Review of elementary Group Algebra for Coding Theory

Andersen Ang

First created: 2013-Nov. Last update: 2017-Feb-1

Reviews on algebra

Review on what is "close"

Let a set of elements called S , a binary operation $\circ$ on S is definding how to operate a pair of elements $a, b \in S$: $a \circ b$

If the result of the operation $a \circ b$, denoted as c (i.e. $a \circ b = c$), is also the member in S ($c \in S$), then the operation $\circ$ is said to be *close* in S

$$\text{Symbolically , } \circ \text{ is} close \text{ if} a, b \in S \Rightarrow c \in S \text{ for} c = a \circ b$$

Review on what is "group"

A set G with operation $\circ$, together denoted as $(G, \circ)$ is called a *group* if

1. $\circ$ is associative : $a \circ (b \circ c) = (a \circ b) \circ c$
2. G has one and only one (exactly one) *identiy element* e (i.e. $e \circ a = a \circ e = a \; \forall a \in G$)
3. Inverse. $\forall a \in G$, $\exists! b \in G \; s.t. \; b = a^{-1}$ or $a \circ b = e$

Review of abelian group

A group G is abelian group if $\circ$ is commutative in G ($a \circ b = b \circ a$)

Review of cardinality

The cardinality is the number of element of the group , denoted as $|G|$ or $card(G)$

Review of finite group and infinite group

G is finite if $|G| < \infty$, G is infinite if $|G| = \infty$

Review of fields

A set F , with operation $\circ$ and $\cdot$ (2 operations) , denoted as $(F, \circ, \cdot)$, is a $field$ if

1. F is abelian group under $\circ$ (the identity is denoted by 0)
2. The set of non-zero elements in S is a abelian group under $\cdot$ (the identity is denoted by 1)
3. $\cdot$ is distributive over $\circ$ ($a \cdot (b \circ c) = a \cdot b + a \cdot c$)

Notice that

$\min |F| = 2$ (min number of element of a field F is 2), the 2 element is 1 and 0

the operation $\circ$ is called *addition* , $\cdot$ is called *multiplication*, and thus 1 is the multiplicative identity, 0 is the additive identity

the $additiveinverse$ of a is $-a$, therefore we can **define subtraction** by $a - b = a + (-b)$ (subtract an element is same as adding it's additive inverse !)

the *multiplicative inverse* of a is a^{-1} , therefore we can **define division** by $a \div b = a \cdot b^{-1}$ (divide an element is same as multiply it's multiplicative inverse !)

Review on Galois Field

For field F s.t. $|F| < \infty$ (Field F has finite elements) , the field F is called *Galois Field*

Galois Fields

The set $\{0, 1\}$ called binary Galois field is a field of order 2 under modulo-2 addition and modulo-2 multiplication

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

The set {0,1,2,...,p-1} where p is prime number is a prime Galois field under modulo-p addition and modulo-p multiplication

For example, when $p = 5$

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

∘	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	2	4
3	0	3	2	4	2
4	0	4	3	2	1

Extension Field $GF(p^m)$

$\forall GF(p)$, it is possible to form an extension field $GF(p^m)$, $m \in \mathbb{Z}$(m is integer)

Review of cyclic group

For element a (non-zero) of $GF(p)$, the smallest integer n s.t. $a^n = 1$ is the order of field element a

The group G is *cyclic* if there exists an element whose power constitute the whole group (i.e. all other element is the power of that element)

i.e. $G = \{0, a^n = 1 , a , a^2 , a^3 \dots , a^{n-1}\}$

Then for $GF(q)$ (GF of $q - element$), and n is the order of a, then

$a^{q-1} = 1$

n divides $q - 1$

a is the *primitive element* if its order is $q - 1$

The GF(2)

There are only 2 element inside the GF(2) , they are '0' and '1'

There are 2 operations on GF(2), the additiion (The logic OR operation) and the multiplication (the logic AND operation)

+	0	1
0	0	1
1	1	0

×	0	1
0	0	0
1	0	0

Notice that

$0 + 0 = 0$, $0 + 1 = 1$, and $1 + 0 = 1$ that means $0 + a = a$ and $a + 0 = a$, this measn '0' is the additive identity

Thus, with additive identity, additive inverse can be defined, and the additive inverse of '0' is '0'. (itself)

For the additive inverse of '1', since $1 + 1 = 0$, thus $1 + \underbrace{1 + (-1)}_{cancel} = \underbrace{0 + (-1)}_{=-1\,(0+a=a)}$ and thus $1 = -1$

That means $-1 = 1$ or $-a = +a$ in GF(2), and the additive inverse of '1' is '1' (itself too!)

