LAB 06 EXCERCISE

2021 / 10 / 27

LECTEROR : HUAN-JUNG LEE

GALOIS FIELD (FINITE FIELD)

- Finite field (GF(2^k)) is a field with finite number 2^k with the set {0 , 1 , 2 , ... , 2^k-1}, and can do addition(+), substaction(-), multiplication(*), and Division(/).
- The set can also behavior as {00..00, 00..01 , 00..10 , ... , 11..11 } or {0 , 1 , x , ... , $x^{k-1} + x^{k-2} +$ ... $+ 1$}
- Arithmetic under finite field always fall in the same field. And reduce the result to degree k-1 by the irreducible function f(x).
- Ex: GF(2^k) ; k =1 . GF(2) has finite number describe in the set {0, 1}, irreducible function f(x) = x
    - Add : (1 + 0) % x = 1
    - Sub : (0 – 1) % x = (0 + (-1)) % x = (0 + 1) % x = 1
    - Mult : (1 * 1) % x = 1
    - Div : (0 / 1) % x = (0 $*$ 1^{-1})= (0 * 1) % x = 0

ADDITION IN GF(2^K) ; K =2

- Set = { 0 , 1 , 2 , 3} = { 0 , 1 , x , $x + 1$}
- Irreducible function $f(x) = x^2 + x + 1$.
- If A = 3, B = 2 , A + B = ?
  - A = 3 = $x + 1$
  - B = 2 = x
  - A + B = $(x + 1 + x)$ % $f(x)$

    = $((1 + 1)\,x + 1)$ % $f(x)$

    = $((0)\,x + 1)$% $f(x)$

    = 1 % $f(x)$ = 1

SUBSTACTION IN GF(2^K) ; K =2

- Set = { 0 , 1 , 2 , 3} = { 0 , 1 , x , $x + 1$}
- Irreducible function f(x) = $x^2 + x + 1$.
- If A = 3, B = 2 , A - B = ?
  - A = 3 = $x + 1$
  - B = 2 = x
  - A - B = $(x + 1 - x)$ % f(x)

    = $((1 - 1) x + 1)$ % f(x)

    = $((0) x + 1)$% f(x)

    = 1 % f(x) = 1

MULTIPLICATION IN GF(2^K) ; K =2

- Set = { 0 , 1 , 2 , 3} = { 0 , 1 , x , x + 1}
- Irreducible function f(x) = $x^2 + x + 1$.
- If A = 3, B = 2 , A * B = ?
  - A = 3 = $x + 1$
  - B = 2 = x
  - A * B = $(x + 1) * x$ % f(x)

    = $(x * x + 1 * x)$ % f(x)

    = $(x^2 + x)$ % f(x)

    = $(x^2 + x)$ % $(x^2 + x + 1)$

    = $((x + 1) + x) = 1$

Degree >= k !!!!(here is 2)

Hint : modulo function can use f(x) = 0 and fill the target function with it.

ex : f(x) = $x^2 + x + 1 = 0$

target function : g(x) = $(x^2 + x)$ % f(x)

$x^2 + x + 1 = 0$

$x^2 = x + 1$

g(x) = $(x^2 + x)$ % f(x)

= $(x + 1 + x) = 1$

DIVISION IN GF(2^K) ; K = 4

- Set = { 0 , 1 , ..., 15} = { 0 , 1 , ..., $x^3 + x^2 + x + 1$}
- Irreducible function f(x) = $x^4 + x^3 + 1$.
- If A = 2, B = 9 ,A / B = ?
  - A = 2 = x
  - B = 9 = $x^3 + 1$
  - A / B = A $*$ B^{-1}

Hint : how to find B^{-1} ?

DIVISION IN GF(2^K) ; K = 4

- B^{-1} can found by extended "Euclid's algorithm" with irreducible function f(x) and B
  - f(x) = $x^4 + x^3 + 1$
  - B = $x^3 + 1$

Preview : Eucild algorithm (in positve interger field)
A = 19, B = 5 find gdc(greatest common divisor) ?

A = 19
B = 5
A % B = 4 = A'
B % A' = 1 = B'
A' % B' = 0 (while remainder is 0 this divisor is gcd)

And we know $B * B^{-1} = 1$, so B , B^{-1} has gcd 1.
Extended algorithm use this result.

