通信情報保護學會誌
第6卷 第1號, 1996. 3

GMW 계열의 특성 분석

염 흥 열*, 김 춘 수**, 이 홍 섭**

요 약

본 고에서는 참고문헌 [9]을 바탕으로 선형복잡도 특성이 우수하고 이상적인 자기상관함수 특성을 갖는 GMW 계열의 특성을 분석한다. 이를 위하여 먼저 LFSR 계열의 특성방정식을 제시한 후, 트레이스함수를 이용하여 GMW 계열을 정의한다. 그리고 GMW 계열의 자기상관함수를 구하며, 차수가 6인 GMW 계열의 생성기의 구조를 제시한다. 마지막으로 GMW 계열의 선형복잡도와 갯수를 구하는 수식을 유도한다.

제1장 트레이스 함수 및 난수 계열

정수 M이 J에 의해 나누어 질 때, 트레이스 함수 $tr_J^M(\alpha)$는 식 (1)과 같이 $GF(2^M)$상의 원소 α를 부분체 $GF(2^J)$ 상의 원소로 사상한다.

$$tr_J^M(\alpha) = \sum_{i=0}^{(M/J)-1} \alpha^{2^{Ji}} \quad (1)$$
$$= \alpha + \alpha^{2^J} + \alpha^{2^{2J}} + \cdots + \alpha^{2^{(M/J-1)J}}$$

트레이스 함수는 다음 5가지 특성을 만족한다.

① $GF(2^M)$ 상의 임의의 원소 α와 이의 복소근에 대한 트레이스 값은 식 (2)와 같이 동일하다.

$$tr_J^M(\alpha) = tr_J^M(\alpha^{2^{Ji}}),\ i = 1, \cdots, M-1 \quad (2)$$

② $GF(2^M)$상의 임의의 원소 α와 β, $GF(2^J)$ 상의 원소 a와 b에 대해, 식 (3)이 만족하므로 트레이스 함수는 선형(Linearity) 특성을 갖는다.

$$tr_J^M(a\alpha + b\beta) = atr_J^M(\alpha) + atr_J^M(\beta) \quad (3)$$

③ $GF(2^J)$내의 임의의 원소 b가 주어진 경우, $tr_J^M(\alpha) = b$을 만족하는 $GF(2^M)$내의 원소의 개수는 2^{M-J}개 이다.

④ 실수 연산 상에서 $GF(2^M)$상의 0이 아닌 임의의 원소 γ에 대해, 식 (4)가 성립한다.

$$\sum_{\alpha \in GF(2^M)} (-1)^{tr_1^M(\gamma_\alpha)} = 0 \quad (4)$$

⑤ $GF(2^M)$상의 임의의 원소 α에 대해, 식 (5)가 성립한다.

$$tr_1^M(\alpha) = tr_1^J(tr_J^M(\alpha)) \quad (5)$$

LFSR(Linear Feedback Shift Register) 계열을 $\overline{b}$라 하고, 계열의 계열 요소(Sequence

* 순천향대 공과대학 전기전자공학부
** 한국전자통신연구소

Element)를 $b_n(n = 1, 2, \cdots)$이라 하자. r단 쉬프트 레지스터로 생성되는 LFSR 계열의 선형 반복 방정식(Linear Recursive Equation)과 이에 대응되는 r 차의 특성방정식(Characteristic Equation)은 각각 식 (6)과 같다.[1-7]

$$b_n + \sum_{i=1}^{r} m_i b_{n-i} = 0, \; n \geq r \qquad (6)$$
$$c(x) = x^r + \sum_{i=1}^{r} m_i x^{r-i}$$

일반적으로 특성방정식 $c(x)$는 $GF(2^M)$상의 원시원(Primitive Element) α를 근으로 갖도록 선정된다. 즉, $\alpha \in GF(2^M)$은 $c(x)$, 원시다항식(Primitive Polynomial)의 근이다. 따라서 $c(\alpha) = 0$이다.

(정리 1) 특성방정식 $c(x)$가 M차일 경우, 계열 $b_n = tr_1^M(\alpha^n)$은 선형 반복방정식 $b_n = \sum_{i=1}^{M} m_i \cdot b_{n-i}$의 '0'이 아닌 해이다.

(증 명) 식 (7)의 관계식이 성립하므로 정리 1은 증명될 수 있다.

$$\begin{aligned} & b_n - \sum_{i=1}^{M} m_i b_{n-i} \\ & = tr_1^M(\alpha^n) - \sum_{i=1}^{M} m_i \cdot tr_1^M(\alpha^{n-i}) \qquad (7) \\ & = tr_1^M\{\alpha^{n-M}(\alpha^M - m_1\alpha^{M-1} - m_2\alpha^{M-2} - \cdots - m_M)\} \\ & = tr_1^M\{\alpha^{n-M} \cdot c(\alpha)\} = tr_1^M\{\alpha^{n-M} \cdot 0\} \\ & = 0 \end{aligned}$$

(증명완료)

난수 계열 $\bar{b}$에 대한 실계열(Real Sequence) $\bar{a}$은 식 (8)과 같이 정의된다.

$$a_n = (-1)^{b_n} \qquad (8)$$

제 2 장 GMW 계열

제1절 GMW 계열 정의 및 이의 자기상관함수[9]

