[x]$ but the roots are in $\mathbb{C}$. As we know the roots $+i, -i$ are called conjugate elements.

Theorem 28. *Let $GF(q) = GF(p^r)$ for some $r \geqslant 1$. Let $f(x) = \sum_1^d f_j x^j \in GF(q)[x]$. That is $f_j \in GF(q)$. Then*

$$f(x^{q^n}) = [f(x)]^{q^n}.$$

for any $n \geqslant 0$.

Proof.

$$\begin{aligned}[f(x)]^{q^n} &= \left[\sum_{1}^{d} f_j x^j\right]^{q^n} \\ &= \sum_{1}^{d} f_j^{q^n} (x^j)^{q^n} \\ &= \sum_{1}^{d} f_j (x^{q^n})^j \\ &= f(x^{q^n}).\end{aligned}$$

□

Thus if $\beta \in \mathrm{GF}(q^m)$ is a root of $f(x) \in \mathrm{GF}(q)[x]$ then β^{q^n} is also a root of $f(x)$.

Definition 29. Let $\beta \in \mathrm{GF}(q^m)$.The conjugates of β with respect to a subfield $\mathrm{GF}(q)$ are $\beta, \beta^q, \beta^{q^2}, \ldots,$. The conjugates of β with respect to $\mathrm{GF}(q)$ form a set called the **conjugacy class** of β with respect to $\mathrm{GF}(q)$.

Definition 30. Let $\beta \in \mathrm{GF}(q^m)$. The **minimal polynomial** of β with respect to $\mathrm{GF}(q)$ is the smallest degree, non-zero, monic polynomial $p(x) \in \mathrm{GF}(q)[x]$ such that $p(\beta) = 0$.

Theorem 31. *Let $\beta \in GF(q^m)$ have order n and let $\{\beta, \beta^q, \beta^{q^2}, \ldots, \beta^{q^d}\}$ be the conjugacy class of β with respect to $GF(q)$. Then the coefficients of the polynomial $p(x) = \prod_{i=1}^{d}(x - \beta^{q^i})$ are in $GF(q)$. Furthermore $p(x)$ is irreducible. That is, $p(x)$ is **minimal polynomial** for β.*

6 Factoring $x^n - 1$

We come to the question of critical importance to us: Factorization of $x^n - 1$. We now have the necessary tools. Let's assume $n = q^m - 1$. Then all the $q^m - 1$ elements in $\mathrm{GF}(q^m)\backslash\{0\}$ are roots of $x^n - 1$. Therefore

$$x^n - 1 = \prod_{1}^{q^m-1} (x - \alpha^i)$$

where α is a primitive element in $\mathrm{GF}(q^m)$. Now to obtain factors from $\mathrm{GF}(q)[x]$ rather than $\mathrm{GF}(q^m)[x]$ we group the linear factors above according to the conjugacy classes and we end up with factors from $\mathrm{GF}(q)[x]$ (see Theorem 31).

To the case when $n \neq q^m - 1$. Then we find q, m such that $n \mid (q^m - 1)$. This guarantees the existence of an element β of order n in $\mathrm{GF}(q^m)$. If β is a root of $x^n - 1$ then so are the elements $1, \beta^2, \beta^3, \ldots, \beta^{n-1}$. Thus

$$x^n - 1 = \prod_{0}^{n-1} (x - \beta^i).$$

Now we group the factors according to their conjugacy classes and we obtain factors from $\mathrm{GF}(q)[x]$.

References

[1] T. K. Moon, *Error Correction Coding: Mathematical Methods and Algorithms.* John Wiley & Sons, Inc., 2005.