論文 88-25-5-8

GF(2^m)上의 乘法과 乘法逆 計算을 위한 可變型 算術 演算시스템의 設計

(Design of Variable Arithmetic Operation Systems for Computing Multiplications and Multiplicative Inverses in GF(2^m))

朴 東 泳*, 姜 聖 洙*, 金 興 壽*

(Dong Young Park, Sung Su Kang and Heung Soo Kim)

要 約

本 論文에서는 Galois體 元素 次數의 modulo 演算性質을 이용하여 有限體 GF(2^m)上의 乘法과 乘法逆 計算을 위한 可變型 算術演算시스템의 構成理論을 提示하였다. 제안된 乘算器는 零元素制御部, 入力元素變換部, 循環式 mod(2^m-1)加算器部 및 出力元素變換部로 構成되었으며, 乘法逆 回路는 入力元素變換部, 反轉回路 및 出力元素變換部로 構成되었다. 이 시스템들은 入出力元素變換部를 共通으로 使用하여 回路面積의 節減이 可能하며, PLA와 모듈構造로 構成되어 回路變更없이 다른 有限體上의 算術演算시스템으로 轉換使用이 可能한 可變的 特性을 提供한다. 또한 本 設計方式은 回路構成의 單純性, 規則性, 擴張性 및 出力의 並發性 等의 特性에 기인하여 VLSI實現에 適合하다. 특히 乘法逆回路는 旣存에 發表된 方法들보다 高速으로 乘法逆元을 發生할 수 있는 特性이 期待된다.

Abstract

This paper presents a constructing theory of variable arithmetic operation systems for computing multiplications and multiplicative inverses in GF (2^m) based on a modulo operation of degrees on elements in Galois fields. The proposed multiplier is composed of a zero element control part, input element conversion part, recursive mod (2^m-1) adder part, and output element conversion part. And the multiplicative inverse circuit is constructed with an input element conversion part, inversion circuit, and output element conversion part. These systems can reduce reasonable circuit areas due to the common use of input/output element conversion parts, and the PLA and module structure provide a variable property capable of convertible uses as arithmetic operation systems over different finite fields. This type of designs gives simple, regular, expandable, and concurrent properties suitable for VLSI implementation. Especially, the multiplicative inverse circuit proposed here is expected to offer a characteristic of the high operational speed than conventional methods.

*正會員, 仁荷大學校 電子工學科

(Dept. of Elec. Eng., Inha Univ.)

接受日字 : 1987年 12月 28日

I. 序 論

有限體의 應用分野는 誤診訂正코드, 保安通信, 스윗칭理論 및 디지탈信號處理 등으로 요약할 수 있

다.[1-4] 특히 有限體 GF(2^m)은 單純性과 實用性에 기인하여 BCH코드,[1] Reed-Solomon코드[1,3] 및 保安通信의 暗號化와 解讀化[4]를 위해 중요한 역할을 하고 있다.

GF(2^m)에서 加法, 乘法 및 逆과 같은 算術演算은 서로 다른 特性을 갖는다. 일반적으로 加法은 용이한데 반해 乘法과 逆은 더욱 복잡한 演算을 요한다. 최근에는 이와 같은 算術演算을 실행하기 위해 設計되는 시스템들이 VLSI 實現을 위해 적합한 구조를 만족할 것을 요구받고 있다.

지난 십년간 有限體 GF(2^m)上에서의 乘算을 위해 여러가지 알고리즘[5,6,7]들이 提案되어 왔으나, 불행히도 이들은 電線通路(wire routing)와 制御問題로 인해 VLSI 구조에 적합치 못하였다. 그러나 Massey와 Omura,[8] McCanny와 McWhirter,[9] Yeh, Reed 및 Trung,[10] 그리고 Wang, Trung, Shao, Deutsch, Omura 및 Reed[11]에 의해 VLSI 구조에 적합한 乘算시스템의 發明이 이루어졌다. 그중 C. S. Yeh외[10]는 有限體 GF(2^m)上의 임의 두 基底元素 A와 B의 乘算을 P=AB+C인 형태로 변환하여 直並列入出力型 乘算셀에 의해 실행하도록 하였으며, C. C. Wang외[11]는 定規基底元素를 제곱하면 한 元素씩 循環的으로 쉬프트시킨 것과 같게 된다는 性質을 이용하여 Massey-Omura乘算器[8]를 보다 발전시켰다. 한편 逆元을 求하기 위해 종래에는 Euclid 알고리즘과 테이블調査 方法이 이용되어 왔으나 이 方法들은 VLSI 구조로의 實現이 용이하지가 못하였다. 그럼에도 불구하고 C. C. Wang외[11]는 Massey-Omura 乘算器를 이용하는 循環式 파이프라인型 逆回路를 開發하였다. 그러나 이들 乘算器는 한개의 Galosis體에 대한 乘算器로만 사용이 가능하며, 逆回路는 逆元搜索에 많은 시간이 소요되어 速度가 느린 단점을 포함하고 있다.

本 論文에서는 PLA의 出力並發性과 선택적 活性化 特性을 이용하여 有限體 元素 次數의 mod(2^m-1) 演算에 근거한 GF(2^m)上의 乘法과 乘法逆 計算을 위한 算術演算시스템의 設計方法을 提示하였다. 제안된 乘法과 乘法逆시스템은 GF(2^m)의 m보다 작은 다른 有限體 시스템으로의 轉換使用시 어떠한 回路變更도 필요로 하지 않지만 PLA의 프로그램과(乘算器의 경우) 入力制御에 의존한다. 또한 乘法과 乘法逆시스템은 共用回路를 사용함으로서 回路面積의 節減 特性을 제공하며 簡單性, 規則性, 擴張性, 모듈化 可能性 및 出力의 並發 特性 때문에 VLSI 構造에도 적합하다. 특히 本 論文에서 제안한 乘法逆 시스템은 현재까지 발표된 方法들보다 高速의 動作과 簡單한 構造의 特性을 제공한다.

