MEMO NAME: GFAU_BACKGROUND
DATE: November 8, 2017
TO: EFC LaBerge
SUBJECT: Background on the Galois Field Arithmetic Unit

1 Background

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. In $GF(q)$ the parameter q must be a power of a prime. For each prime power there exists exactly one finite field. The binary field $GF(2)$ is the most frequently used Galois field.

1.1 Purpose and Scope

The Galois Field Arithmetic Unit operates in fields of q^n, where $2 \leq n \leq 16$. This document will demonstrate the functionality of the unit by deriving all its functionality through mathematical approaches. The mathematical algorithms will be followed by their corresponding implementations in digital design.

1.2 Terms and Keywords

1.2.1 Input Primitive Polynomials

Input primiteive polynomials in the Galois Field are represented as:

$$c_n x^n + \ldots + c_2 x^2 + c_1 x^1 + c_0 x^0, \ where\ c, x \ \epsilon\ GF(2) = \{0, 1\}$$

For convenience and simplicity, all the examples provided will refer to the following polynomial: $x^3 + x^2 + x^0$.

1.2.2 Elements

The elements of an input polynomial refer to the $2^n - 1$ elements in the field.

1.2.3 Polynomial Form

The polynomial forms of the elements refer to the $2^n - 1$ symbolic representations of the of an input primitive polynomials in the field.

2 Algorithms

Input polynomials will be represented as 16 bit zero- base arrays. For example, the polynomial $x^3 + x^2 + x^0$ will be represented as

$$< 0000\ 0000\ 0000\ 1101 > (3rd,\ 2nd,\ and\ 0th\ bits)$$

2.1 Determining Irreducibility

A polynomial is said to be irreducible if and only if there exists no roots for it.

2.1.1 Analytical Approach

If the sum of the coefficients of the polynomial equals 1 when $x = 0$ and $x = 1$, the polynomial is irreducible.

2.1.1.1 Example

Show that the polynomial $x^3 + x^2 + x^0$ is irreducible in $GF(2)[x]$ using the mathematical algorithm:

$$\begin{aligned} x = 0 : 0^3 + 0^2 + 0^0 \\ = 0 + 0 + 1 \\ = 1 \\ x = 1 : 1^3 + 1^2 + 1^0 \\ = 1 + 1 + 1 \\ = 1 \end{aligned}$$

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

Since the sum of the coefficients is 1 for both the cases, the polynomial is therefore determined irreducible.

2.1.2 Digital Logic

To design such algorithm, the polynomial may be checked for the following attributes:

1. the coefficient of its 0th term is 1
2. the total number of non-zero coefficients is odd

If both of these conditions are met, the polynomial is irreducible.

2.1.2.1 Example

Show that the polynomial $x^3 + x^2 + x^0$ is irreducible using the digital algorithm:

$$< 0000\ 0000\ 0000\ 1101 >$$

The 0th bit is 1 and the total number of non-zero coefficients is 3. Therefore, the polynomial is determined irreducible.

2.2 Symbols

Once a polynomial is determined irreducible, its symbols may be generated. The number of terms grow exponentially, $2^n - 1$, where n is the highest degree of the polynomial.

2.2.1 Default Symbols

Default symbols refer to terms in the field that exist for Galois Fields of all irreducible polynomials of q^n, where $2 \leq n \leq 16$. Since the number of elements cannot be smaller than 2, only zero and the 0th and 1st elements are shared among all fields.

Table 1: Default Symbols Generated for All Irreducible Polynomials

Element	Polynomial Form	Symbol
0	$0_{15} + \ldots + 0_2 + 0_1 + 0_0$	$\{0_{15} \ldots 0_2 0_1 0_0\}$
α^0	$0_{15} + \ldots + 0_2 + 0_1 + \alpha_0^0$	$\{0_{15} \ldots 0_2 0_1 1_0\}$
α^1	$0_{15} + \ldots + 0_2 + \alpha_1^1 + 0$	$\{0_{15} \ldots 0_2 1_1 0_0\}$

Table 1 have all the bits of their values set to 0 except where indicated.

2.2.1.1 Analytical Approach

Using the example polynomial $x^3 + x^2 + x^0$, show that 0, the 0th element and the first element exist in $GF(2^3)$.

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 $GF(2) \implies \beta^3 = \beta^2 + \beta^0$

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

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

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

2.2.2 Automatic Symbols

Automatic symbols refer to terms up to x^{n-1}. Automatic symbols may be generated concurrently, and consist of the following attributes:

1. The symbols for $\{x^0, x^1, \ldots, x^{n-1}\}$ 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.

Automatic symbols consist of $n+1$ terms. Therefore, the maximum of 16 bits would have 17 terms generated by default.

Table 2: Automatic Symbols Generated for An Irreducible Polynomial of Degree $\boldsymbol{n < 16}$.