GMW 계열은 Gordon, Mills, 그리고 Welch에 의해 제안된 선형복잡도가 우수한 부호이다.[9] 합성수 M이 식 (9)와 같은 두 정수 J와 K의 곱이고,

$$M = JK \qquad (9)$$

α가 $G(2^M)$상의 원시원이며, 정수 $r(1 \leq r < 2^J-1)$과 2^J-1가 서로소 관계(Relatively Prime)일 경우, GMW 계열의 계열 요소는 식 (10)과 같이 정의된다.

$$b_n = tr_1^J\{tr_J^M(\alpha^n)\}^r\} \qquad (10)$$

$r = 1$인 경우 GMW 계열은 식 (11)에서 알 수 있듯이 최대장 계열(Maximal Length Sequence)이 됨을 알 수 있다.

$$b_n = tr_1^J\{tr_J^M(\alpha^n)\} = tr_1^M(\alpha^n) \qquad (11)$$

(정리 2) $GF(2^J)$상의 계열 $\bar{b}_n'$이 식 (12)와 같고, 정수 T가 식 (13)과 같이 정의된다면,

$$b_n' = tr_J^M(\alpha^n) \qquad (12)$$
$$T = (2^M-1)/(2^J-1) \qquad (13)$$

계열 $\bar{b}_n'$의 T개의 연속적인 계열 요소에는 정확히 $(2^{M-J}-1)/(2^J-1)$개의 '0' 요소가 있다.

(증 명) 식 (13)에서 α^T의 차수(Order)는 2^J-1이다. 따라서 $\alpha^T \in GF(2^J)$이다. 따라서 트레이스 함수의 두번째 특성을 이용하면 식 (14)를 구할 수 있다.

$$tr_j^M(\alpha^n) = tr_j^M(\alpha^{n+iT} \cdot \alpha^{-iT}) \quad (14)$$
$$= tr_j^M(\alpha^{-iT} \cdot \alpha^{n+iT})$$
$$= \alpha^{-iT} \cdot tr_j^M(\alpha^{n+iT})$$

임의의 n에 대하여 식 (14)는 '0'이어야 한다. 이 경우, $\alpha^{-iT} \neq 0$ 이므로 식 (15)가 성립한다.

$$tr_j^M(\alpha^{n+iT}) = 0 \quad (15)$$

식 (15)는 심벌 '0'의 반복 주기는 T임을 나타내고 있다. $tr_j^M(\alpha^n) = 0$을 만족하는 $GF(2^M)$상의 원소의 갯수는 트레이스 함수 특성 3에 의하여 2^{M-J}있다. 한편, $\alpha = 0$인 경우는 제외되어야 하므로 $\alpha \neq 0$인 원소의 갯수는 $(2^{M-J}-1)$이다. 그러므로 $(2^M-1)/(2^J-1) = T$개의 연속적인 계열 요소에는 정확히 $(2^{M-J}-1)/(2^J-1)$개의 '0' 요소가 있다. (증명완료)

(정리 3) 실계열 $\overline{a}$의 계열 요소 a_n이 GMW 계열로부터 생성되고 식 (16)과 같이 정의될 경우, 계열 $\overline{a}$의 자기상관함수는 식 (17)과 같이 구해진다. 즉 GMW 계열의 자기 상관함수는 최대장 계열의 자기상관함수와 정확히 일치함을 알 수 있다.

$$a_n = (-1)^{tr\{[tr_j^M(a^n)]^r\}} \quad (16)$$

$$P(\tau) = \sum_{n=0}^{2^M-2} a_{n+\tau} \cdot a_n \quad (17)$$
$$= \begin{cases} 2^M-1, & for\ \tau = 0\ mod\ (2^M-1) \\ -1, & for\ \tau \neq 0\ mod\ (2^M-1) \end{cases}$$

(증명) 일반적으로 자기상관함수는 식 (18)과 같이 표현될 수 있다.

$$P(\tau) = \sum_{n=0}^{2^M-2} a_{n+\tau} \cdot a_n$$
$$= \sum_{n=0}^{2^M-2} (-1)^{tr\{[tr_j^M(a^{n+\tau})]^r + [tr_j^M(a^n)]^r\}} \quad (18)$$

정수 T를 식 (13)과 같이 정의하고, 지수 n을 식 (19)와 같이 정의하자.

$$n = j + iT \quad (19)$$

여기서, $0 \leq j < T$, $0 \leq i < 2^J-1$이다. 식 (18)의 지수 부의 내부식은 식 (20)과 같이 변경될 수 있다.

$$\{tr_j^M(\alpha^{n+\tau})\}^r + \{tr_j^M(\alpha^N)\}^r = \alpha^{iTr}\,\delta(\tau, j) \quad (20)$$

여기서, $\delta(\tau, j) = \{tr_j^M(\alpha^{j+\tau})\}^r + \{tr_j^M(\alpha^j)\}^r$이다. r은 2^J-1과 서로소 관계에 있으므로 α^{rT} 역시 $GF(2^J)$의 원시원이다. 그러므로 α^{rTi}는 i가 변하면서 $GF(2^J)$상의 '0'이 아닌 모든 원소를 취한다. 그러므로 자기상관함수는 식 (21)과 같이 변형될 수 있다.