本 論文의 構成은 다음과 같다. Ⅱ節에서는 Galois體 元素次數의 乘算性質을 分析한 후 이 性質을 만족하는 循環式 mod(2^m-1)加算器를 設計하고 아울러 코드割當 알고리즘을 제안하였다. Ⅲ節과 Ⅳ節에서는 GF(2^m)上의 乘法과 乘法逆 計算을 위한 새로운 算術演算 시스템의 構成알고리즘을 제안하고 有限體 GF(2^4)를 대상으로 시스템을 設計한 후 有限體 GF(2^3)에 대하여 提案된 시스템의 可變使用 例를 보였다.

Ⅱ. 有限體 元素 次數의 modulo 演算을 위한 數學的 背景

m이 陽의 整數일 때 有限體 GF(2^m)에는 基底元素集合 GF=$\{0, \alpha, \alpha^2, \cdots, \alpha^{2^m-2}, \alpha^{2^m-1}=1\}$이 항상 존재한다. 특히 零이 아닌 元素集合 GF'는 原始元素 α에 의해 生成되며, 이때 α는 GF(2)上에서 原始旣約多項式

$$E(\alpha)=\sum_{i=0}^{m-1}\mu_i\cdot\alpha^i$$

의 根이다(여기서, $\mu_i\in\{0, 1\}$). 따라서 集合GF'의 元素들은 $E(\alpha)$에 의해 m보다 작은 次數를 갖는 α의 慣用基底 多項式으로 表示할 수 있다. 즉, 有限體 GF(2^m)으로부터의 임의 두 α同型, α^a와 α^b는

$$\alpha^a=\sum_{i=0}^{m-1}f_i\cdot\alpha^i,\quad \alpha^b=\sum_{i=0}^{m-1}g_i\cdot\alpha^i;$$

$$f_i,\ g_i\in\{0, 1\},\ 0\le a, b\le 2^m-2 \qquad (1)$$

과 같이 나타낼 수 있다.

이제 本 論文에서 引用한 有限體 GF(2^m)의 몇가지 有用한 性質을 기술하면 다음과 같으며, 여기서 記術되지 않은 다른 性質들은 參考文獻에 準한다.[12]

1) $S\cdot 0=0\cdot S=0$;$S\in GF$ (2)

2) $S\cdot S^{-1}=1$;$S\in GF'$ (3)

3) $\alpha^a\cdot\alpha^b=\alpha^{a+b \bmod(2^m-1)}=\alpha^{f \bmod(2^m-1)}$;$\alpha^a, \alpha^b\in GF$, $f=a+b$ (4)

式(4)의 性質을 구체적으로 分析하기 위하여 本 論文에서 사용한 화살표 記號(⇄)를 다음과 같이 定義하였다.

[定義1]

a와 b가 $a\ge 0$, $b\ge 0$ 및 $a\ge b$인 整數일 때 화살표 記號 →와 ←는 아래와 같은 規則性을 제공하는 回一合 數雙 發生記號로서 Galois體 元素의 固有乘算에 어떤 영향도 주지 않는다.

1) $\alpha^a \tilde{\cdot} \alpha^b = (\alpha^a \cdot \alpha_1^b\ \alpha^{a-1} \cdot \alpha_1^{b+1} \cdots,\ \alpha^{b+1} \cdot \alpha_1^{a-1}\ \alpha^b \cdot \alpha^a)$

$[\alpha^a \tilde{\cdot} \alpha^b] = \{\alpha^a \cdot \alpha_1^b\ \alpha^{a-1} \cdot \alpha_1^{b+1} \cdots,\ \alpha^{b+1} \cdot \alpha_1^{a-1}\ \alpha^b \cdot \alpha^a\}$

2) $\alpha^b \tilde{\cdot} \alpha^a = (\alpha^b \cdot \alpha_1^a\ \alpha^{b+1} \cdot \alpha_1^{a-1} \cdots,\ \alpha^{a-1} \cdot \alpha_1^{b+1}\ \alpha^a \cdot \alpha^b)$

$[\alpha^b \tilde{\cdot} \alpha^a] = \{\alpha^b \cdot \alpha_1^a\ \alpha^{b+1} \cdot \alpha_1^{a-1} \cdots,\ \alpha^{a-1} \cdot \alpha_1^{b+1}\ \alpha^a \cdot \alpha^b\}$ (5)

〔定義2〕

集合 GF′와 同値인 두 集合을 $h_{GF'}$와 $v_{GF'}$라 하고 이들을 벡타空間으로 나타낸 것을 $H_{GF'}$와 $V_{GF'}$라 하자. 이때 $H_{GF'}$와 $V_{GF'}$의 모든 元素를 横 및 縦軸 方向으로 배열한 것을 $H_{GF'(X)}$와 $V_{GF'(Y)}$라 하고 각 軸의 a 및 b번째에 위치한 元素를 α_x^a와 α_y^b라 할 때, 同一根을 갖는 두 元素의 乘算은 式(6)과 같다.

$$\alpha_x^a \tilde{\cdot} \alpha_y^b = \alpha_x^a \cdot \alpha_y^b = \alpha^{a+b} = \alpha^f;$$

i) a→b 및 a←b에 대하여 각각 a≥b 및 a≤b,

ii) $\alpha_x^a \in H_{GF'(X)}$, $\alpha_y^b \in V_{GF'(Y)}$, $f=a+b$,
$0 \le a, b \le p^m-2$, 및 $0 \le f \le 2p^m-4$ (6)

그러면 Galois體 上에서 對角線的 根對稱構造를 갖는 同一根 乘算元素雙 集合의 일반적 表記에 필요한 理論을 앞서 定義한 記號와 用語를 사용하여 전개하면 定理 1 과 같다.