EXTENDED EUCLID'S ALGORITHM

- Part A : Polynomial divide
- Part B : multiple quotient
- Part C : Muiltiple inverse

EXTENDED EUCLID'S ALGORITHM PART A : POLYNOMIAL DIVIDE

- B = $x^3 + 1$
- f(x) = $x^4 + x^3 + 1$

i	Remainder($\mathrm{R_i}$)	Quotient(Q_i)	division($\mathrm{DN_i}$)	divisor($\mathrm{DR_i}$)
-I	$x^4 + x^3 + 1$	-	-	-
0	$x^3 + 1$	-	-	-

EXTENDED EUCLID'S ALGORITHM PART A : POLYNOMIAL DIVIDE

- $DN_1 = \mathbf{f}(\mathbf{x}) = x^4 + x^3 + 1$
- $DR_1 = B = x^3 + 1$

i	Remainder(R_i)	Quotient(Q_i)	division(DN_i)	divisor(DR_i)
-1	$x^4 + x^3 + 1$	-	-	-
0	$x^3 + 1$	-	-	-
1			$x^4 + x^3 + 1$	$x^3 + 1$

EXTENDED EUCLID'S ALGORITHM PART A : POLYNOMIAL DIVIDE

- DN_0 / DR_0 = Q_1

i	Remainder(R_i)	Quotient(Q_i)	division(DN_i)	divisor(DR_i)
-1	$x^4 + x^3 + 1$	-	-	-
0	$x^3 + 1$	-	-	-
1		x	$x^4 + x^3 + 1$	$x^3 + 1$

EXTENDED EUCLID'S ALGORITHM PART A : POLYNOMIAL DIVIDE

- $DN_1 + Q_1 * DR_1 = R_1$

i	Remainder(R_i)	Quotient(Q_i)	division(DN_i)	divisor(DR_i)
-1	$x^4 + x^3 + 1$	-	-	-
0	$x^3 + 1$	-	-	-
1	$x^3 + x + 1$	x	$x^4 + x^3 + 1$	$x^3 + 1$

EXTENDED EUCLID'S ALGORITHM PART A : POLYNOMIAL DIVIDE

- If $\mathrm{DR_1}$ >= $\mathrm{R_1}$ $\mathrm{DN_2} = \mathrm{DR_1}, \mathrm{DR_2} = \mathrm{R_1}$
- else $\mathrm{DN_2} = \mathrm{R_1}, \mathrm{DR_2} = \mathrm{DR_1}$

i	Remainder($\mathrm{R_i}$)	Quotient(Q_i)	division($\mathrm{DN_i}$)	divisor($\mathrm{DR_i}$)
-1	$x^4 + x^3 + 1$	-	-	-
0	$x^3 + 1$	-	-	-
1	$x^3 + x + 1$	x	$x^4 + x^3 + 1$	$x^3 + 1$
2			$x^3 + x + 1$	$x^3 + 1$

EXTENDED EUCLID'S ALGORITHM PART A : POLYNOMIAL DIVIDE

- DN_1 / DR_1 = Q_2

i	Remainder(R_i)	Quotient(Q_i)	division(DN_i)	divisor(DR_i)
-1	$x^4 + x^3 + 1$	-	-	-
0	$x^3 + 1$	-	-	-
1	$x^3 + x + 1$	x	$x^4 + x^3 + 1$	$x^3 + 1$
2		1	$x^3 + x + 1$	$x^3 + 1$

EXTENDED EUCLID'S ALGORITHM PART A : POLYNOMIAL DIVIDE

- $DN_2 + Q_2 * DR_2 = R_2$

i	Remainder(R_i)	Quotient(Q_i)	division(DN_i)	divisor(DR_i)
-1	$x^4 + x^3 + 1$	-	-	-
0	$x^3 + 1$	-	-	-
1	$x^3 + x + 1$	x	$x^4 + x^3 + 1$	$x^3 + 1$
2	x	1	$x^3 + x + 1$	$x^3 + 1$

EXTENDED EUCLID'S ALGORITHM
PART A : POLYNOMIAL DIVIDE

- $DN_2 + Q_2 * DR_2 = R_2$

i	Remainder(R_i)	Quotient(Q_i)	division(DN_i)	divisor(DR_i)
-1	$x^4 + x^3 + 1$	-	-	-
0	$x^3 + 1$	-	-	-
1	$x^3 + x + 1$	x	$x^4 + x^3 + 1$	$x^3 + 1$
2	x	1	$x^3 + x + 1$	$x^3 + 1$
3			$x^3 + 1$	x

EXTENDED EUCLID'S ALGORITHM PART A : POLYNOMIAL DIVIDE

- If $\mathrm{DR_{i-1}}$ >= R_{i-1}, $\mathrm{E}_i = 0, \mathrm{DN_i} = \mathrm{DR_{i-1}}$, $\mathrm{DR_i} = \mathrm{R_{i-1}}$
- else $\mathrm{E_i} = 1$, $\mathrm{DN_i} = \mathrm{R_{i-1}}$, $\mathrm{DR_i} = \mathrm{DR_{i-1}}$

i	Remainder($\mathrm{R_i}$)	Quotient(Q_i)	division($\mathrm{DN_i}$)	divisor($\mathrm{DR_i}$)
-1	$x^4 + x^3 + 1$	-	-	-
0	$x^3 + 1$	-	-	-
1	$x^3 + x + 1$	x	$x^4 + x^3 + 1$	$x^3 + 1$
2	x	1	$x^3 + x + 1$	$x^3 + 1$
3		x^2	$x^3 + 1$	x

