MEMO NUMBER: 02
DATE: October 6, 2017
TO: EFC LaBerge
FROM: Sabbir Ahmed, Jeffrey Osazuwa, Howard To, Brian Weber
SUBJECT: Background Homework

1 Background

A Galois Field is a field with a finite number of elements. The nomenclature $GF(q)$ is to indicate a Galois field with q elements. For $GF(q)$ in general, q must be a power of a prime. The best known and most used Galois field is $GF(2)$, the binary field.

2 Show that $x^3 + x^2 + x^0$ is irreducible in $GF(2)[x]$

$$x = 0 : (0)^3 + (0)^2 + (0)^0 = 0 + 0 + 1 = 1\ (not\ a\ root)$$

$$x = 1 : (1)^3 + (1)^2 + (1)^0 = 1 + 1 + 1 = 1\ (not\ a\ root)$$

$$\therefore x^3 + x^2 + x^0 \text{ has no roots in } GF(2)[x].$$

3 Generate the 8 elements of $GF(2^3)$ using the primitive polynomial $x^3 + x^2 + x^0$.

Let $\beta \,\epsilon\, GF(2^3)$ be a root of $x^3 + x^2 + x^0 \implies \beta^3 + \beta^2 + \beta^0$
$\therefore$ The coefficients are in $GF(2) \implies \beta^3 = \beta^2 + \beta^0$

$$\because a\ field\ has\ additive\ and\ multiplicative\ identities :$$

$$\therefore 0, 1 = \beta^0 \,\epsilon\, GF(2^3)$$

$$\therefore \beta^1 \,\epsilon\, GF(2^3)\ (\because\ closure\ of\ multiplication)$$

$$\therefore \beta^2 \,\epsilon\, GF(2^3)\ (\because\ assumption)$$

$$\therefore \beta^3 \,\epsilon\, GF(2^3)\ (\because \beta^3 = \beta^2 + \beta^0)$$

$$\begin{aligned}\because \beta^4 &= \beta^1 \times \beta^3 \\ &= \beta^1(\beta^2 + \beta^0) \\ &= \beta^3 + \beta^1 \\ &= \beta^2 + \beta^1 + \beta^0\end{aligned}$$

$$\therefore \beta^4 \,\epsilon\, GF(2^3)$$

$$
\begin{aligned}
\because \beta^5 &= \beta^1 \times \beta^4 \\
&= \beta^1(\beta^2 + \beta^1 + \beta^0) \\
&= \beta^3 + \beta^2 + \beta^1 \\
&= \beta^2 + \beta^0 + \beta^2 + \beta^1 \\
&= \beta^1 + \beta^0
\end{aligned}
$$

$$\therefore \beta^5 \,\epsilon\, GF(2^3)$$

$$
\begin{aligned}
\because \beta^6 &= \beta^1 \times \beta^5 \\
&= \beta^1(\beta^1 + \beta^0) \\
&= \beta^2 + \beta^1
\end{aligned}
$$

$$\therefore \beta^6 \,\epsilon\, GF(2^3)$$

$$
\begin{aligned}
\because \beta^7 &= \beta^1 \times \beta^6 \\
&= \beta^1(\beta^2 + \beta^1) \\
&= \beta^3 + \beta^2 \\
&= \beta^2 + \beta^0 + \beta^2 \\
&= \beta^0 = 1
\end{aligned}
$$

$$\therefore \beta^7 \,\epsilon\, GF(2^3)$$

Table 1: The 8 Element Vectors of $x^3 + x^2 + x^0$ in $GF(2)[x]$

Element	**Polynomial Form**	**Symbol**
0	$0+0+0$	000
β^0	$0+0+\beta^0$	001
β^1	$0+\beta^1+0$	010
β^2	β^2+0+0	100
β^3	$\beta^2+0+\beta^0$	101
β^4	$\beta^2+\beta^1+\beta^0$	111
β^5	$0+\beta^1+\beta^0$	011
β^6	$\beta^2+\beta^1+0$	110
β^7	$0+0+\beta^0$	001

4 Generate the addition (bitwise XOR) and multiplication tables for the implementation of $GF(2)[x]$

Table 2: Addition Table for $x^3 + x^2 + x^0$ in $GF(2)[x]$

$+$	$\mathbf{0}$	$\boldsymbol{\beta^0}$	$\boldsymbol{\beta^1}$	$\boldsymbol{\beta^2}$	$\boldsymbol{\beta^3}$	$\boldsymbol{\beta^4}$	$\boldsymbol{\beta^5}$	$\boldsymbol{\beta^6}$
$\mathbf{0}$	0	β^0	β^1	β^2	β^3	β^4	β^5	β^6
$\boldsymbol{\beta^0}$	β^0	0	β^5	β^3	β^2	β^6	β^1	β^4
$\boldsymbol{\beta^1}$	β^1	β^5	0	β^6	β^4	β^3	β^0	β^2
$\boldsymbol{\beta^2}$	β^2	β^3	β^6	0	β^0	β^5	β^4	β^1
$\boldsymbol{\beta^3}$	β^3	β^2	β^4	β^0	0	β^1	β^6	β^5
$\boldsymbol{\beta^4}$	β^4	β^6	β^3	β^5	β^1	0	β^2	β^0
$\boldsymbol{\beta^5}$	β^5	β^1	β^0	β^4	β^6	β^2	0	β^3
$\boldsymbol{\beta^6}$	β^6	β^4	β^2	β^1	β^5	β^0	β^3	0

Table 3: Multiplication Table for $x^3 + x^2 + x^0$ in $GF(2)[x]$

$\times$	$\mathbf{0}$	$\boldsymbol{\beta^0}$	$\boldsymbol{\beta^1}$	$\boldsymbol{\beta^2}$	$\boldsymbol{\beta^3}$	$\boldsymbol{\beta^4}$	$\boldsymbol{\beta^5}$	$\boldsymbol{\beta^6}$
$\mathbf{0}$	0	0	0	0	0	0	0	0
$\boldsymbol{\beta^0}$	0	β^0	β^1	β^2	β^3	β^4	β^5	β^6
$\boldsymbol{\beta^1}$	0	β^1	β^2	β^3	β^4	β^5	β^6	β^0
$\boldsymbol{\beta^2}$	0	β^2	β^3	β^4	β^5	β^6	β^0	β^1
$\boldsymbol{\beta^3}$	0	β^3	β^4	β^5	β^6	β^0	β^1	β^2
$\boldsymbol{\beta^4}$	0	β^4	β^5	β^6	β^0	β^1	β^2	β^3
$\boldsymbol{\beta^5}$	0	β^5	β^6	β^0	β^1	β^2	β^3	β^4
$\boldsymbol{\beta^6}$	0	β^6	β^0	β^1	β^2	β^3	β^4	β^5