Lecture Notes

Advanced Discrete Structures

COT 4115.001 S15

2015-02-17

Recap

- DES
  - DES is not a group

Group $(G,*)$

A **group** is a set G equipped with a binary operation $*$ that satisfies the axioms:

1. Closure: if $a \in G$ and $b \in G$, then $a * b \in G$
2. Associativity: $a * (b * c) = (a * b) * c$

   for all $a, b, c \in G$
3. Identity: there is an $1_G \in G$ such that

   $$a * I_G = a$$

   for all $a \in G$
4. Inverse: for each $a \in G$, there is an $a^{-1} \in G$ such that

   $$a * a^{-1} = I_G$$

A group is call **Abelian** if it has the additional property:

5. Commutativity: $a * b = b * a$ for all $a, b \in G$

Example of a Group

- $(\mathbb{Z}, +)$: Integers with addition
  - $3 \in \mathbb{Z}$ and $5 \in \mathbb{Z}$, so $3 + 5 = 8 \in \mathbb{Z}$
  - $3 + (4 + 5) = (3 + 4) + 5$
  - 0 is the group identity, e.g., $3 + 0 = 3$
  - Each element has an inverse, e.g., the inverse of 4 is -4 since
  $$4 + (-4) = 0$$

- $(\mathbb{Z}, \cdot)$: Integers with multiplication

Basic Number Theory - Section 3.11

FINITE FIELDS

Field $(F, +, \cdot)$

A **field** is a set F equipped with two operations (usually denoted $+$ and $\cdot$) that satisfy the following axioms:

1. Closure: for all $a, b \in F$ both $a + b \in F$ and $a \cdot b \in F$

2. Associativity: for all $a, b, c \in F$ both
$$a + (b + c) = (a + b) + c \quad \text{and} \quad a \cdot (b \cdot c) = (a \cdot b) \cdot c$$

3. Commutativity: for all $a, b \in F$ both
$$a + b = b + a \quad \text{and} \quad a \cdot b = b \cdot a$$

4. Identities: there exists distinct 0_F and 1_F such that
$$a + 0_F = a \quad \text{and} \quad a \cdot 1_F = a$$

5. Inverses: for all $a \in F$, there exists $-a \in F$ and $a^{-1} \in F$ $(a \neq 0_F)$ s.t.
$$a + (-a) = 0_F \quad \text{and} \quad a \cdot a^{-1} = 1_F$$

6. Distributivity: for all $a, b, c \in F$
$$a \cdot (b + c) = (a \cdot b) + (a \cdot c)$$

Galois Field

A field with *finitely* many elements is called a **finite** or **Galois field**.

<u>Example</u>:

$F = \{0,1,2,3,4\}$,

$\oplus$: addition $(\mathbf{mod}\ 5)$

$\otimes$: multiplication $(\mathbf{mod}\ 5)$

$$(3 \oplus 2) \otimes 4 = 0 \otimes 4 = 0$$
$$(3 \otimes 4) \oplus (2 \otimes 4) = 2 \oplus 3 = 0$$

Theorems

1. Each finite field has p^n elements for some prime p.

2. For each prime p and $n \in \mathbb{N}$, there exists a field with p^n elements.

3. If two finite fields have the same number of elements, then they are the same (up to "isomorphism").

Note

The elements of the finite field are ***not*** $\mathbb{Z}_{p^n}$ since

$$p\,x \equiv 1 \pmod{p^n}$$

has no solution, i.e., p does not have an inverse.