〔定理1〕

有限體 GF(p^m)上에서 零元素를 제외한 다른 모든 元素의 乘算시 同一根을 갖는 모든 乘算元素雙 集合을 $S(\alpha^f)$라 하면, $S(\alpha^f)$는

$$S(\alpha^f) = \{[\alpha_x^f \tilde{\cdot} \alpha_y^0],\ [\alpha_x^{1+f} \tilde{\cdot} \alpha_y^{p^m-2}]\}$$
$$= \{[\alpha_x^0 \tilde{\cdot} \alpha_y^f],\ [\alpha_x^{p^m-2} \tilde{\cdot} \alpha_y^{1+f}]\} \quad (7)$$
; 각 원소의 최대 차수는 p^m-2

과 같다. 式(7)은 GF(p^m)上에서 零元素를 제외한 모든 元素의 乘算을 나타낼 수 있는 一般式이며 동시에 對角線的 根對稱構造를 만족하는 式이다.

(證 明)

$$H_{GF'(X)} \cdot V_{GF'(Y)} = (\alpha_x^0\ \alpha_x^1 \cdots,\ \alpha_x^{p^m-2}\ \alpha_x^{p^m-1}\ \alpha_x^{p^m} \cdots,\ \alpha^{2p^m-4})$$
$$= (\alpha_x^0\ \alpha_x^1 \cdots,\ \alpha_x^{p^m-2}\ 1,\ \alpha_x \cdots,\ \alpha^{p^m-3}) \quad (8)$$

式(8)을 分割하여

1循環部 $= (\alpha_x^0\ \alpha_x^1 \cdots,\ \alpha^{p^m-2})$

2循環部 $= (\alpha^{p^m-1}\ \alpha_y^{p^m} \cdots,\ \alpha^{2p^m-4})$

과 같이 놓으면 定義 1 과 2 에 의해

1循環部 $= (\alpha_x^0\ \alpha_x^1\ \alpha_x^2 \cdots,\ \alpha^{p^m-2})$
$= (\alpha_x^0 \tilde{\cdot} \alpha_y^0,\ \alpha_x^1 \tilde{\cdot} \alpha_y^0,\ \alpha_x^2 \tilde{\cdot} \alpha_y^0, \cdots, \alpha_x^{p^m-2} \tilde{\cdot} \alpha_y^0) = \alpha_x^f \tilde{\cdot} \alpha_y^0$
$= (\alpha_x^0 \tilde{\cdot} \alpha_y^0,\ \alpha_x^0 \tilde{\cdot} \alpha_y^1,\ \alpha_x^0 \tilde{\cdot} \alpha_y^2, \cdots, \alpha_x^0 \tilde{\cdot} \alpha_y^{p^m-2}) = \alpha_x^0 \tilde{\cdot} \alpha_y^f$
; $0 \le f \le p^m-2$ (9)

2循環部 $= (\alpha^{p^m-1}, \alpha^{p^m}, \alpha^{p^m+1}, \cdots, \alpha^{2p^m-4})$
$= (\alpha_x^1 \tilde{\cdot} \alpha_y^{p^m-2}, \alpha_x^2 \tilde{\cdot} \alpha_y^{p^m-2}, \alpha_x^3 \tilde{\cdot} \alpha_y^{p^m-2}, \cdots, \alpha_x^{p^m-2} \tilde{\cdot} \alpha_y^{p^m-2})$
$= \alpha_x^{1+f} \tilde{\cdot} \alpha_y^{p^m-2}$
$= (\alpha_x^{p^m-2} \tilde{\cdot} \alpha_y^1, \alpha_x^{p^m-2} \tilde{\cdot} \alpha_y^2, \alpha_x^{p^m-2} \tilde{\cdot} \alpha_y^3, \cdots, \alpha_x^{p^m-2} \tilde{\cdot} \alpha_y^{p^m-1})$
$= \alpha_x^{p^m-2} \tilde{\cdot} \alpha_y^{1+f}$
; $0 \le f \le p^m-3$ (10)

그러므로, 式(9)와 (10)으로부터

$$S(\alpha^f) = \{[\alpha_x^f \tilde{\cdot} \alpha_y^0],\ [\alpha_x^{1+f} \tilde{\cdot} \alpha_y^{p^m-2}]\}$$
$$= \{[\alpha_x^0 \tilde{\cdot} \alpha_y^f],\ [\alpha_x^{p^m-2} \tilde{\cdot} \alpha_y^{1+f}]\}$$

단, 각 元素의 最大次數는 p^m-2이다. 또한 $\alpha_x^f \tilde{\cdot} \alpha_y^0 = \alpha_x^0 \tilde{\cdot} \alpha_y^f$ 및 $\alpha_x^{1+f} \tilde{\cdot} \alpha_y^{p^m-2} = \alpha_x^{p^m-2} \tilde{\cdot} \alpha_y^{1+f}$ 이므로 次數 合이 同一한 乘算元素雙은 對角線上에서 根對稱構造를 이룬다. (證明끝).

定理 1 의 結果를 이용하여 乘算根의 次數를 乘算元素 次數의 合形態로 나타낼 수 있음을 定理 2 에서 보였다.