$$P(\tau) = \sum_{j=0}^{T-1} \sum_{i=0}^{2^J-2} (-1)^{tr\{(\alpha^{rTi} \cdot \delta(\tau,j)\}}$$
$$= -\sum_{j=0}^{T-1} (-1)^{tr\{(0 \cdot \delta(\tau,j)\}} + \sum_{j=0}^{T-1} \sum_{\beta \in GF(2^J)} (-1)^{tr\{(\beta \cdot \delta(\tau,j)\}}$$
$$= -T + \sum_{j=0}^{T-1} \sum_{\beta \in GF(2^J)} (-1)^{tr\{(\beta \cdot \delta(\tau,j)\}}$$
$$= -T + \sum_{\beta \in GF(2^J)} \sum_{j=0}^{T-1} (-1)^{tr\{(\beta \cdot \delta(\tau,j)\}} \quad (21)$$

일반적으로 $GF(2^M)$상의 0이 아닌 모든 원소 δ에 대해 식 (22)의 특성이 만족된다.

$$\sum_{\beta \in GF(2^M)} (-1)^{tr\{(\delta, \alpha)} = 0 \quad (22)$$

따라서 $\delta(\tau, j) \neq 0$일때 식 (21)의 오른쪽 항의 내부 합은 0이 된다. 따라서 $\delta(\tau, j) = 0$인 경우에만 자기상관함수에 영향을 미친다. $N_0(\tau)$를 $0 \leq j < T$에 걸쳐 $\delta(\tau, j) = 0$이 되는 j의 갯수라 정의한다. $\delta(\tau, j) \neq 0$일때 식 (21)의 오른쪽 항이 '0'이 되고, $\delta(\tau, j) = 0$일때만 자기상관함수에 영향을 미치므로 식 (21)은 식 (23)과 같이 변형될 수 있다. 따라서 자기상관 함수는 $N_0(\tau)$가 결정되면 구할 수 있다.

$$P(\tau) = -T + 2^l \cdot N_0(\tau) \quad (23)$$

r은 2^l-1과 서로소 관계에 있으므로, 식 (24)의 관계식을 만족하는 r^{-1}이 반드시 존재한다.

$$r \cdot r^{-1} = 1 \ mod\ 2^l\text{-}1 \quad (24)$$

식 (20)으로 부터 $\delta(\tau, j) = 0$의 관계는 식 (25)의 관계식들과 등가임을 알 수 있다.

$$\begin{aligned} tr_l^M(\alpha^{\tau+j}) &= tr_l^M(\alpha^j) \\ tr_l^M(\alpha^{\tau+j} - \alpha^j) &= 0 \\ tr_l^M((\alpha^\tau - 1)\cdot\alpha^j) &= 0 \end{aligned} \quad (25)$$

α^τ-1 = 0일 경우, 식 (25)의 관계식은 T개의 모든 j에 대해 만족됨을 알 수 있다. 따라서 식 (26)의 관계식이 성립한다.

$$\begin{aligned} P(\tau) &= -T + 2^l \cdot T, \ for\ \tau = 0\ mod\ 2^M\text{-}1 \\ &= 2^M\text{-}1 \end{aligned} \quad (26)$$

α^τ-1 ≠ 0일 경우를 고려하자. 정리 1에 의해 계열 $b_n = tr_l^M(\alpha^n)$에서 T개의 연속적인 계열 요소에는 정확히 $(2^{M-l}\text{-}1)(2^l\text{-}1)$개의 '0' 요소가 존재한다. 따라서 α^τ-1 ≠ 0일 경우 $N_0(\tau) = (2^{M-l}\text{-}1)/(2^l\text{-}1)$이다. 그러므로 식 (23)은 식 (27)과 같이 된다.

$$\begin{aligned} P(\tau) &= -T + 2^l \cdot \frac{(2^{M-l}\text{-}1)}{(2^l\text{-}1)}, \ for\ \tau \neq 0\ mod\ 2^M\text{-}1 \\ &= 1 \end{aligned} \quad (27)$$

따라서 식 (26)과 식 (27)로 부터 식 (17)의 관계식이 만족됨을 알 수 있다.

(증명완료)

제2절 GMW 계열의 생성기 설계 예

6차의 최소 다항식을 이용한 GMW 계열의 $GF(2^l)$상의 생성다항식과 GMW 계열 생성기의 구조를 제시한다. 6차의 최소 다항식 (Minimal Polynomial)은 식 (28)과 같다고 가정한다.

$$p(x) = x^6 + x^5 + x^2 + x + 1 \quad (28)$$

표 1 $GF(2^3)$

원 소	다항식 표현
0	0
1	1
$\alpha^9 = \gamma$	$1 + \alpha^2 + \alpha^3$
$\alpha^{18} = \gamma^2$	$\alpha + \alpha^2 + \alpha^4 + \alpha^5$
$\alpha^{27} = \gamma^3$	$\alpha^2 + \alpha^3$
$\alpha^{36} = \gamma^4$	$1 + \alpha + \alpha^3 + \alpha^4 + \alpha^5$
$\alpha^{45} = \gamma^5$	$\alpha + \alpha^3 + \alpha^4 + \alpha^5$
$\alpha^{54} = \gamma^6$	$1 + \alpha + \alpha^2 + \alpha^4 + \alpha^5$

식 (28)을 이용하여 $GF(2^6)$을 생성한 후, 차수가 7인 $GF(2^3)$의 원소를 구하면 표 1과 같다.