Example

$$GF(2^2) = \{0,1,\omega,\omega^2\}$$

with the rules:

1. $0 + x = x$ for all x
2. $x + x = 0$ for all x
3. $1 \cdot x = x$ for all x
4. $\omega + 1 = \omega^2$
5. $+$ and $\cdot$ are commutative, associative, and distributivity holds

Example

$$GF(2^2) = \{0,1,\omega,\omega^2\}$$

with the rules:

$+$	0	1	ω	ω^2
0	0	1	ω	ω^2
1	1	0	ω^2	ω
ω	ω	ω^2	0	1
ω^2	ω^2	ω	1	0

$\cdot$	0	1	ω	ω^2
0	0	0	0	0
1	0	1	ω	ω^2
ω	0	ω	ω^2	1
ω^2	0	ω^2	1	ω

$$\omega^3 = \omega \cdot \omega^2 = \omega \cdot (\omega + 1) = \omega^2 + \omega = (\omega + 1) + \omega = 1$$

Notation

The set of polynomials whose coefficients are integers mod p is denoted as $\mathbb{Z}_p[X]$.

<u>Example</u>:

$$4X^6 + 3X^5 + X^2 + 2X + 4 \in \mathbb{Z}_5[X]$$

$$4X^6 + 3X^5 + X^2 + 2X + 4 \in \mathbb{Z}_5[X]$$

Polynomial Arithmetic

Addition / Subtraction:

$$(3x^2 + 4x + 2) + (4x^3 - 3x + 5)$$
$$= 4x^3 + 3x^2 + x + 7$$

Multiplication:

$$\begin{aligned}
&(x - 7)(2x^2 + 7x + 3) \\
&\quad = x\,(2x^2 + 7x + 3) - 7\,(2x^2 + 7x + 3) \\
&\quad = (2x^3 + 7x^2 + 3x) - (14x^2 + 49x + 21) \\
&\quad = 2x^3 - 7x^2 - 46x - 21
\end{aligned}$$

Basic Number Theory - Section 3.11.1

DIVISION

Division Algorithm (for Polynomials)

Let F be a field and $f(x), g(x) \in F[x]$ with $g(x) \neq 0_F$. Then there exist unique polynomials $q(x)$ and $r(x)$ such that

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

and either

$$r(x) = 0_F \quad \text{or} \quad \deg r(x) < \deg g(x).$$

Example (Long Division)

$$
\begin{array}{r|l}
 & \quad\quad\quad\quad\quad\quad 2x^2 - x - 14 \\
\cline{2-2}
x^2 + 3x + 7 & 2x^4 + 5x^3 - 3x^2 - x + 7 \\
 & -(2x^2)(x^2 + 3x + 7) \\
 & -2x^4 - 6x^3 - 14x^2 \\
\cline{2-2}
 & \quad\quad -x^3 - 17x^2 - x + 7 \\
 & \quad -(-x)(x^2 + 3x + 7) \\
 & \quad\quad +x^3 + 3x^2 + 7x \\
\cline{2-2}
 & \quad\quad\quad -14x^2 + 6x + 7 \\
 & \quad\quad -(-14)\,(x^2 + 3x + 7) \\
 & \quad\quad\quad +14x^2 + 42x + 98 \\
\cline{2-2}
 & \quad\quad\quad\quad\quad\quad 48x + 105
\end{array}
$$

Division Example

$$2x^4 + 5x^3 - 3x^2 - x + 7$$

$$= (2x^2 - x - 14)(x^2 + 3x + 7) + (48x + 105)$$

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

$$\deg g(x) > \deg r(x)$$

$$2x^4 + 5x^3 - 3x^2 - x + 7 \equiv 48x + 105 \pmod{x^2 + 3x + 7}$$

Divisibility

Let F be a field and $f(x), g(x) \in F[x]$ with $f(x) \neq \mathbf{0}$. We say that $f(x)$ *divides* $g(x)$, or $f(x)$ is a *factor* of $g(x)$, and write

$$f(x) \mid g(x),$$

if $g(x) = h(x)f(x)$ for some $h(x) \in F[x]$.

Reducibility

Let F be a field. A non-constant polynomial $f(x) \in F[x]$ is said to be *reducible* if it can be factored into two non-constant polynomials $p(x), q(x) \in F[x]$.

A non-constant polynomial which is not reducible over the field F is called *irreducible* over F.