〔定理2〕

有限體 GF(p^m)上에서 零元素를 제외한 임의 두 元素의 乘算시 根元素의 次數는 式(11)의 規則的인 根 條件을 만족한다.

$$f = \begin{cases} a+b & ;\ a+b \le p^m-2 \\ a+b-(p^m-1) & ;\ a+b \ge p^m-1 \end{cases} \quad (11)$$

(證 明)

定理 1 에서 1循環部는 $0 \le f \le p^m-2$ 이므로

$\alpha_x^a \tilde{\cdot} \alpha_y^b = \alpha_x^f \tilde{\cdot} \alpha_y^0 = \alpha_x^0 \tilde{\cdot} \alpha_y^f$, $\therefore f = a+b$

2循環部는 $p^m-1 \le f \le 2p^m-4$ 이므로

$\alpha_x^a \tilde{\cdot} \alpha_y^b = \alpha_x^{1+f} \tilde{\cdot} \alpha_y^{p^m-2} = \alpha_x^{p^m-2} \tilde{\cdot} \alpha_y^{1+f}$, $\therefore f = a+b-(p^m-1)$

(證明끝).

定理 2 는 乘算根을 乘算元素 次數의 計算으로부터 直接的으로 구할 수 있음을 보여 주며, 이는 또한 앞서 기술한 有限體 乘法 性質3 을 만족한다.

1. 코드화 알고리즘

有限體 GF(2^m)에서 零이 아닌 모든 元素의 次數는 一連의 陽의 整數 $1,2,\cdots,2^m-2,\ 2^m-1$를 構成하므로, 集合 GF로부터의 α同型을 α同型의 次數β로 定義하고 β와 同値인 m비트 2進벡타를 $B_m(\beta)$라 하면

$$\alpha : \alpha^\beta \to \beta \triangleq B_m(\beta)\ ;\ \text{i)}\ \alpha^0 = \alpha^{2^m-1}$$
ii) $\beta \in \{0,1,2,\cdots,2^m-1\}$,
$B_m(\beta) \in \{0,1\}$ (12)

관계가 성립한다. 또한 置換된 元素의 復元을 위하여 式(12)에 대한 逆을

$$B_m(\beta) \triangleq \beta \rightarrow \alpha^{\beta} : \alpha \qquad (13)$$

로 定義하였다. 式(12)와 (13)은 GF(2^m)에서 乘法과 乘法逆 計算을 위한 코드화 알고리즘이다. 이때 式(12)와 (13)에서 α^0元素 대신에 α^{2^m-1} 元素가 사용되었으므로 式(11)의 循環境界値는

$$f = \begin{cases} a+b & ; a+b \le p^m-1 \\ a+b-(p^m-1) & ; a+b \ge p^m \end{cases} \qquad (14)$$

과 같이 再調整되어야만 한다. 式(12)와 (13)에 의해 有限體 GF(2^m)上에서 임의 두 α同型間의 乘算은 式(14)를 만족하는 두개 m비트 2進벡타間의 加算과 같다고 假定할 수 있다. 그러므로 式(14)를 만족하는 循環式 mod(2^m-1) 2進加算器의 設計가 요구된다.

2. 循環式 mod(2^m-1) 2進 加算器의 設計

m 비트 2進벡타의 加算은 式(14)를 만족하기 위해 循環境界値2^m-1을 基準으로 1次 및 2次의 2개 演算部로 구분되었다. 각 벡타에 대한 算術演算은 mod 2와 캐리(carry)를 취함으로서 實行되어 지며, 코드화 알고리즘에 의해 두乘算元素에 割當된 2進벡타가

$B_m(a) = (A_m, A_{m-1}, \cdots, A_i, \cdots, A_2, A_1)$ 과
$B_m(b) = (B_m, B_{m-1}, \cdots, B_i, \cdots, B_2, B_1)$

과 같을 때 1次 및 2次 演算部의 算術演算式은 각각 式(15) 및 (16)과 같다.

$$\begin{array}{l} (A_m, \ A_{m-1}, \cdots, A_i, \ \cdots, A_2, \ A_1) \\ (B_m, \ B_{m-1}, \cdots, B_i, \ \cdots, B_2, \ B_1) \\ \hline (C_m, \ C_{m-1}, \ C_{m-2}, \cdots, C_{i-1}, \cdots, C_1) \\ \quad (K_m, \ K_{m-1}, \cdots, K_i, \ \cdots, K_2, \ K_1) \end{array}$$

$; A_i, \ B_i, \ C_i, \ K_i \in \{0,1\}, \ K_i = A_i \oplus B_i \oplus C_{i-1},$
$C_i = A_iB_i + (A_i \oplus B_i) \cdot C_{i-1}, \ C_0 = 0$ 및 $i = 1,2,\cdots,m$

(15)

$$\begin{array}{l} (K_m, \ K_{m-1}, \ \cdots, K_i, \ \cdots, K_2, \ K_1) \\ \hline (C_{mm}, \ C_{mm-1}, \ C_{mm-2}, \cdots, C_{mi-1}, \cdots, C_{m1}, \ C_m) \\ \quad (L_m, \ L_{m-1}, \ \cdots, L_i \ , \cdots, L_2 \ , \ L_1) \end{array}$$

$; K_i, \ L_i, \ C_{mi}, \ C_m \in \{0,1\}, \ L_i = K_i \oplus C_{mi-1},$
$C_{mi} = K_i \cdot C_{mi-1}, \ C_{m0} = C_m, \ C_{mm} = 0, i = 1,2,\cdots,m$

(16)

式(15)와 (16)에서 C_i와 C_{mi}는 각각 1次 및 2次演算시 i번째 벡타演算에 의해 발생되는 캐리를 나타낸다. 그림 1에는 K_i와 L_i를 計算하기 위한 半加算器가 單位셀로서 도시되었다.