GMW 계열의 계열요소 $b_n = tr_1^l\{\{tr_l^M(\alpha^n)\}^r\}$은 먼저 $GF(2^l)$상의 원소 $tr_l^M(\alpha^n)$을 구하고, 이 $GF(2^l)$상의 계열요소를 r승한 후, 이를 $tr_1^l(.)$한 결과이다. 일반적으로 $GF(q^M)$에서 원소 β에 대한 최소다항식은 식 (29)와 같다.

$$m(x) = (x\text{-}\beta)(x\text{-}\beta^q)\ldots(x\text{-}\beta^{q^{e-1}}) \quad (29)$$

여기서 e는 $\beta^{q^e} = \beta$를 만족하는 정수이다. 따라서 $q = 8$인 $GF(q^2)$ 즉, $GF(2^6)$상의 원시원 α에 대한 최소다항식은 식 (30)과 같다.

$$\begin{aligned} m(x) &= (x\text{-}\alpha)(x\text{-}\alpha^8) \\ &= x^2 + (1+\alpha+\alpha^2+\alpha^4+\alpha^5)x + \alpha^9 \\ &= x^2 + \alpha^{54}x + \alpha^9 \end{aligned} \quad (30)$$

길이가 63이고 r이 3인 GMW 계열은 식 (31)과 같이 정의된다.

$$b_n = tr_1^3\{\{tr_3^6(\alpha^n)\}^3\} \quad (31)$$

식 (30)과 같은 최소다항식을 이용한 식 (31)과 같이 정의되는 GMW 계열의 생성기는 그림 1과 같다.

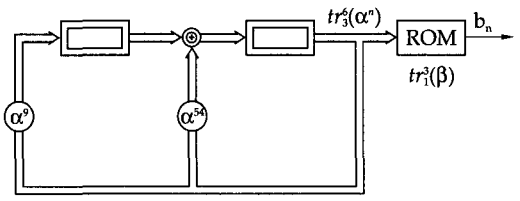


그림 1 길이가 63이고 r이 3인 GMW 계열

$GF(8)$상의 기저 1, α^9, α^{18}로 $GF(8)$상의 원소 γ를 표현하면 식 (32)와 같다.

$$\gamma = \gamma_0 \cdot 1 + \gamma_1 \cdot \alpha^9 + \gamma_2 \cdot \alpha^{18} \qquad (32)$$

여기서, $\gamma_0 \in GF(2)$이다. 원소 γ에 α^{54}, α^9을 각각 곱한 결과는 식 (33)과 같다.

$$\begin{aligned} \alpha^{54} \cdot \gamma &= \alpha^{54}\{\gamma_0 + \gamma_1\alpha^9 + \gamma_2\alpha^{18}\} \\ &= (\gamma_0 + \gamma_1) \cdot 1 + \gamma_2\alpha^9 + \gamma_0\alpha^{18} \end{aligned}$$

$$\begin{aligned} \alpha^9\gamma &= \alpha^9\gamma_0 + \alpha^{18}\gamma_1 + \alpha^{27}\gamma_2 \qquad (33) \\ &= \gamma_2 \cdot 1 + (\gamma_0 + \gamma_2) \cdot \alpha^9 + \gamma_1\alpha^{18} \end{aligned}$$

$GF(2^3)$상의 원소 $\gamma = 0$인 경우, 이를 3승 한 $\gamma^3 = 0$이 되며, 이 원소의 트레이스 값은 $tr_1^3(0) = 0$이 됨을 알 수 있다. 같은 방법으로 $GF(2^3)$상의 원소 $\gamma = 1$인 경우, 이를 3승한 $\gamma^3 = 1$이 되며, 이 원소의 트레이스 값은 $tr_1^3(1) = 1$이 된다. $GF(2^3)$상의 원소 $\gamma = \alpha^9$인 경우, 이를 3승한 $\gamma^3 = \alpha^{27}$이 되며, 이 원소의 트레이스 값은 $tr_1^3(\alpha^{27}) = 1$이 된다. $GF(2^3)$상의 원소 $\gamma = \alpha^{18}$인 경우, 이를 3승한 $\gamma^3 = \alpha^{54}$이 되며, 이 원소의 트레이스 값은 $tr_1^3(\alpha^{54}) = 1$이 된다. $GF(2^3)$상의 원소 $\gamma = \alpha^{27}$인 경우, 이를 3승한 $\gamma^3 = \alpha^{18}$이 되며, 이 원소의 트레이스 값은 $tr_1^3(\alpha^{18}) = 0$이 된다. $GF(2^3)$상의 원소 $\gamma = \alpha^{36}$인 경우, 이를 3승한 $\gamma^3 = \alpha^{45}$가 되며, 이 원소의 트레이스 값은 $tr_1^3(\alpha^{45}) = 1$이 된다. $GF(2^3)$상의 원소 $\gamma = \alpha^{45}$인 경우, 이를 3승한 $\gamma^3 = \alpha^9$이 되며, 이 원소의 트레이스 값은 $tr_1^3(\alpha^9) = 0$이 된다. GF(2^3)상의 원소 $\gamma = \alpha^{54}$인 경우, 이를 3승한 $\gamma^3 = \alpha^{36}$이 되며, 이 원소의 트레이스 값은 $tr_1^3(\alpha^{36}) = 0$이 된다. 이를 종합하면 표 2와 같다. 표 2를 이용하면 그림 1의 ROM 부분을 논리 조합 회로(Combinational Logic Circuit)로 실현할 수 있다.

