

MEMO NUMBER: 03
DATE: October 15, 2017
TO: EFC LaBerge
FROM: Sabbir Ahmed, Jeffrey Osazuwa, Howard To, Brian Weber
SUBJECT: Background on the Galois Field

1 Purpose and Scope

1.1 Introduction

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

2 Algorithm

Input polynomials will be represented as 16 bit arrays, where the coefficient of the terms are represented as 1. The arrays are zero-based, so the 16th bit shall be placed on the 15th index. For example, the polynomial $x^3 + x^2 + x^0$ will be represented as

$\langle 0000\ 0000\ 0000\ 1101 \rangle$ (3rd, 2nd, and 0th bits)

2.1 Determining Irreducibility

A polynomial is irreducible if and only if:

1. the coefficient of its 0th term is 1
2. the number of terms is odd

2.2 Default Symbols

Once a polynomial is determined irreducible, its default symbols may be generated.

1. The symbols for $\{x^0, x^1, \dots, x^{n-1}\}$ are generated by setting the corresponding bits to 1.
2. The symbol for x^n is generated by setting the corresponding bits for the terms in the polynomial after the highest degree term.
3. The symbol for x^{2^n-1} cycles back to x^0 , and is set to x^0 .

This would generate $n + 1$ terms. Therefore, the maximum of 16 bits would have 17 terms generated by default.

Table 1: Default Symbols Generated for An Irreducible Polynomial of Degree n

Element	Polynomial Form	Symbol
0	$0_{n-1} + \dots + 0_2 + 0_1 + 0_0$	$\{0_{n-1} \dots 0_2 0_1 0_0\}$
α^0	$0_{n-1} + \dots + 0_2 + 0_1 + \alpha_0^0$	$\{0_{n-1} \dots 0_2 0_1 1_0\}$
α^1	$0_{n-1} + \dots + 0_2 + \alpha_1^1 + 0$	$\{0_{n-1} \dots 0_2 1_1 0_0\}$
α^2	$0_{n-1} + \dots + \alpha_2^2 + 0_1 + 0_0$	$\{0_{n-1} \dots 1_2 0_1 0_0\}$
\dots	\dots	\dots
α^{n-1}	$1_{n-1} + \dots + 0_2 + 0_1 + 0_0$	$\{1_{n-1} \dots 0_2 0_1 0_0\}$
α^n	$\alpha_{n-1}^{n-1} + \dots + \alpha_2^2 + \alpha_1^1 + \alpha_0^0$	$\{x_{n-1} \dots x_2 x_1 x_0\}$
α^{2^n-1}	$0_{n-1} + \dots + 0_2 + 0_1 + \alpha_0^0$	$\{0_{n-1} \dots 0_2 0_1 1_0\}$

2.3 Generated Symbols

The rest of the symbols for the terms x^{n+1} to x^{2^n-2} must be generated. In total, that would require $2^n - 2 - n - 1 + 1 = 2^n - 2 - n$ terms. Therefore, the maximum of 16 bits would require 65,518 terms to be generated.

Generating the rest of the symbols may be implemented with a linear feedback shift register (LFSR), using the following recursive equation:

$$\begin{aligned}
 \alpha^{n+m} &= \alpha^{n+(m-1)} \times \alpha^n \\
 &= (\alpha^{n+(m-1)} \ll 1)[n-1] = 1 \implies (\alpha^{n+(m-1)} \ll 1)[n-2:0] \oplus \alpha^n[n-2:0] \\
 &\wedge \neg(\alpha^{n+(m-1)} \ll 1)[n-1] = 1 \implies (\alpha^{n+(m-1)} \ll 1)[n-2:0]
 \end{aligned}$$

3 VHSIC Hardware Design Language (VHDL) Implementation

TODO:

4 Example

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

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

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

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

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

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

\therefore a field has additive and multiplicative identities :

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

$$\therefore \beta^1 \in GF(2^3) (\because \text{closure of multiplication})$$

$$\therefore \beta^2 \in GF(2^3) (\because \text{assumption})$$

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

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

$$\therefore \beta^4 \in GF(2^3)$$

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

$$\therefore \beta^5 \in GF(2^3)$$

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

$$\therefore \beta^6 \in GF(2^3)$$

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

$$\therefore \beta^7 \in GF(2^3)$$

Table 2: 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	$\beta^2 + 0 + 0$	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

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

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

+	0	β^0	β^1	β^2	β^3	β^4	β^5	β^6
0	0	β^0	β^1	β^2	β^3	β^4	β^5	β^6
β^0	β^0	0	β^5	β^3	β^2	β^6	β^1	β^4
β^1	β^1	β^5	0	β^6	β^4	β^3	β^0	β^2
β^2	β^2	β^3	β^6	0	β^0	β^5	β^4	β^1
β^3	β^3	β^2	β^4	β^0	0	β^1	β^6	β^5
β^4	β^4	β^6	β^3	β^5	β^1	0	β^2	β^0
β^5	β^5	β^1	β^0	β^4	β^6	β^2	0	β^3
β^6	β^6	β^4	β^2	β^1	β^5	β^0	β^3	0

Table 4: Multiplication Table for $x^3 + x^2 + x^0$ in $GF(2)[x]$

\times	0	β^0	β^1	β^2	β^3	β^4	β^5	β^6
0	0	0	0	0	0	0	0	0
β^0	0	β^0	β^1	β^2	β^3	β^4	β^5	β^6
β^1	0	β^1	β^2	β^3	β^4	β^5	β^6	β^0
β^2	0	β^2	β^3	β^4	β^5	β^6	β^0	β^1
β^3	0	β^3	β^4	β^5	β^6	β^0	β^1	β^2
β^4	0	β^4	β^5	β^6	β^0	β^1	β^2	β^3
β^5	0	β^5	β^6	β^0	β^1	β^2	β^3	β^4
β^6	0	β^6	β^0	β^1	β^2	β^3	β^4	β^5