EXTENDED EUCLID'S ALGORITHM PART A : POLYNOMIAL DIVIDE

- Until $\mathrm{R_i} = 1$
- $\mathrm{R_i} = \mathrm{DN_i} + \mathrm{DR_i} * \mathrm{Q}_i$

i	Remainder($\mathrm{R_i}$)	Quotient(Q_i)	division($\mathrm{DN_i}$)	divisor($\mathrm{DR_i}$)
-1	$x^4 + x^3 + 1$	-	-	-
0	$x^3 + 1$	-	-	-
1	$x^3 + x + 1$	x	$x^4 + x^3 + 1$	$x^3 + 1$
2	x	1	$x^3 + x + 1$	$x^3 + 1$
3	1	x^2	$x^3 + 1$	x

EXTENDED EUCLID'S ALGORITHM PART B : MULTIPLE QUOTIENT

- $MQ_{-1} = 0$
- $MQ_0 = 1$

i	$MQ_i(\textit{muliple quotinet})$	$mqh_i(MQ\ high)$	$mql_i(MQ\ low)$	Remainder(R_i)	Quotient(Q_i)	division(DN_i)	divisor(DR_i)
-1	0	-	-	$x^4 + x^3 + 1$	-	-	-
0	1	-	-	$x^3 + 1$	-	-	-
1				$x^3 + x + 1$	x	$x^4 + x^3 + 1$	$x^3 + 1$
2				x	1	$x^3 + x + 1$	$x^3 + 1$
3				1	x^2	$x^3 + 1$	x

EXTENDED EUCLID'S ALGORITHM
PART B : MULTIPLE QUOTIENT

- $\mathrm{mqh}_{\mathbf{1}} = \mathrm{MQ}_{-\mathbf{1}}$
- $\mathrm{mq}l_{\mathbf{1}} = \mathrm{MQ}_{\mathbf{0}}$

i	$MQ_{\mathrm{i}}(muliple\ quotinet)$	$mqh_{\mathrm{i}}(MQ\ high)$	$mql_{\mathrm{i}}(MQ\ low)$	Remainder($\mathrm{R_i}$)	Quotient(Q_{i})	division($\mathrm{DN_i}$)	divisor($\mathrm{DR_i}$)
-1	0	-	-	$x^4 + x^3 + 1$	-	-	-
0	1	-	-	$x^3 + 1$	-	-	-
1		0	1	$x^3 + x + 1$	x	$x^4 + x^3 + 1$	$x^3 + 1$
2				x	1	$x^3 + x + 1$	$x^3 + 1$
3				1	x^2	$x^3 + 1$	x

EXTENDED EUCLID'S ALGORITHM PART B : MULTIPLE QUOTIENT

- $\mathrm{MQ}_1 = \mathrm{mqh}_1 + mql_1 * \mathrm{Q}_1$

i	$MQ_{\mathrm{i}}(muliple\ quotinet)$	$mqh_{\mathrm{i}}(MQ\ high\ )$	$mql_{\mathrm{i}}(MQ\ low)$	Remainder($\mathrm{R_i}$)	Quotient(Q_{i})	division($\mathrm{DN_i}$)	divisor($\mathrm{DR_i}$)
-1	0	-	-	$x^4 + x^3 + 1$	-	-	-
0	1	-	-	$x^3 + 1$	-	-	-
1	x	0	1	$x^3 + x + 1$	x	$x^4 + x^3 + 1$	$x^3 + 1$
2				x	1	$x^3 + x + 1$	$x^3 + 1$
3				1	x^2	$x^3 + 1$	x

EXTENDED EUCLID'S ALGORITHM
PART B : MULTIPLE QUOTIENT

- If DR_1 >= R_1, $\mathrm{mq}h_2 = mql_1, mql_2 = \mathrm{MQ}_1$
- else $\mathrm{mqh}_2 = \mathrm{MQ}_1, mql_2 = \mathrm{mql}_1$

i	$MQ_{\mathrm{i}}(muliple\ quotinet)$	$mqh_{\mathrm{i}}(MQ\ high\ )$	$mql_{\mathrm{i}}(MQ\ low)$	Remainder($\mathrm{R_i}$)	Quotient(Q_{i})	division($\mathrm{DN_i}$)	divisor($\mathrm{DR_i}$)
-1	0	-	-	$x^4 + x^3 + 1$	-	-	-
0	1	-	-	$x^3 + 1$	-	-	-
1	x	0	1	$x^3 + x + 1$	x	$x^4 + x^3 + 1$	$x^3 + 1$
2		x	1	x	1	$x^3 + x + 1$	$x^3 + 1$
3				1	x^2	$x^3 + 1$	x