표 2 $tr_1^3(\gamma^3)$의 값

γ	기저 표현 γ_0	γ_1	γ_2	γ^3	$tr_1^3(\gamma^3)$
0	0	0	0	0	0
1	1	0	0	1	1
$\gamma = \alpha^9$	0	1	0	α^{27}	1
$\gamma = \alpha^{18}$	0	0	1	α^{54}	1
$\gamma = \alpha^{27}$	1	1	0	α^{18}	0
$\gamma = \alpha^{36}$	0	1	1	α^{45}	1
$\gamma = \alpha^{45}$	1	1	1	α^9	0
$\gamma = \alpha^{54}$	1	0	1	α^{36}	0

제3절 GMW 계열의 선형복잡도

계열 $\bar{b}$의 선형복잡도는 해당 계열 $\bar{b}$을 생성할 수 있는 선형귀환 방정식의 최소 차수를 의미한다. 계열 $\bar{b}_n$의 선형복잡도는 계열 요소를 식 (34)와 같이 표현하고, 식 (35)와 같이 식 (34)에서 계수가 '0'이 아닌 계수의 갯수다.[6]

$$b_n = \sum_{j=0}^{2^M-2} C_j \alpha^{jn}, \text{ for all } n \tag{34}$$

여기서, α는 $GF(2^M)$상의 원시원이다.

$$b = \#\{C_j \ ; \ C_j \neq 0, \ 0 \leq j < 2^M - 1\} \tag{35}$$

(정리 4) GMW 계열의 계열 요소가 식 (36)과 같을 경우,

$$b_n = tr_1^l\{[\, tr_f^M(\alpha^n)\,]^r\} \tag{36}$$

여기서, α는 $GF(2^M)$의 원시원이고, r $(0 < r < 2^l-1)$은 2^l-1과 서로소 관계이다. 그러면 GMW 계열의 선형복잡도는 식 (37)과 같다.

$$L = J \cdot (M/l)^w \tag{37}$$

여기서, w는 r을 이진 표현했을 경우 "1"의 갯수이다.

(증 명) $GCD(2^l-1, r) = 1$, $0 < r < 2^l-1$인 지수부 r은 식 (38)과 같이 표현될 수 있다.

$$r = \sum_{i=1}^{w} 2^{j_i} \tag{38}$$

여기서, j_i는 $0 \leq j_i < J$에서 서로 다른 정수들이다. 식 (36)은 식 (38)을 이용하면 식 (39)와 같이 변경될 수 있다.

$$\begin{aligned} b_n &= tr_1^l\{\{tr_f^M(\alpha^n)\}^r\} \\ &= tr_1^l\{tr_f^M(\alpha^n)\}^{2^{j_1}+2^{j_2}+\cdots+2^{j_w}}\} \\ &= tr_1^l\{\prod_{i=1}^{w}\{\sum_{k=0}^{M/l-1}(\alpha^n)^{2^{l\cdot k}}\}^{2^{j_i}}\} \\ &= tr_1^l\{\prod_{i=1}^{w}\sum_{k=0}^{K-1}(\alpha^n)^{2^{l\cdot k+j_i}}\} \end{aligned} \tag{39}$$

$\bar{k} = (k_1, k_2, \cdots k_w)$라 정의한다. 여기서, $k_i \in \{0, \cdots, K-1\}$, $i \in \{1, \cdots, w\}$이다. 그러면 식 (39)는 식 (40)과 같이 변경될 수 있다.

$$\begin{aligned} b_n &= tr_1^l\{\prod_{i=1}^{w}\sum_{k=0}^{M/l-1}\alpha^{n\cdot 2^{l\cdot k+j_i}}\} \\ &= tr_1^l\Big(\sum_{k_1=0}^{K-1}\cdots\sum_{k_w=0}^{K-1}\alpha^{n\cdot(2^{j_1+k_1 l}+\cdots+2^{j_w+k_w l})}\Big) \end{aligned} \tag{40}$$

한편, $C(\bar{k}, r)$를 식 (41)과 같이 정의하자.

$$\begin{aligned} C(\bar{k}, r) &= C((k_1, \cdots, k_w), r) \\ &= \sum_{i=1}^{w} 2^{l\cdot k_i+j_i}, \ 0 \leq j_i < J \end{aligned} \tag{41}$$

여기서, $0 \leq k_i \leq (K-1 = M/l-1)$, $0 \leq j_i < J$이다. 식 (40)은 식 (41)을 이용하여 식 (42)와 같이 변경될 수 있다.

$$b_n = tr_1^l\Big(\sum_{k_1=0}^{K-1}\cdots\sum_{k_w=0}^{K-1}\alpha^{n\cdot C(\bar{k},r)}\Big) \tag{42}$$

여기서, $K = M/l$이고, $C(\bar{k}, r) = \sum_{i=1}^{w} 2^{lk_i+j_i}$이다. $C(\bar{k},r)$는 모든 $k_i = (M/l)-1$ 일때 최대값이 되므로 식 (43)과 같은 관계식을 만족한다. 따라서 모듈러 2^M-1은 무시될 수 있다.

$$\begin{aligned} C(\bar{k},r) &= \sum_{i=1}^{w} 2^{lk_i+j_i} \\ &= 2^{j_1+(M\cdot l)}+\cdots+2^{j_w+(M\cdot l)} \\ &= 2^{M\cdot l}\cdot r \\ &\leq 2^{M\cdot l}\cdot(2^l-1) \\ &= 2^M-2^{M\cdot l} \\ &< 2^M-1 \end{aligned} \tag{43}$$