그림 1의 單位셀을 이용하여 式(15)와 (16)을 回路實現하면 그림 2와 같다.

그림 2에서와 같이 mod(2^m-1) 2進 加算器는 3段의 파이프라인構造를 가진다. 左側 2段과 右側 1段의 單位셀들은 각각 1次 및 2次 演算部 回路를 나타낸다. 이때 r과 w를 定常 및 剩餘入力이라 하고 이들이 $1 \le r \le m$ 및 $r+1 \le w \le m$인 범위의 값을 가진다면, 剩餘入力으로부터의 캐리C_w는 式(15) 에서 定常入力의 마지막 2進벡타 演算시 發生된 C_r에 의해 式(17)과 같이 表示될 수 있다.

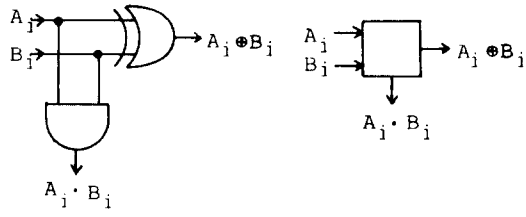

그림 1. K_i와 L_i 計算을 위한 單位 셀
(a) 單位 셀 (b) 記號
Fig. 1. An unit cell to compute K_i and L_i.
(a) unit cell. (b) symbol.

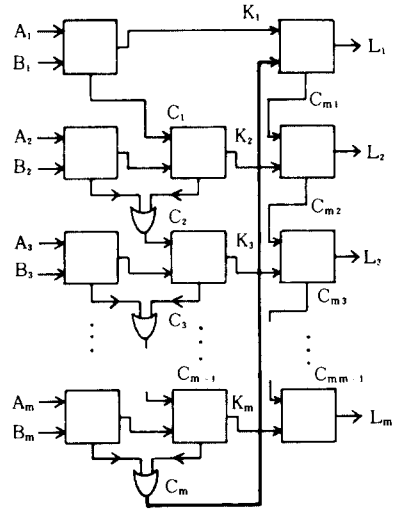

그림 2. 循環式 mod(2^m-1) 2進 加算器
Fig. 2. A recursive mod(2^m-1) binary adder.

$$C_w = A_wB_w + (A_w \oplus B_w)\cdot C_r \quad ; C_r = A_rB_r + (A_r \oplus B_r)\cdot C_{r-1} \tag{17}$$

式(17)은 만약 $A_w \oplus B_w = 1$이면 항상 $C_w = C_r$ 임을 함축한다. 그러므로 循環式 mod(2^m-1) 2進 加算器는 어떤 回路變更없이 모든 剩餘入力雙에 補數의 2進벡타를 入力시킴으로서 자유롭게 分割的으로 사용할 수 있다. 그러나 C_i와 C_{mi}의 順次的 傳播에 의한 不可避한 게이트 遲延과 出力의 不一致가 존재한다.

Ⅲ. GF(2^m)上의 可變型 乘算器

이 節에서는 PLA와 前節에서 提案한 mod(2^m-1) 加算器를 이용하여 GF(2^m)上 元素들간의 乘法演算을 實行하는 可變型 乘算器 構成理論을 論하였다.

그림 3 은 GF(2^m)上의 並列入出力 可變型 乘算器 構成圖이다.

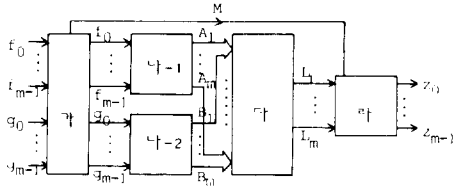

그림 3. GF(2^m)上의 並列入出力 可變型 乘算器
Fig. 3. A parallel-in, parallel-out variable multiplier in GF(2^m).

그림 3 에서 "가," "나-1,2," "다," 그리고 "라" 는 각각 零元素制御部, 入力元素變換部, 循環式 mod(2^m-1) 加算器部 및 出力元素變換部를 나타낸다. 각 構成部의 動作特性은 다음과 같다.

零元素制御部는 循環式 mod(2^m-1) 加算器가 "0" 元素를 制御할 수 없기 때문에 이의 獨立的인 制御를 위해 導入되었다. 零元素의 獨立的 制御는 m入力線, 2積項線 및 1出力線의 한개 OR-AND PLA에 의해 式(18)을 만족하도록 構成되었다.

$$M = (f_{m-1}+f_{m-2}+\cdots+f_1+\cdots+f_0)\cdot(g_{m-1}+g_{m-2}+\cdots+g_1+\cdots+g_0) = \begin{cases} 0 & ; \text{iff } {}^{\forall}f_i \text{ and/or } {}^{\forall}g_i = 0 \\ 1 & ; \text{otherwise} \end{cases} \tag{18}$$

式(18)에서 M은 OR-AND PLA의 出力이며 "라" 部의 2m入力線과 AND 接續으로 連結되었다. 만약 零元素가 演算에 不必要 하다면 零元素制御部는 直接的으로 제거될 수 있으며 目標시스템은 더욱 簡單해 질 수 있다.

入力元素變換部는 m入力線, 2^m-1 積項線 및 m出力線을 갖는 두개의 AND-OR PLA로 構成되었으며, 이때 2^m-1 積項線은 2^m-1 個의 零이 아닌 元素들과 一對一 對應關係로 割當되었다. 한편 PLA를 프로그램하기 前에 集合 GF′의 모든 基底元素들은 mod $E(\alpha)$ 演算에 의해 α同型의 多項式으로 表示되어야 하며, 이 條件은 式(12)를 式(19)와 같이 나타낼 수 있게 해준다.

$$\sum_{i=0}^{m-1} f_i\cdot\alpha^i : \alpha^\beta \rightarrow \beta \triangleq B_m(\beta) \ ;$$
$$f_i,\ B_m(\beta) \in \{0,1\},\ \beta \in \{0,1,2,\cdots,2^m-1\} \tag{19}$$

式(19)에서 f_i와 $B_m(\beta)$는 각각 同一積項線上의 AND와 OR平面에 프로그램되어야만 한다. 여기서 "나-1, 2" 部는 同一構造이므로 두 構成部의 프로그램順序는 一致해야만 한다.

