ELG 5372 Error Control Coding

Lecture 4: Algebra 2: Fields and Polynomials

Fields

- A field is a set of elements on which we can perform addition, subtraction, multiplication and division without leaving the set.

Formal Definition of a Field

- Let *F* be a set of elements on which two binary operations called addition '+' and multiplication '×' are defined. The set is a field under these two operations if the following conditions are satisfied:
  1. *F* is a commutative group under addition. The identity element with respect to addition is called the zero element of F and is denoted by 0.
  2. The nonzero elements of *F* {{*F*}-0} form a commutative group under multiplication. The multiplicative identity is termed the unity element in *F* and is denoted by 1.
  3. Multiplication is distributive over addition. In other words, for a, b, c in F, $a \times (b+c) = a \times b + a \times c$.

Some Notation

- For a in F, $-a$ is the additive inverse of a.
  - Example: in GF(3) if a =1, $-a$ = 2.
- For a in F, $1/a$ is the multiplicative inverse of a.
  - Example: in GF(3) if a = 2, $1/a$ = 2.
- This will become evident as we progress through the lecture.

Properties of Fields

1. For every element a in F, $a \times 0 = 0 \times a = 0$.
2. For every two non-zero elements a, b in F, $a \times b \neq 0$.
3. For a, b in F, $a \times b = 0$ for $a \neq 0$ implies $b = 0$.
4. For any two elements in a field $-(a \times b) = (-a) \times b = a \times (-b)$.
5. For $a \neq 0$, $a \times b = a \times c$ implies that $b = c$.

Galois Field 2 (GF(2)): The Binary Field

- A binary field can be constructed under modulo-2 addition and modulo-2 multiplication.

+	0	1
0	0	1
1	1	0

Modulo-2 Addition

×	0	1
0	0	0
1	0	1

Modulo-2 Multiplication

GF(p)

- Using the same idea as GF(2), we can generate any Galois field with a prime number, p, of elements over modulo-p addition and multiplication.

Example GF(3)

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Modulo-3 Addition

×	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Modulo-3 Multiplication

Extension Fields GF(p^m)

- We cannot construct finite fields simply by using modulo arithmetic.
- For example, GF(4) is not 0,1,2,3 using modulo-4 addition and multiplication.
- GF(4) can be constructed by considering it as 2 dimensional GF(2).
- GF(4)={(0,0), (0,1), (1,0), (1,1)}.
- We say that GF(4) is an extension field of GF(2).

Characteristic of a Field

- Consider a finite field of q elements, GF(q).
- Let $t_k = \sum_{i=1}^{k} 1$.
- Let λ be the smallest value of k for which t_k = 0.
- Then λ is called the characteristic of the field GF(q).
- For example, in GF(2), λ = 2 (since 1+1 = 0). In GF(3), 1+1+1 = 0, thus λ = 3.

Theorem 5

- The characteristic of a field is always a prime number.

Order of an element in GF(q)

- Suppose α is a nonzero element in GF(q).
- Since the non-zero elements in a field form a closed set under multiplication, then α^2, α^3, α^4 … are also elements in GF(q).
- The order of element α in GF(q) is the smallest integer, ord(α), for which $\alpha^{\mathrm{ord}(\alpha)} = 1$.

Example GF(3)

- GF(3)={0,1,2}
- 1: $1^1 = 1$, therefore ord(1) = 1.
- 2: $2^1 = 2$, $2^2 = 4 \bmod 3 = 1$, therefore ord(2) = 2.

Theorem 6

- Let α be a non-zero element in GF(q). Then $\alpha^{q-1} = 1$.