Notice that

$1 \cdot 1 = 1$, '1' is the multiplicative identity : $1 \cdot a = a$ and $a \cdot 1 = a$ for nonzero element in the set , although there is only 1 nonzero element $a = 1$

With multiplicative identity, multiplicative inverse (division) can be defined , since $1 \cdot 1 = 1$ thus $1 \cdot \underbrace{1 \cdot (1^{-1})}_{cancel} = \underbrace{1 \cdot (1^{-1})}_{=1^{-1}\ (1 \cdot a = a)}$, thus $1 = 1^{-1}$

Therefore the multiplicative inverse of $'1'$ is '1' (itself)

For '0' , there is no multiplicative inverse, since by definition, no element in this set has the following relation with '0' : $a \cdot 0 = 1$, $0 \cdot a = 1$ (such a does not exist !)

Notice that $GF(2)$ has 2 element, $'0'$ and '1' , the number of elements in this set is '2', which is a finite number

$\langle GF(2), +, \cdot \rangle$ also fulfill the *commutative*, *associateive* , *distributive* properties

$\langle GF(2), +, \cdot \rangle$ is thus a finite fields / Galois Field with 2 element

Polynomial over GF(2)

A polynomial over the GF(2) is a polynomial $f(x) = a_0 + a_1 x + a_2 x^2 + ... + a_n x^n$

The degree n is defined as the largest power of x with non-zero coefficient

Operations of 2 polynomial
$f(x) = a_0 + a_1 x + a_2 x^2 + ... + a_n x^n$
$g(x) = b_0 + b_1 x + b_2 x^2 + ... + b_n x^n$

$(f + g)(x) = (a_0 + b_0) + (a_1 + b_1)\, x + (a_2 + b_2)\, x^2 + ... + (a_m + b_m)\, x^m$
$(f \cdot g)(x) = (a_0 b_0) + (a_0 b_1 + a_1 b_0)\, x + (a_0 b_2 + a_1 b_1 + b_0 a_2)\, x^2 + ... + (a_m b_m)\, x^m$
$\left(\frac{f}{g}\right)(x) \iff q(x)g(x) + r(x)$ where degree of remainder $r(x)$ has to be smaller than divider $g(x)$, and $q(x)$ is the quotient

The roots of polynomial over GF(2)

A polynomial $f(x) = f_0 + f_1 x + f_2 x^2 + f_3 x^3 + ... + f_n x^n$ over $GF(2)$ that $f_1, f_2, ..., f_n$ are all either 0 or 1 (elements of GF(2))

n is called the degree of the polynomial

f is *monic* if $f_n = 1$

Theorem $[f(x)]^{2^l} = f\left(x^{2^l}\right)$
Illustration : consider $l = 1$, i.e. $[f(x)]^2 = f\left(x^2\right)$

Expand . $[f(x)]^2$: . $[f(x)]^2 = \left[f_0 + f_1 x + f_2 x^2 + f_3 x^3 + ... + f_n x^n\right]^2 = \left[(f_0) + \left(f_1 x + f_2 x^2 + f_3 x^3 + ... + f_n x^n\right)\right]^2$
By $(a + b)^2 = a^2 + 2ab + b^2$

$$[f(x)]^2 = f_0^2 + 2f_0\left(f_1 x + f_2 x^2 + f_3 x^3 + ... + f_n x^n\right) + \left(f_1 x + f_2 x^2 + f_3 x^3 + ... + f_n x^n\right)^2$$