循環式 mod(2^m-1) 2進 加算器部는 Ⅱ節에 準한다.

出力元素變換部는 入力元素變換部와 對稱的 構造를 갖는다. 만약 $\alpha^a\cdot\alpha^b=\alpha^r$가

$$\sum_{i=0}^{m-1} f_i\cdot\alpha^i \cdot \sum_{i=0}^{m-1} g_i\cdot\alpha^i = \sum_{i=0}^{m-1} z_i\cdot\alpha^i$$

와 對應한다면, 乘算根은

$$B_m(f) \triangleq f \rightarrow \alpha^r : \sum_{i=0}^{m-1} z_i\cdot\alpha^i \ ;$$
$$B_m(f),\ z_i \in \{0,1\},\ f \in \{0,1,2,\cdots,2^m-1\} \tag{20}$$

과 같이 求해지며, 이때 $B_m(f)$와 z_i는 각각 同一積項線上의 AND와 OR平面에 프로그램되어져야만 한다. 附加的 特性으로서, 出力元素變換部는 循環式 mod(2^m-1) 加算器部로 부터의 不一致 出力의 並發이 가능하도록 해준다. 이것은 PLA의 規則性에 기인하여 가능하다.

그림 4 는 GF(2^4)上 可變型 乘算器의 實際例를 보여 주며, 여기서 既約多項式은 $E(\alpha)=\alpha^4+\alpha+1$이 사용되었다.

그림 4 에 例示된 시스템은 回路變更없이 m= 4 보다 작은 次數를 갖는 다른 Galois體의 乘算器로 轉換할 수 있다. 이 경우 入力元素變換部 PLA는 回路分割技法이 要求되며 이 技法은 그림 5 에 提示되었다.

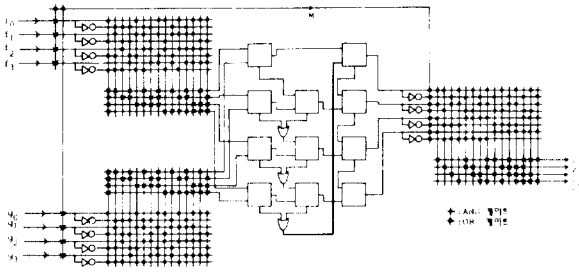

그림 4. E(α)=α⁴+α+1에 대한 GF(2⁴)上 可變型 乘算器

Fig. 4. A variable multiplier in GF(2⁴) for E(α)=α⁴+α+1.

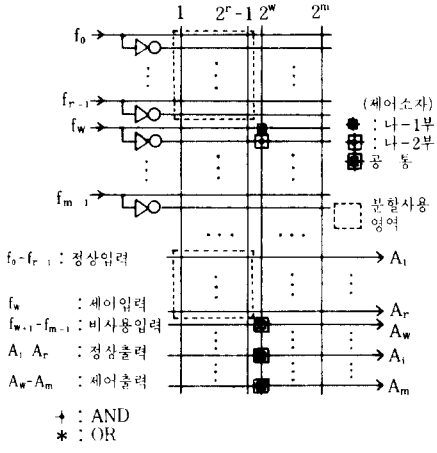

그림 5. 入力元素變換部 PLA의 回路分割技法

Fig. 5. A circuit partition technique for the input element conversion part PLA's.

그림 5에서 非使用領域의 1入力線, 1積項線 및 m−r 出力線이 循環式 mod(2^m−1) 加算器의 剩餘入力을 制御하기 위해 사용되었으나 實質的인 外部制御線은 한개의 f_w 또는 g_w이다. 즉 $f_w=g_w=1$ 이면 $A_i \oplus B_i = 1$이며 여기서 i와 w는 $w \le i \le m$와 $w=r+1$이다. 이 事實은 그림 4의 乘算器에 容易한 制御性과 自由로운 分割特性을 제공한다.

그림 6은 GF(2⁴)上의 乘算器를 GF(2³)上의 乘算器로의 轉換使用 例를 보여 주며 이때 $E(\alpha)=\alpha^3+\alpha+1$이 使用되었다.

本 節에서 提案한 GF(2^m)上 可變型 乘算器의 일반적 特性을 要約하면 다음과 같다.

첫째, 演算速度는 PLA, 加算셀, 플립플롭 및 레지스터 等을 각각 單位素子遲延으로할 때, 本 方法은 PLA와 가산셀에 의한 2m+2遲延特性을 가지며

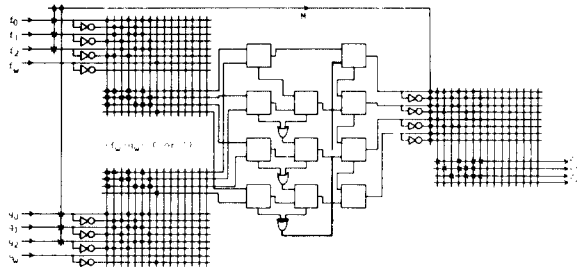

그림 6. 그림 4 乘算器를 $E(\alpha)=\alpha^3+\alpha+1$에 대한 GF(2³)上 乘算器로의 轉換例

Fig. 6. An example of converting the multiplier in Fig. 4 to one in GF(2³) for $E(\alpha)=\alpha^3+\alpha+1$.