식 (42)는 식 (44)와 같이 변경될 수 있다.

$$b_n = tr_1^l\{\sum_{k_1=0}^{K-1}\cdots\sum_{k_w=0}^{K-1}\alpha^{nC(\bar{k},r)}\} \quad (44)$$
$$= \sum_{m=0}^{J-1}\sum_{k_1=0}^{K-1}\cdots\sum_{k_w=0}^{K-1}\alpha^{nC(\bar{k},r)\cdot 2^m}$$

$C(\bar{k}, \gamma)\cdot 2^m$은 α의 차수인 2^M-1로 모듈러를 취할 때 서로 다름을 보이자. 즉, 서로 다른 $\bar{k}$에 대해 서로 다른 값을 가짐을 보이자. 만약 서로 다른 $(\bar{k}^{(1)}, m_1)$, $(\bar{k}^{(2)}, m_2)$에 대해 구한 각각의 $C(\bar{k}, r)\cdot 2^m$이 서로 같다고 가정하면, 식 (45)의 관계식이 만족된다.

$$C(\bar{k}^{(1)},r)\cdot 2^{m_1} = C(\bar{k}^{(2)},r)\cdot 2^{m_2} \ mod\ 2^M\text{-}1 \quad (45)$$

2^l-1이 2^M-1을 나누므로 식 (46)이 만족된다.

$$C(\bar{k}^{(1)},r)\cdot 2^{m_1} = C(\bar{k}^{(2)},r)\cdot 2^{m_2} \ mod\ 2^l\text{-}1 \quad (46)$$

일반적으로 식 (47)의 관계식이 만족된다.

$$2^{lk_1+j_1} \ mod\ 2^l\text{-}1 = 2^{j_1} \quad (47)$$

식 (47)을 이용하면 $C(\bar{k}, r)$은 식 (48)과 같다.

$$C(\bar{k}, r) \ mod\ 2^l\text{-}1 = r \quad (48)$$

따라서 식 (46)은 식 (49)와 등가이다.

$$r\cdot 2^{m_1} = r\cdot 2^{m_2},\ mod\ 2^l\text{-}1 \quad (49)$$
$$r(2^{m_1}\text{-}2^{m_2}) = 0,\ mod\ 2^l\text{-}1$$

$GCD(r,\ 2^l\text{-}1)=1$이므로 식 (49)는 식 (50)과 등가이다.

$$2^{m_1} = 2^{m_2} \quad (50)$$
$$m_1 = m_2$$

$m_1 = m_2$일때만 식 (45)가 만족된다. 그러나 두개의 m이 서로 다르다는 가정을 모순한다. 그러므로 식 (45)는 만족되지 않는다. 따라서 식 (44)의 지수부는 모두 다르다.

$$b_n = \sum_{m=0}^{J-1}\sum_{k_1=0}^{K-1}\cdots\sum_{k_w=0}^{K-1}\alpha^{n\cdot C(\bar{k},r)\cdot 2^m} \quad (44)$$

따라서 식 (44)에서 알 수 있듯이 계열 요소에서 '0'이 아닌 계수의 갯수는 식 (51)과 같다.

$$J\cdot(K)^w = J\cdot(M/J)^w \quad (51)$$

그러므로 GMW 계열의 선형복잡도는 식 (52)와 같다.

$$L = J\cdot(M/J)^w \quad (52)$$

(증명완료)

GMW 계열의 계열 요소는 식 (53)과 같이 쓸 수 있다.

$$b_n = \sum_{j=0}^{2^M-2} C_j\alpha^{jn} \quad (53)$$
$$= C_0 + C_1\alpha^n + C_2(\alpha^n)^2 + \cdots + C_{2^M-2}\cdot(\alpha^n)^{2^M-2}$$

식 (53)은 식 (54)와 같이 변경될 수 있다.

$$b_n = \sum_{\beta\in S} tr_1^{\delta}(C_j(\alpha^j)^n) \quad (54)$$
$$= \sum_{\beta\in S} tr_1^{\delta}(C_j\beta^n)$$

여기서, $\beta = \alpha^j$이고, S는 각 Conjugate Class에서 한 원소만을 추출한 원소들로 구성된 집합이며, $GF(2^{\delta_\beta})$는 β를 포함하는 최소의 서브 유한체이다. GMW 계열 $\bar{b}$의 특성방정식 $c(x)$는 식 (55)와 같다.

$$c(x) = \prod_{\beta\in S} m_\beta(x) \quad (55)$$

따라서 GMW 계열의 선형복잡도는 식 (56)과 같이 표현된다.

$$L = \sum_{\beta \in S} \deg[m_\beta(x)] \tag{56}$$

제2절에서 제시된 예제에 대한 선형복잡도와 특성 다항식을 구해보자. $r = 3$이므로 $w = 2$가 되므로 선형복잡도는 식 (57)과 같이 12가 됨을 알 수 있다.

$$\begin{aligned} &M = 6,\ J = 3,\ w = 2 \\ &L = J \cdot (M/J)^2 = 3 \cdot (6/3)^2 = 3 \times 4 = 12 \end{aligned} \tag{57}$$

식 (57)과 같은 변수들을 갖는 GMW 계열의 계열요소는 식 (58)과 같이 표현된다.