Element	Polynomial Form	Symbol
α^2	$0_{15} + \ldots + 0_{n-1} + \ldots + \alpha_2^2 + 0_1 + 0_0$	$\{0_{15} \ldots 0_{n-1} \ldots 1_2 0_1 0_0\}$
$\ldots$	$\ldots$	$\ldots$
α^{n-1}	$0_{15} + \ldots + \alpha_{n-1}^{n-1} + \ldots + 0_2 + 0_1 + 0_0$	$\{0_{15} \ldots 1_{n-1} \ldots 0_2 0_1 0_0\}$
α^n	$0_{15} + \ldots + \alpha_{n-1}^{n-1} + \ldots + \alpha_2^2 + \alpha_1^1 + \alpha_0^0$	$\{0_{15} \ldots x_{n-1} \ldots x_2 x_1 x_0\}$
α^{2^n-1}	$0_{15} + \ldots + 0_{n-1} + \ldots + \alpha_2^2 + 0_1 + 0_0$	$\{0_{15} \ldots 0_{n-1} \ldots 0_2 0_1 0_0\}$

Table 2 refers to polynomials with their highest degree of $\boldsymbol{n < 15}$. $0_{15}\ldots$ indicates zero-padding of the bits. For $\boldsymbol{n = 16}$, the most significant bit will be 1_{15}.

2.2.2.1 Analytical Approach

Assuming the preceding values exist from the proof above, use the example polynomial $x^3 + x^2 + x^0$ to show that the $n-1$th and the nth elements exist in $GF(2^3)$.

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

$$\therefore \beta^2 \in GF(2^3)\ (\because\ closure\ of\ multiplication)$$

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

2.2.3 Generated Symbols

The rest of the symbols for the elements 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.

2.2.3.1 Analytical Approach

Assuming the preceding values exist from the proof above, use the example polynomial $x^3 + x^2 + x^0$ to show that the elements up to the (2^{n-2})th elements exist in $GF(2^3)$.

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

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

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

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

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

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

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

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

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

2.2.4 Example

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

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

(1) Zero is a reserved element where its binary symbol does not represent its decimal value.
(2) Elements beyond the $(2^n - 1)$th element will be handled with special conditions since they cycle back to previous.

2.2.4.1 Digital Logic

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

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

2.3 Operations

Operations in the Galois Field Arithmetic Unit consist of addition, subtraction, multiplication, division and logarithm.

2.3.1 Addition and Subtraction

Binary addition and binary subtraction are synonymous in the Galois Field. Addition and subtraction of Galois operands may be done by bitwise exclusive OR-ing the operands.

$$
\begin{aligned}
\alpha^i \pm \alpha^j &= \{x_{i,n-1}, \ldots x_{i,2}, x_{i,1}, x_{i,0}\} + \{x_{j,n-1}, \ldots x_{j,2}, x_{j,1}, x_{j,0}\} \\
&= \{(x_{i,n-1} \oplus x_{j,n-1}), \ldots (x_{i,2} \oplus x_{j,2}), (x_{i,1} \oplus x_{j,1}), (x_{i,0} \oplus x_{j,0})\} \\
&= \alpha^k
\end{aligned}
$$

2.3.2 Multiplication

Binary multiplication of Galois operands is congruent to the sum of the indices of the operands. If the indices sum to greater than or equal to $2^n - 1$, then $2^n - 1$ is subtracted from the sum to prevent overflow.

$$
\begin{aligned}
\alpha^i \cdot \alpha^j &= \{x_{i,n-1}, \ldots, x_{i,2}, x_{i,1}, x_{i,0}\} \cdot \{x_{j,n-1}, \ldots, x_{j,2}, x_{j,1}, x_{j,0}\} \\
&= \begin{cases} \alpha^{(i+j)-(2^n-1)} & \text{if } (i+j) \geq 2^n - 1 \\ \alpha^{(i+j)} & \text{if } (i+j) < 2^n - 1 \end{cases}
\end{aligned}
$$

2.3.3 Division

Binary division of Galois operands is congruent to the difference of the indices of the operands. If the difference is negative, then the absolute value of the difference is subtracted from $2^n - 1$ to prevent underflow. If the difference is zero, then the quotient is α^0.

$$
\begin{aligned}
\alpha^i/\alpha^j &= \{x_{i,n-1}, \ldots x_{i,2}, x_{i,1}, x_{i,0}\}/\{x_{j,n-1}, \ldots x_{j,2}, x_{j,1}, x_{j,0}\} \\
&= \begin{cases} \alpha^{(2^n-1)-(j-i)} & \text{if } (i-j) < 0 \\ \alpha^{(i-j)} & \text{if } (i-j) > 0 \\ \alpha^0 & \text{if } (i-j) = 0 \\ ERROR & \text{if } (j-i) = 0 \end{cases}
\end{aligned}
$$

2.3.4 Logarithm

Logarithm is considered a unary operation in the Galois Field, where only one operand is required. This is because implicitly, the base of the logarithm operation in the Galois Field is 2. The logarithm of a Galois operand is congruent to its index.

$$log_2(\alpha^i) = i$$