이는 C. S. Yeh외[10]의 플립플롭에 의한 3m遲延 보다는 빠르고 C. C. Wang외[11]의 PLA와 레지스터에 의한 2m+1 遲延보다는 느린 動作特性을 제공한다.

둘째, 統 하드웨어는 $6m\times(2^m-1)+3m\times 2^m+(m+1)\times 2$ 규모의 PLA, 3m−1加算셀 및 3m인버터가 소요된다. 단, PLA가 아닌 固定素子 사용시는 前者에 對比하여 約 1/3규모로 構成이 가능하다.

셋째, 本 可變型 乘算器는 C. S. Yeh외[10]와 C. C. Wang외[11]의 경우와 같이 簡單性, 規則性, 對稱性, 出力並發性 및 모듈 構造에 기인하여 VLSI 實現에 適合하다.

넷째, PLA는 標準 AND−OR (또는 OR−AND)型이 사용되었으므로 NOR−NOR 또는 NAND−NAND 型으로 轉換이 容易하다.

또한 他 方法[10,11]이 갖지 않는 本 方法의 重要한 몇가지 特性을 기술하면 다음과 같다.

첫째, 本 方法은 既約多項式과 m이 可變的이므로 回路變更없이 프로그램과 容易한 入力制御만에 의해 m次數 以下의 他 有限體上 乘法演算器로 轉換使用이 가능하며, 필요시에 그림 3의 入出力元素變換部("나-1,2"및"라"部)의 除去로 入出力이 乘法元素 次數型의 乘算器로 轉換이 가능한 우수한 可變的 特性을 제공한다.

둘째, 本 方法은 計算過程이 不必要하고 規則的인 回路構造를 가지므로 他 方法[10,11]에 비해 시스템構成方法이 簡單하다.

Ⅳ. GF(2^m)上의 乘法逆 計算을 위한 高速演算 시스템

이 節에서는 PLA를 이용하여 GF(2^m)上에서 乘法逆을 구하기 위한 高速演算시스템이 提示되었다.

제안된 시스템은 그림3의 可變型 乘算器의 모든 動作 特性을 包含한다. Ⅱ節의 코드화 알고리즘에 의해 각 元素에 割當된 m비트 2進벡타들은 $\alpha^a \cdot \alpha^b = 1$ 이면 $\alpha^b = \alpha^a$ 이므로, α^a 元素의 乘法逆은

$$\sum_{i=0}^{m-1} g_i \cdot \alpha^i : \alpha^b \rightarrow \bar{a} \triangleq B_m(a);$$

$$g_i,\ B_m(a) \in \{0,1\},\ a, b \in \{0,1,2,\cdots,2^m-2\},\ (21)$$

과 같이 m個 並列인버터에 의해 쉽게 구할 수 있다. 그러나 α^{2^m-1} 元素는 α^{2^m-1} 이 모든 出力을 零狀態로 만들며 이 結果는 零元素의 狀態와 같기 때문에 α^{2^m-1} α^{2^m-1}과 같은 特別한 制御가 要한다. 이와 같은 類型의 特殊制御는 그림7과 같이 m入力線, m 積項線 및 1出力線을 갖는 1個 OR-AND PLA와 1入力線, m積項線 및 m出力線을 갖는 1個 AND-OR PLA로 式(22)를 만족하는 反轉回路를 構成함으로써 가능한데, 이때 L_i는

$$L_i = A_i + \prod_{i=1}^{m} A_i \ ;\ i = 1,2,\cdots,m \qquad (22)$$

을 함축한다. 따라서 GF(2^m)上의 乘法逆 計算을 위한 高速演算시스템을 그림8과 같이 構成할 수 있다.

그림8에서 "마"와 "사"는 그림3의 入出力元素變換部의 複製回路이며, "바"는 그림7의 反轉回路를 나타낸다. 그림8의 算術演算시스템은 乘法逆을 提供하며 그림3의 可變型 乘算器에 대하여 한개의 反轉回路를 제외하고는 어떤 附加回路도 使用되지 않았다. 이 경우 그림3의 "라"部 制御線M은 不必要하므로 그림8 시스템의 定常動作에 영향을 주지 않도록 除去되거나 또는 M=1 狀態를 유지해야만 한다. 그림9에는 GF(2^4)上에서 乘法逆 計算을 위한 並發特性의 高速演算시스템이 例示되었으며 이때 사용된 既約多項式은 $E(\alpha) = \alpha^4 + \alpha + 1$ 이다.

그림10은 그림9의 GF(2^4)上 乘法逆 計算을 위한 高速演算시스템을 回路變更없이 PLA 프로그램만에 의해 GF(2^3)上의 乘法逆 演算시스템으로 轉換使用한 例이며 여기서 $E(\alpha) = \alpha^3 + \alpha + 1$이 使用되었다.

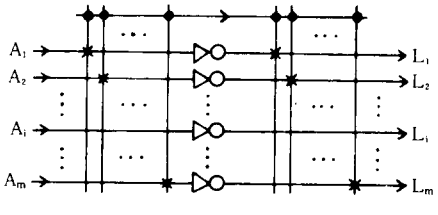

그림7. 反轉回路
Fig. 7. An inversion circuit.

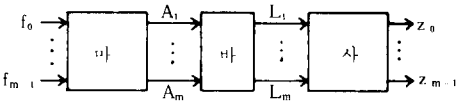

그림8. GF(2^m)上의 乘法逆 計算을 위한 可變型 算術演算시스템
Fig. 8. A variable arithmetic operation system for computing multiplicative inverses in GF(2^m).