Reducibility

<u>Example</u>:

$$6x^2 + 31x + 35 = (3x + 5)(2x + 7)$$

is reducible over the field $(\mathbb{Z}, +, \cdot)$, but

$$x^2 + 1$$

is irreducible over this field. However,

$$x^2 + 1 = x^2 - (-1)^2 = (x + \mathbb{i})(x - \mathbb{i})$$

which means $x^2 + 1$ is reducible over the field $(\mathbb{C}, +, \cdot)$.

Constructing $GF(p^n)$

General procedure to construct a finite field with p^n elements, where p is prime and $n \geq 1$:

1. Pick $P(X)$ to be an irreducible polynomial $(\bmod p)$ of degree n.

2. Then $GF(p^n) = \mathbb{Z}_p[X] \pmod{P(X)}$.

Example: $GF(2^2)$

1. Choose a polynomial of degree 2 that is irreducible over $\mathbb{Z}_2$.

Note:

$$X^2 + 1 \equiv X^2 + 2X + 1 = (X+1)^2 \in \mathbb{Z}_2[X]$$

So $X^2 + 1$ is reducible over $\mathbb{Z}_2$. However,

$$X^2 + X + 1$$

is irreducible over $\mathbb{Z}_2$.

Example: $GF(2^2)$

2. The Galois field $GF(2^2)$ consists of $\mathbb{Z}_2[X]$, i.e., $\{0,1,X,X+1\}$ taken $\pmod{X^2+X+1}$.

$+$	0	1	X	$X+1$
0	0	1	X	$X+1$
1	1	0	$X+1$	X
X	X	$X+1$	0	1
$X+1$	$X+1$	X	1	0

$\cdot$	0	1	X	$X+1$
0	0	0	0	0
1	0	1	X	$X+1$
X	0	X	$X+1$	1
$X+1$	0	$X+1$	1	X

Compare this to what we had before:

$$\omega = X, \qquad \omega^2 = \omega + 1 = X + 1$$

Inverse

Consider the finite field:

$$GF(2^8) = \mathbb{Z}_2[X] \ (\mathrm{mod}\ X^8 + X^4 + X^3 + X + 1)$$

- Since $X^7 + X^5 + X^2 + 1$ is not $\mathbf{0}$, it should have an inverse.
- Use the Extended Euclidean Algorithm to compute this

Inverse

$$X^8 + X^4 + X^3 + X + 1 \equiv (X)\,(X^7 + X^5 + X^2 + 1) + (X^6 + X^4 + 1)$$

$$X^7 + X^5 + X^2 + 1 \equiv (X)\,(X^6 + X^4 + 1) + (X^2 + X + 1)$$

$$X^6 + X^4 + 1 \equiv (X^4 + X^3 + X^2 + 1)\,(X^2 + X + 1) + (X)$$

$$X^2 + X + 1 \equiv (X + 1)\,(X) + (1)$$

$$X \equiv (X)\,(1) + 0$$

$\gcd(X^8 + X^4 + X^3 + X + 1, X^7 + X^5 + X^2 + 1) = 1$ in $\mathbb{Z}_2[X]$

- Reverse the process to find the inverse.

Inverse

$$1 \equiv (1)(X^2 + X + 1) + (X + 1)(X)$$

$$\equiv (1)(X^2 + X + 1) + (X + 1)[(X^6 + X^4 + 1) + (X^4 + X^3 + X^2 + 1)\ (X^2 + X + 1)]$$

$$\equiv (X^5 + X^2 + X)(X^2 + X + 1) + (X + 1)(X^6 + X^4 + 1)$$

$$\equiv (X^5 + X^2 + X)\ [(X^7 + X^5 + X^2 + 1) + (X)\ (X^6 + X^4 + 1)] + (X + 1)(X^6 + X^4 + 1)$$

$$\equiv (X^5 + X^2 + X)(X^7 + X^5 + X^2 + 1) + (X^6 + X^3 + X^2 + X + 1)(X^6 + X^4 + 1)$$

$$\begin{aligned}\equiv\ & (X^5 + X^2 + X)(X^7 + X^5 + X^2 + 1) \\ & + (X^6 + X^3 + X^2 + X + 1)[(X^8 + X^4 + X^3 + X + 1) + (X)\ (X^7 + X^5 + X^2 + 1)]\end{aligned}$$

$$\begin{aligned}\equiv\ & (X^7 + X^5 + X^4 + X^3)(X^7 + X^5 + X^2 + 1) \\ & + (X^6 + X^3 + X^2 + X + 1)(X^8 + X^4 + X^3 + X + 1)\end{aligned}$$