EXTENDED EUCLID'S ALGORITHM PART B : MULTIPLE QUOTIENT

- $\mathrm{MQ}_2 = \mathrm{mqh}_2 + mql_2 * \mathrm{Q}_2$

i	$MQ_i(muliple\ quotinet)$	$mqh_i(MQ\ high\ )$	$mql_i(MQ\ low)$	Remainder(R_i)	Quotient(Q_i)	division(DN_i)	divisor(DR_i)
-1	0	-	-	x^4+x^3+1	-	-	-
0	1	-	-	x^3+1	-	-	-
1	x	0	1	x^3+x+1	x	x^4+x^3+1	x^3+1
2	$x+1$	x	1	x	1	x^3+x+1	x^3+1
3				1	x^2	x^3+1	x

EXTENDED EUCLID'S ALGORITHM PART B : MULTIPLE QUOTIENT

- If DR_{i-1} >= R_{i-1}, $\mathrm{mq}h_i$ = $mql_{\mathrm{i}-1}, mql_i$ = MQ_{i-1}
- else mqh_i = MQ_{i-1}, mql_i = mql_{i-1}

i	$MQ_{\mathrm{i}}(muliple\ quotinet)$	$mqh_{\mathrm{i}}(MQ\ high\ )$	$mql_{\mathrm{i}}(MQ\ low)$	Remainder($\mathrm{R_i}$)	Quotient(Q_{i})	division($\mathrm{DN_i}$)	divisor($\mathrm{DR_i}$)
-1	0	-	-	$x^4 + x^3 + 1$	-	-	-
0	1	-	-	$x^3 + 1$	-	-	-
1	x	0	1	$x^3 + x + 1$	x	$x^4 + x^3 + 1$	$x^3 + 1$
2	$x + 1$	x	1	x	1	$x^3 + x + 1$	$x^3 + 1$
3		1	$x + 1$	1	x^2	$x^3 + 1$	x

EXTENDED EUCLID'S ALGORITHM PART B : MULTIPLE QUOTIENT

- $\mathrm{MQ_i} = \mathrm{mqh}_i + mql_i * \mathrm{Q_i}$

i	$MQ_{\mathrm{i}}(muliple\ quotinet)$	$mqh_{\mathrm{i}}(MQ\ high\ )$	$mql_{\mathrm{i}}(MQ\ low)$	Remainder($\mathrm{R_i}$)	Quotient(Q_{i})	division($\mathrm{DN_i}$)	divisor($\mathrm{DR_i}$)
-1	0	-	-	$x^4 + x^3 + 1$	-	-	-
0	1	-	-	$x^3 + 1$	-	-	-
1	x	0	1	$x^3 + x + 1$	x	$x^4 + x^3 + 1$	$x^3 + 1$
2	$x + 1$	x	1	x	1	$x^3 + x + 1$	$x^3 + 1$
3	$x^3 + x^2 + 1$	1	$x + 1$	1	x^2	$x^3 + 1$	x

EXTENDED EUCLID'S ALGORITHM
PART B : MULTIPLE QUOTIENT

- $B^{-1} = x^3 + x^2 + 1$

i	$MQ_i(muliple\ quotinet)$	$mqh_i(MQ\ high\ )$	$mql_i(MQ\ low)$	Remainder(R_i)	Quotient(Q_i)	division(DN_i)	divisor(DR_i)
-1	0	-	-	$x^4 + x^3 + 1$	-	-	-
0	1	-	-	$x^3 + 1$	-	-	-
1	x	0	1	$x^3 + x + 1$	x	$x^4 + x^3 + 1$	$x^3 + 1$
2	$x + 1$	x	1	x	1	$x^3 + x + 1$	$x^3 + 1$
3	$x^3 + x^2 + 1$	1	$x + 1$	1	x^2	$x^3 + 1$	x

EXTENDED EUCLID'S ALGORITHM PART C : MUILTIPLE INVERSE

- $B^{-1} = x^3 + x^2 + 1$
- $A = x$
- $A\ /\ B = \left(A\ *\ B^{-1}\right)\ \%\ f(x) = (x * (x^3 + x^2 + 1))\%\ f(x)$

$= (x^4 + x^3 + x)\ \%\ (x^4 + x^3 + 1)$

$= x + 1$

$= 3$

EXERCISE

- IP design : GF(2^k) + - * /
- Design : GF(4), GF(8), GF(16), GF(32) inverse matrix
- You need to fill the space in 02_SYN/syn.tcl by yourself

THANK YOU FOR YOUR LISTENING ~