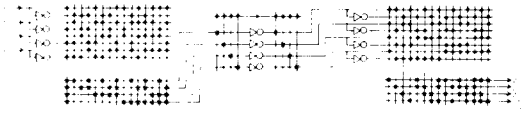

그림9. $E(\alpha) = \alpha^4 + \alpha + 1$에 대한 GF(2^4)上의 乘法逆을 위한 高速計算시스템
Fig. 9. A fast computing system for multiplicative inverses in GF(2^4) for $E(\alpha) = \alpha^4 + \alpha + 1$.

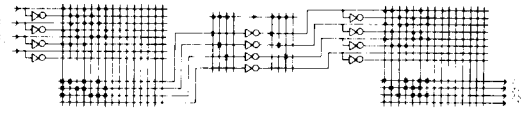

그림10. 그림9 시스템의 $E(\alpha) = \alpha^3 + \alpha + 1$에 대한 GF(2^3)上 시스템으로의 轉換例
Fig. 10. An example of converting the system in Fig. 9 to one in GF(2^3) for $E(\alpha) = \alpha^3 + \alpha + 1$.

本 節에서 提案한 GF(2^m)上 可變型 乘法逆 演算시스템은 前節에서 제안한 GF(2^m)上 可變型 乘法演算시스템의 모든 動作特性을 包含하여 아울러 다음과 같은 附加的 特性을 提供한다.

첫째, m이 同一할 때 GF(2^m)上 乘法演算시스템의 一部回路에 簡單한 反轉回路 첨가로 回路構成이 가능하므로, 共用回路 使用에 따른 回路面積 節減이 가능하다.

둘째, PLA에 의한 單位遲延 4의 函數獨立的인 演算速度를 제공하며, 이는 比較搜索에 時間이 많이 소요되는 C. C. Wang외[11]의 循環型 乘法逆回路보다 우수한 動作特性이다.

V. 結 論

本 論文에서는 有限體 元素次數의 modulo演算性質을 이용하여 GF(2^m)上의 乘法과 乘法逆을 計算할 수 있는 새로운 方式의 算術演算시스템 設計方式을 提案하였다. 제안된 乘法演算시스템은 旣存의 方法[10,11]과 演算速度, 回路素子數 및 VLSI 實現 可能性 面에서 大同小異한 特性이 기대되며, 특히 可變的 特性과 簡單한 構成節次는 本 方法이 우수한 것으로 사려된다. 또한 乘法逆 시스템은 乘法시스템의 모든 特性을 포함하며 他 方法[11]보다 動作速度, 回路構成의 簡單性 및 可變的 特性面에서 우수한 것으로 나타났다. 그러나, m의 증가에 따른 回路의 大型化는 他 方法과 마찬가지로 불가피하여 차후 이의 解決이 硏究課題이다. 따라서 本 論文에서 제안한 GF(2^m)上 可變型 算術演算시스템은 有限體 GF(2^m) 上體元素를 記號로 사용하며 아울러 GF(2^m)上 算術演算이 要求되는 BCH 코드, RS코드 및 保安通信器의 符號器와 復號器를 위한 算術演算部에 應用될 수 있을 것으로 기대한다.

參 考 文 獻

[1] S. Lin and D.J. Costello, Error Control Coding. New Jersey: Prentice-Hall, 1983.

[2] B. Benjauthrit and I.S. Reed, "Galois switching functions and their applications," *IEEE Trans. Compt.*, vol. C-25, pp. 78-86, Jan. 1976.

[3] I.S. Hsu, I.S. Reed, T.K. Trung, K. Wang, C.S. Yeh, and L.J. Deutsch, "The VLSI implementation of a Reed-Solomon encoder using Berlekamp's bit-serial multiplier algorithm," *IEEE Trans. Compt.*, vol. C-33, pp. 906-911, Oct. 1984.

[4] S. Berkovits, J. Kowalchuk, and B. Schanning, "Implementing public key scheme," *IEEE Commun. Mag.*, vol. 17, pp. 2-3, May 1979.

[5] T.C. Bartee and D.I. Schneider, "Computation with finite fields," Inform. Contr., vol. 6, pp. 79-98, Mar. 1963.

[6] B.A. Laws and C.K. Rushforth, "A cellular-array multiplier for GF (2^m)," *IEEE Trans. Compt.*, vol. C-20, pp. 1573-1578, Dec. 1971.

[7] R.G. Gallagher, Information Theory and Reliable Communication. New York: Wiley, 1968.

[8] J.L. Massey and J.K. Omura, "Computational method and apparatus for finite field arithmetic," U.S. Patent application, submitted 1981.

[9] J.V. McCanny and J.G. McWhirter, "Completely iterative pipelined multiplier array suitable for VLSI," *IEEE Proc. G, Electronic Circuits and Systems*, vol. 129, no. 2, pp. 40-46, Apr. 1982.

[10] C.S. Yeh, I.S. Reed, and T.K. Trung, "Systolic multipliers for finite fields GF(2^m)," *IEEE Trans. Compt.*, vol. C-33, pp. 357-360, Apr. 1984.

[11] C.C. Wang, T.K. Trung, H.M. Shao, L.J. Deutsch, J.K. Omure, and I.S. Reed, "VLSI architecture for computing multiplications and inverses in GF (2^m)," *IEEE Trans. Compt.*, vol. C-34, pp. 709-717, Aug. 1985.

[12] R. Lidl and G. Pilz, Applied Abstract Algebra. New York: Springer-Verlag, 1984.

[13] B.S. Shin, D.Y. Park, and H.S. Kim, "A constructing theory for GF (p^m) multipliers based on the modulo arithmetic of the multiplication element powers," Proceedings of KIEE Fall Conference, vol. 10, no. 1, pp. 522-525, Nov. 1987.