Since $1 + 1 = 2 = 0$

$$[f(x)]^2 = f_0^2 + \left(f_1 x + f_2 x^2 + f_3 x^3 + ... + f_n x^n\right)^2 = f_0^2 + \left((f_1 x) + \left(f_2 x^2 + f_3 x^3 + ... + f_n x^n\right)\right)^2$$

$$[f(x)]^2 = f_0^2 + (f_1 x)^2 + 2f_1 x\left(f_2 x^2 + f_3 x^3 + ... + f_n x^n\right) + \left(f_2 x^2 + f_3 x^3 + ... + f_n x^n\right)^2$$

$$[f(x)]^2 = f_0^2 + (f_1 x)^2 + \left(f_2 x^2 + f_3 x^3 + ... + f_n x^n\right)^2$$

$$\vdots$$

$$[f(x)]^2 = f_0^2 + (f_1 x)^2 + \left(f_2 x^2\right)^2 + \left(f_3 x^3\right)^2 + ... + (f_n x^n)^2$$

Since f_i are either '0' and '1' and $0 \cdot 0 = 0$ and $1 \cdot 1 = 1$, then $f_i^2 = f_i$

$$[f(x)]^2 = f_0 + f_1(x^2) + f_2(x^2)^2 + f_3(x^2)^3 + ... + f_n\left(x^2\right)^n = f\left(x^2\right)$$

Using same logic, $f(x)^4 = f(x^4)$ ... $f(x)^{2^l} = f(x^{2^l})$

Theorem For $f(x)$, if $f(\alpha) = 0$, then α is the *root* of $f(x)$

With the previous theorems, the following theorems is important
Theorem (Conjugate) If α is the root of $f(x)$, so as α^2 , α^4 , α^8 , ...
Illustration For $f(x)$, if $f(\alpha) = 0$, then :

$$[f(\alpha)]^{2^l} = 0^{2^l} = 0$$

$$\iff f\left(\alpha^{2^l}\right) = 0 \qquad \Rightarrow \alpha^{2^l} \text{ is also a root } : \alpha^2 , \alpha^4 , \alpha^8 , \text{....all are roots}$$

$\alpha^2, \alpha^4, \alpha^8, ...$ are the *conjugate* of α

Irreducible Polynomial

A polynomial $d(x)$ is a factor of $f(x)$ if $f(x) = q(x)d(x)$

$f(x) \in K[x]$ is irreducible over K if it has no factor in K

Examples

$f(x) = 1 + x + x^2$over $GF(2)$ has no factor (x, $1 + x$ are not factor), since $f(0) = 1 \neq 0$ and $f(1) = 1 \neq 0$, so it is irreducible.

$f(x) = 1 + x + x^4$ over $GF(2)$ has on factor , since $f(0) = 1 \neq 0$ and $f(1) = 1 \neq 0$, that means $f(x)$ has an irreducible quadratic factor. The only possible irreducible quadratic factor is $1+x+x^2$, but $Rem\left[\dfrac{1+x+x^4}{1+x+x^2}\right] \neq 0$, that means $1 + x + x^2$ is not a factor of $1 + x + x^4$, so $1 + x + x^4$ is also irreducible.

Note. Polynomial with *even* number of terms must be reducible
e.g. $f(x) = 1 + x^3 + x^5 + x^9$, $f(1) = 1 + 1^3 + 1^5 + 1^9 = 1 + 1 + 1 + 1 = 0$

Primitive Polynomial

Irreducible polynomial with degree n is *primitive* if it is not a factor of $1 + x^m$ that $m < 2^n - 1$
e.g. $1 + x + x^2$, $n = 2$, $2^n - 1 = 3$, $1 + x + x^2$ is not a factor of $1 + x^m = 1 + x^3$, so it is primitive
e.g. $1 + x + x^2 + x^3 + x^4$ is irreducible, but it is a factor of $1 + x^5$ and thus it is not primitive
Primitive element. For $GF(2^m)$, α is a primitive element if all non-zero element can be expressed as a power of α. i.e. the elements of $GF(2^m)$ are $\{0, \alpha^0 = 1, \alpha, \alpha^2, \alpha^3, ..., \alpha^k, ...\}$

Construction of GF(2^m)