$$\begin{aligned} b_n &= tr_1^3\{[\,tr_3^6(\alpha^n)\,]^3\} \\ &= tr_1^3\{(\alpha^n + (\alpha^n)^{2^3})^3\} \\ &= tr_1^3\{(\alpha^n)^3 + (\alpha^n)^{2^3 \cdot 3} + (\alpha^n)^2(\alpha^n)^{2^3} \\ &\quad + \alpha^n(\alpha^n)^{2^3})^2\} \\ &= tr_1^6((\alpha^3)^n) + tr_1^6((\alpha^5)^n) \\ &= \sum_{\beta \in S} tr_1^6(c_\beta \beta^n) \end{aligned} \tag{58}$$

여기서, $S = \{\alpha^3, \alpha^5\}$, $C_{\alpha^3} = 1$, $C_{\alpha^5} = 1$이다. 따라서 α^3, α^5에 대한 최소다항식들은 식 (59)와 같다.

$$\begin{aligned} m_{\alpha^3}(x) &= (x+\alpha^3)(x+(\alpha^3)^2)(x+(\alpha^3)^{2^2}) \\ &\quad (x+(\alpha^3)^{2^3})(x+(\alpha^3)^{2^4})(x+(\alpha^3)^{2^5}) \\ &= (x+\alpha^3)(x+\alpha^6)(x+\alpha^{12})(x+\alpha^{24}) \\ &\quad (x+\alpha^{48})(x+\alpha^{33}) \\ &= x^6 + x^5 + x^2 + 1 \end{aligned}$$

$$\begin{aligned} m_{\alpha^5}(x) &= (x+\alpha^5)(x+(\alpha^5)^2)((x+(\alpha^5)^{2^2}) \\ &\quad (x+(\alpha^5)^{2^3})(x+(\alpha^5)^{2^4})(x+(\alpha^5)^{2^5}) \\ &= (x+\alpha^5)(x+\alpha^{10})(x+\alpha^{20})(x+\alpha^{40}) \\ &\quad (x+\alpha^{17})(x+\alpha^{34}) \\ &= x^6 + x^5 + x^3 + x^2 + 1 \end{aligned} \tag{59}$$

따라서 특성방정식은 식 (60)과 같다.

$$\begin{aligned} c(x) &= \prod_{\beta \in S} m_\beta(x) \\ &= m_{\alpha^3}(x) \cdot m_{\alpha^5}(x) \\ &= (x^6 + x^5 + x^2 + 1)(x^6 + x^5 + x^3 + x^2 + 1) \\ &= x^{12} + x^{10} + x^9 + x^8 + x^7 + x^5 + x^4 + x^3 + 1 \end{aligned} \tag{60}$$

따라서 특성 다항식의 차수와 선형복잡도는 동일함을 입증했다. 정리 4는 GMW 계열의 갯수를 계산하는데 이용되는 정리이다.

제4절 GMW 계열의 갯수

본 절에서는 GMW 계열의 갯수를 구하는 수식을 유도한다.

(정리 5) 2개의 GMW 계열들 $\bar{b}$와 $\bar{c}$의 계열 요소 b_n와 c_n이 식 (61)과 같이 정의되었을 경우, 두 계열이 순회등가(Cyclically Equivalent)일 필요충분 조건은 식 (62)이다.

$$\begin{aligned} b_n &= tr_1^J\{\{tr_J^M(\alpha^n)\}^r\} \\ c_n &= tr_1^J\{\{tr_J^M(\alpha^{dn})\}^s\} \end{aligned} \tag{61}$$

$$\begin{aligned} &r = 2^k \cdot s,\ mod\ 2^J\text{-}1 \text{ for } some\ 0 \le k < J \\ &d = 2^m, \text{ for } some\ 0 \le m < M \end{aligned} \tag{62}$$

(증 명) 정수 T, n을 (63)과 같이 정의하자.

$$\begin{aligned} T &= \frac{2^M\text{-}1}{2^J\text{-}1} \\ n &= j + iT \end{aligned} \tag{63}$$

여기서, $0 \le j < T$, $0 \le i < 2^J\text{-}1$이다. $\beta = \alpha^l$, $\gamma = \alpha^T$이라고 가정하자. 그러면 b_n, $c_{n+\tau}$은 각각 식 (64)와 (65)와 같이 쓸 수 있다.

$$c_{n+\tau} = tr_1^l\{\{tr_J^M(\alpha^{d(n+\tau)})\}^s\} \quad (64)$$
$$= tr_1^l\{\{tr_J^M(\alpha^{d(j+n+\tau)})\}^s\}$$
$$= tr_1^l\{\{\gamma^{ds\,i}\cdot g\}$$

$$b_n = tr_1^l\{\{tr_J^M(\alpha^n)\}^r\} \quad (65)$$
$$= tr_1^l\{\{\gamma^{r\,i}\cdot f\}$$

여기서, $g = \{tr_J^M(\beta\alpha^{dj})\}^s$, $f = \{tr_J^M(\alpha^j)\}^r$이다. 따라서 관계식 $b_n = c_{n+\tau}$는 식 (66)과 등가임을 알 수 있다.

$$tr_1^l(\gamma^{r\,i}\cdot f) = tr_1^l(\gamma^{ds\,i}\cdot g) \quad (66)$$

따라서 임의의 β에 대하여 계열 $tr_1^l(\gamma^{r\,i}\cdot f)$와 $tr_1^l(\gamma^{ds\,i}\cdot g)$가 같을 필요충분 조건은 γ^r과 γ^{ds}가 동일한 최소다항식을 가지는 것이다. 즉 식 (67)의 관계식을 갖는다.