Inverse

$$1 \equiv (X^7 + X^5 + X^4 + X^3)(X^7 + X^5 + X^2 + 1) + (X^6 + X^3 + X^2 + X + 1)(X^8 + X^4 + X^3 + X + 1)$$

which means

$$1 \equiv (X^7 + X^5 + X^4 + X^3)(X^7 + X^5 + X^2 + 1) \pmod{X^8 + X^4 + X^3 + X + 1}$$

Hence,

$$\left(X^7 + X^5 + X^2 + 1\right)^{-1} \equiv X^7 + X^5 + X^4 + X^3 \left(\mathrm{mod}\ \ X^8 + X^4 + X^3 + X + 1\right)$$

Basic Number Theory - Section 3.11.2

GF(2^8)

$GF(2^8)$

- We've shown that the finite field is given by

$$\mathbb{Z}_2[X] \pmod{X^8 + X^4 + X^3 + X + 1}$$

- Every element can be represented uniquely as a polynomial

$$b_7X^7 + b_6X^6 + b_5X^5 + b_4X^4 + b_3X^3 + b_2X^2 + b_1X + b_0$$

  where each b_i is 0 or 1.

- The 8 bits $b_7b_6b_5b_4b_3b_2b_1b_0$ represent a byte, so elements of $GF(2^8)$ may be represented as a byte

$GF(2^8)$ Arithmetic

- <u>**Addition**</u>: XOR of the bits

$$(X^6 + X^5 + X^2 + X + 1) + (X^7 + X^2 + X)$$

$$01100111 \oplus 10000110 = 11100001$$

- <u>**Multiplication**</u>: Consider

$$(X^6 + X^5 + X^2 + X + 1)(X^2)$$

$$\equiv (X^8 + X^7 + X^4 + X^3 + X^2) + (X^8 + X^4 + X^3 + X + 1)$$

$$\equiv X^7 + X^2 + X + 1 \pmod{X^8 + X^4 + X^3 + X + 1}$$

$GF(2^8)$ Arithmetic

- **<u>Multiplication</u>**: Consider

$$(X^6 + X^5 + X^2 + X + 1)(X^2)$$

$$\equiv (X^8 + X^7 + X^4 + X^3 + X^2) + (X^8 + X^4 + X^3 + X + 1)$$

$$\equiv X^7 + X^2 + X + 1 \pmod{X^8 + X^4 + X^3 + X + 1}$$

In binary:

$$01100111 \rightarrow 0110011100 \oplus 0100011011$$

$$\rightarrow 0010000111 = 10000111$$

Multiplication by X^m

1. Shift left, i.e., append m 0s to the end of the byte
2. If the first m bits are 0, then truncate the first m bits and stop.
3. If any of the first m bits are 1, XOR the appropriate multiple of 100011011 to cancel the first 1.
   - Repeat until the first m bits are 0. Go to 2.

Multiplication

Recall:

$$(X^2 + X + 1)(X^5 + X^3 + X^2) =$$
$$X^2\,(X^5 + X^3 + X^2) + X\,(X^5 + X^3 + X^2) + (X^5 + X^3 + X^2)$$

- Arbitrary multiplication can be performed

Comparison

$\mathbb{Z}$	$\leftrightarrow$	$\mathbb{Z}_p[X]$
prime q	$\leftrightarrow$	irreducible $P(X)$ of degree n
$\mathbb{Z}_q$	$\leftrightarrow$	$\mathbb{Z}_p[X]$
field with q elements	$\leftrightarrow$	field with p^n elements