Using primitive polynomial $p(x)$, we can construct $GF(2^m)$.
e.g. $p(x) = 1 + x + x^4$, then $GF(2^4)$ can be constructed using α
$p(\alpha) = 0$, so $1 + \alpha + \alpha^4 = 0$, then

word	polynomial	power of α
0000	0	-
1000	1	$\alpha^0 = 1$
0100	α	α
0010	α^2	α^2
0001	α^3	α^3
1100	$\alpha^4 = 1 + \alpha$	α^4
0110	$\alpha^5 = \alpha + \alpha^2$	α^5
0011	$\alpha^2 + \alpha^3$	α^6
1101	$1 + \alpha + \alpha^3$	α^7
1010	$1 + \alpha^2$	α^8
0101	$\alpha + \alpha^3$	α^9
1110	$1 + \alpha + \alpha^2$	α^{10}
0111	$\alpha + \alpha^2 + \alpha^3$	α^{11}
1111	$1 + \alpha + \alpha^2 + \alpha^3$	α^{12}
1011	$1 + \alpha^2 + \alpha^3$	α^{13}
1001	$1 + \alpha^3$	α^{14}

GF(2^m) operation

Using the previous example,
e.g. $\alpha^7 + \alpha^{12} =?$
First we can expand the elements in polynomial form
$\alpha^7 = 1 + \alpha + \alpha^3$
$\alpha^{12} = 1 + \alpha + \alpha^2 + \alpha^3$
Then perform mod-2 addition
$\alpha^7 + \alpha^{12} = \alpha^2$

e.g. $\alpha^7 \cdot \alpha^{12} =?$
By law of index, $\alpha^7\alpha^{12} = \alpha^{19} = \alpha^{15}\alpha^4 = \alpha^4$, since $\alpha^{15} = 1$

Minimal Polynomial

For GF(2^m) , one element in this set, denoted as γ , can form minimal polynomial $m_\gamma(x)$
1. $m_\gamma(x)$ is irreducible over K
2. if polynomial $f(x)$ that $f(\gamma) = 0$, then $m_\gamma(x)$ is a factor of $f(x)$
3. $m_\gamma(x)$ is unique
4. $m_\gamma(x)$ is a factor of $1 + x^{2^m-1}$

In simple words, for an element in an GF(2^m) , the corresponding minimal polynomial is a unique smallest degree irreducible polynomial $m_\gamma(x)$

Construction of minimal polynomial

Consider the GF(16) constructed using primitive polynomial $p(x) = 1 + x + x^4$

word	polynomial	power of α
0000	0	-
1000	1	$\alpha^0 = 1$
0100	α	α
0010	α^2	α^2
0001	α^3	α^3
1100	$\alpha^4 = 1 + \alpha$	α^4
0110	$\alpha^5 = \alpha + \alpha^2$	α^5
0011	$\alpha^2 + \alpha^3$	α^6
1101	$1 + \alpha + \alpha^3$	α^7
1010	$1 + \alpha^2$	α^8
0101	$\alpha + \alpha^3$	α^9
1110	$1 + \alpha + \alpha^2$	α^{10}
0111	$\alpha + \alpha^2 + \alpha^3$	α^{11}
1111	$1 + \alpha + \alpha^2 + \alpha^3$	α^{12}
1011	$1 + \alpha^2 + \alpha^3$	α^{13}
1001	$1 + \alpha^3$	α^{14}

Consider the element $\beta = \alpha^3$, construct the minimal polynomial $m_3(x)$
$m_3(x) = a_0 + a_1x + a_2x^2 + a_3x^3 + a_4x^4$
Since $m_3(x)$ has β as the root
$m_3(\beta) = a_0 + a_1\beta + a_2\beta^2 + a_3\beta^3 + a_4\beta^4 = 0$
Since β is the 5th element , $\beta = \alpha^3$
i.e. $m_3(\beta) = m_3(\alpha^3) = a_0 + a_1\alpha^3 + a_2\alpha^6 + a_3\alpha^9 + a_4\alpha^{12} = 0$

Expand α with degree higher than 3
$m_3(\beta) = a_0 + a_1\alpha^3 + a_2(\alpha^2 + \alpha^3) + a_3(\alpha + \alpha^3) + a_4(1 + \alpha + \alpha^2 + \alpha^3) = 0$

Thus
$a_0 + a_4 = 0$
$a_3 + a_4 = 0$
$a_2 + a_4 = 0$
$a_1 + a_2 + a_3 + a_4 = 0$

After solving, $a_0 = a_1 = a_2 = a_3 = a_4 = 1$
$m_3(x) = 1 + x + x^2 + x^3 + x^4$

$-END-$