Theorem 7

- Let α be an element in GF(q). Then ord(α) divides q-1. (ord(α)|q-1)

Primitive Elements

- Any element in GF(q) whose order is q-1 is a primitive element of GF(q).
  - For example, in GF(3), element 2 has order 2. Thus 2 is a primitive element of GF(3).
- Let α be a primitive element in GF(q), then the series $\alpha^1, \alpha^2, \ldots, \alpha^{q-1}$ produces q-1 distinct non-zero elements in GF(q).
- In other words, **the q-1 successive powers of a primitive element α produce all of the non-zero elements in GF(q). Thus GF(q) = $\{0, \alpha, \alpha^2, \ldots, \alpha^{q-1}\}$.**

Example GF(4)

- $0 = (0,0)$, $1 = (0,1)$, $\alpha = (1,0)$ and $\alpha^2 = (1,1)$.
- In other words, $\alpha^2 = \alpha+1$ (*).
- If α is the primitive, then $\mathrm{ord}(\alpha) = 3$.
- $\alpha^3 = \alpha^2\alpha = (\alpha+1)\alpha = \alpha^2+\alpha = \alpha+1+\alpha = (1,0)+(0,1)+(1,0) = (1+0+1,0+1+0) = (0,1)$.
- Primitive element is defined by (*).
- How do we define the primitive of a field?
- Special type of polynomial: primitive polynomial.

Polynomials over GF(q)

- The polynomial $f(X) = f_0 + f_1X + f_2X^2 + \ldots + f_nX^n$ is a polynomial of degree n over GF(q) if the coefficients f_i come from GF(q) and obey GF(q) arithmetic.
- Suppose $f(X)$ and $g(X)$ are two polynomials over GF(q) and are given by (assume $m<n$):

$$\begin{aligned} f(X) &= f_o + f_1 X + \ldots + f_n X^n \\ g(X) &= g_o + g_1 X + \ldots + g_m X^m \end{aligned}$$

Addition of polynomials

$$f(X)+g(X)=(f_o+g_o)+(f_1+g_1)X+\ldots+(f_m+g_m)X^m$$
$$+f_{m+1}X^{m+1}+\ldots+f_nX^n$$

Where all additions are performed as defined in GF(q)

Multiplication of polynomials

- $f(X)g(X) = c_0 + c_1X + \ldots\ c_{n+m}X^{n+m}$

$$
\begin{array}{rcl}
c_0 & = & f_0 g_0 \\
c_1 & = & f_0 g_1 + f_1 g_0 \\
c_2 & = & f_0 g_2 + f_1 g_1 + f_2 g_0 \\
\vdots & \vdots & \vdots \\
c_{n+m} & = & f_n g_m
\end{array}
$$

Examples

- Polynomials in GF(2)

$$f(X) = 1 + X + X^3$$
$$g(X) = 1 + X^2$$

- $f(X)+g(X) = (1+1) + (1+0)X + (0+1)X^2 + (1+0)X^3 = X + X^2 + X^3$
- $f(X)g(X) = (1+X+X^3) \times (1+X^2) = 1 + X^2 + X + X^3 + X^3 + X^5 = 1 + X + X^2 + (1 + 1)X^3 + X^5 = 1 + X + X^2 + X^5$.

Examples

- Polynomials in GF(4)

$$f(X) = 1 + \alpha X + \alpha X^2$$
$$g(X) = 1 + \alpha^2 X$$

Properties of Polynomials over GF(q)

Commutative

$$a(X) + b(X) = b(X) + a(X)$$

$$a(X)b(X) = b(X)a(X)$$

Associative

$$a(X) + [b(X) + c(X)] = [a(X) + b(X)] + c(X)$$

$$a(X)[b(X)c(X)] = [a(X)b(X)]c(X)$$

Distributive

$$a(X)[b(X) + c(X)] = a(X)b(X) + a(X)c(X)$$

Polynomial Division

- When we divide *f*(*X*) by *g*(*X*), we get two new polynomials; *q*(*X*) is the quotient and *r*(*X*) is the remainder.
- The degree of the remainder, *r*(*X*) is smaller than the degree of *g*(*X*).

$$
\begin{array}{r|l}
 & X^2 \qquad\qquad\qquad +1 \\
\cline{2-2}
X^3+1 & X^5 + \qquad\qquad\qquad + X^2 \qquad + 1 \\
 & \underline{X^5 \qquad\qquad + X^3 \qquad\qquad\qquad} \\
 & \qquad\qquad\qquad X^3 + X^2 \qquad + 1 \\
 & \qquad\qquad\qquad \underline{X^3 + \qquad\qquad + 1} \\
 & \qquad\qquad\qquad\qquad X^2
\end{array}
$$