Coding and Information Theory

This is the second lecture on Mathematical Fundamentals (B)

Dr. Xuejun Liang

Quick Review of Last Lecture

- Modular Arithmetic
- Group and Examples
- Euclidean Theorem
    - The Euclidean Algorithm
    - The Extended Euclidean Algorithm
    - Examples
- Field

Field

- A set F is a Field
  - At least two elements $0, 1 \in F$
  - Two operations $+$ and $\times$ on F
  - Associative and commutative
  - Operation $\times$ distributes over $+$
  - 0 is the identity for $+$ and 1 for $\times$
  - Additive inverse and multiplicative inverse

Order of Field: The number of elements in a field is known as the *order* of the field. A field having finite number of elements is called a *finite field.*

Property 1: For every element a in a field, $a \times 0 = 0 \times a = 0$.

Property 2: For any two nonzero elements a and b in a field, $a \times b \neq 0$.

Property 3: For $a \neq 0$, $a \times b = a \times c$ implies that $b = c$.

Finite Field Examples

$(Z_7, +, \times, 0, 1)$ is a Field

Example:
Evaluate $((2 - 4) \times 4)/3$ in the field Z_7

[+]	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

[·]	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

- $(Z_p, +, \times, 0, 1)$ is a Field (when p is a prime number.)
  - $+, \times$ are closed
  - $+, \times$ are associative and commutative
  - Operation $\times$ distributes over $+$
  - 0 is the identity for $+$ and 1 for $\times$
  - Additive inverse and multiplicative inverse

Extension Field

Let $f(x)=2x^3+x^2+2$ and $g(x) = x^2+2 \in Z_3[x]$

$f(x)+g(x) =$

$f(x)-g(x) =$

$f(x)g(x) =$

$f(x)/g(x) =$

Goal: Given a prime p and a positive integer n, construct a field with p^n elements.

Definitions and Notations:

$Z_p[x]$: all polynomials in the indeterminate x with coefficients in Z_p.

deg(f) : the degree of f ($f \in Z_p[x]$) is the largest exponent in a term of f.

$f \mid g$: f divides g ($f, g \in Z_p[x]$), if $g = f \cdot h$ for some $h \in Z_p[x]$.

$g \equiv h \pmod{f}$: $f \mid (g - h)$ ($f, g, h \in Z_p[x]$ and def(f)≥ 1)

$Z_p[x]/(f)$: all congruence classes modulo f in $Z_p[x]$ ($f \in Z_p[x]$).

$Z_p[x]/(f)$ is equipped with $+$, $\times$ and $| Z_p[x]/(f) | = p^n$, where n=deg(f)

Example: $Z_3[x]/(x^2-1)$

(1) List all the elements in forms $a_0 + a_1x$, $a_0, a_1 \in Z_3$.

(2) List a complete multiplication table.

$Z_3[x]/(x^2-1)$

$= \{0 + 0x, 0 + 1x, 0 + 2x, 1 + 0x, 1 + 1x, 1 + 2x, 2 + 0x, 2 + 1x, 2 + 2x\}$

$= \{0, 1, 2, x, 2x, 1 + x, 1 + 2x, 2 + x, 2 + 2x\}$

	1	2	*x*	2*x*	1+x	1+2x	2+*x*	2+2*x*
1	1	2	*x*	2*x*	1+x	1+2x	2+*x*	2+2*x*
2	2							
x	*x*							
2*x*	2*x*							
1+x	1+x							
1+2*x*	1+2*x*							
2+*x*	2+*x*							
2+2*x*	2+2*x*							

Extension Fields (Cont.)

In general $Z_p[x]/(f)$ is a ring, not a field.

Definition: A polynomial f in $Z_p[x]$ is called irreducible, if f can not be written as $f = f_1 \cdot f_2$ where $\deg(f_1)>0$ and $\deg(f_2)>0$.

Fact: If f in $Z_p[x]$ is irreducible polynomial of degree n, then $Z_p[x]/(f)$ is a field with p^n elements.

Notation: $Z_p[x]/(f)$ is called Galois field and is denoted by $GF(p^n)$.

Example: $GF(2^3) = Z_2[x]/(x^3+x+1)$

(1) List all the elements in forms $a_0 + a_1x + a_2x^2$, $a_0, a_1, a_1 \in Z_2$.

(2) Compute $(x^2 + 1) \times (x^2 + x + 1)$.

$Z_2[x]/(x^3+x+1)$

$= \{0 + 0x + 0x^2, 0 + 0x + 1x^2, 0 + 1x + 0x^2, 1 + 0x + 1x + 1x^2, 1 + 1x + 1x^2\}$

$= \{0, 1, x, 1 + x, x^2, 1 + x^2, x + x^2, 1 + x + x^2\}$

Linear (vector) space: Definition

A linear space V over a field F is a set whose elements are called vectors and where two operations, addition and scalar multiplication, are defined:

1. **addition**, denoted by $+$, such that to every pair $x, y \in V$ there correspond a vector $x + y \in V$, and
   - $x + y = y + x$,
   - $x + (y + z) = (x + y) + z$, $x, y, z \in V$;

   $(X, +)$ is a group, with identity element denoted by 0 and inverse denoted by $-$, $x + (-x) = x - x = 0$.
2. **scalar multiplication** of $x \in V$ by elements $k \in F$, denoted by $kx \in V$, and
   - $k(ax) = (ka)x$,
   - $k(x + y) = kx + ky$,
   - $(k + a)x = kx + ax$, $x, y \in V$, $k, a \in F$.

   Moreover $1x = x$ for all $x \in V$, 1 being the unit in F.

Example: V_4 of all 4-tuples over Z_2 (GF(2)).

Subspace and Linearly independent

- Subspace: $S \subseteq V$
  - addition and scalar multiplication are closed in S
- Linear combination
  - $a_1v_1+a_2v_2+ \ldots + a_nv_n$
  - Linearly independent of $v_1, v_2, \ldots, v_n$
    - If $a_1v_1+a_2v_2+ \ldots + a_nv_n = 0$ then $a_1=0, a_2=0, \ldots, a_n=0$.
  - Linearly dependent of $v_1, v_2, \ldots, v_n$
    - There are $a_1, a_2, \ldots, a_n$ (not all 0's) such that

$$a_1v_1+a_2v_2+ \ldots + a_nv_n = 0$$