$$r = 2^k\cdot ds, \text{ mod } 2^l\text{-}1 \text{ for } some\ 0 \le k < J \quad (67)$$

식 (67)이 만족한다면, 식 (68)의 관계식을 만족한다.

$$tr_1^l\{\gamma^{r\,i}\cdot f\} = tr_1^l(\gamma^{2^k ds\,i}\cdot f) \quad (68)$$
$$= tr_1^I\{\{\gamma^{ds\,i}\cdot f^{2^k}\}^{2^k}\}$$
$$= tr_1^I\{\gamma^{ds\,i}\cdot f^{2^l\text{-}k}\}$$

$g = f^{2^l\text{-}k}$일 때 두 계열은 동일하다. 따라서 또 다른 조건은 $g = f^{2^l\text{-}k}$이다. g와 $f^{2^l\text{-}k}$는 식 (69)와 같이 표현될 수 있다.

$$f^{2^l\text{-}k} = \{\{tr_J^M(\alpha^j)\}\}^{2^l\text{-}k\,r} \quad (69)$$
$$g = \{\{tr_J^M(\beta\alpha^j)\}\}^s$$

$g = f^{2^l\text{-}k}$의 관계식이 만족하기 위해서는 식 (70)의 관계식이 만족해야 한다.

$$\{tr_J^M(\alpha^j)\}^{2^l\text{-}k\cdot r} = \{tr_J^M(\beta\alpha^{dj})\}^s \quad (70)$$

$s\cdot s^{-1} = 1 \text{ mod } 2^l\text{-}1$를 만족하는 s의 역원 s^{-1}을 구한 후, 식 (70)의 양변에 곱하면 식 (71)을 구할 수 있다.

$$\{tr_J^M(\alpha^j)\}^{2^l\text{-}k\cdot r\cdot s^{-1}} = \{tr_J^M(\beta\alpha^{dj})\}^{s\cdot s^{-1}} \quad (71)$$
$$= tr_J^M(\beta\alpha^{dj})$$

식 (71)은 식 (72)와 같이 변형될 수 있다.

$$\{tr_J^M(\alpha^j)\}^d = tr_J^M(\beta\alpha^{dj}) \quad (72)$$

따라서 식 (72)는 $g = f^{2^l\text{-}k}$와 등가이다. $GF(2^l)$상의 두개의 계열인 $\{tr_J^M(\alpha^j)\}^d$와 $tr_J^M(\beta\alpha^{dj})$가 순회적으로 등가라면 이 계열의 선형복잡도는 같아야 한다. 그런데 $tr_J^M(\beta\alpha^{dj})$의 선형복잡도는 M/J이고, $\{tr_J^M(\alpha^j)\}^d$의 선형복잡도는 $(M/J)^w$이므로, $\{tr_J^M(\alpha^j)\}^d = tr_J^M(\beta\alpha^{dj})$을 만족하기 위해서는 $w=1$이어야 한다. 여기서 w는 d를 이진 표현했을 경우 '1'의 갯수이다. $w=1$인 경우, 일반화한 d는 식 (73)과 같이 중(Weight)이 1인 경우이다.

$$d = 2^m, \text{ for } some\ 0 \le m < M \quad (73)$$

따라서 증명이 완료된다. (증명완료)

일반적인 GMW 계열은 식 (74)와 같이 표현될 수 있다.

$$b_n = tr_1^l\{\{tr_J^M(\alpha^{dn})\}^s\} \quad (74)$$

$GF(2^M)$에서 원시다항식의 갯수는 식 (75)와 같다.

$$N_p(M) = \frac{\Phi(2^M\text{-}1)}{M} \quad (75)$$

그리고 $r = 2^k\cdot s \ mod\ 2^l\text{-}1$이 아닌 $GF(2^l)$상의 r의 갯수 $N_p(J)$는 식 (76)과 같다.

$$N_p(J) = \frac{\Phi(2^l\text{-}1)}{J} \quad (76)$$

만약 $N_p(D)$를 $GF(2)$상의 D차인 원시다항식의 갯수이고, $N_p(J)$를 하나의 원시다항식이 결정되었을 경우 서로 다른 계열을 생성하는 r의 갯수라고 하며, N_{GMW}를 서로 다른 GMW 계열의 갯수라고 가정하자. 그러면 GMW 계열의 갯수는 식 (77)과 같다.

$$N_{GMW} = N_P(M) \cdot N_P(J) \qquad (77)$$

예를 들어 $J=7$, $2^J-1 = 2^7-1 = 127$인 경우, r 값에 대한 w값은 표 3과 같다.

표 3 r에 대한 w

w	r값
1	1
2	3, 5, 9
3	7, 11, 13, 19, 21
4	15, 23, 27, 29, 43
5	31, 47, 55
6	63

전체 GMW 계열의 갯수는 식 (77)에 의해 2,268임을 알 수 있다. $J=7$인 경우의 설계변수는 표 4와 같다.

제3장 결 론

본 논문에서는 선형복잡도 특성이 우수한 GMW 계열의 특성을 분석하였다. 이를 위하여 먼저 트레이스 함수를 정의하고, 트레이스 함수의 다섯가지 특성을 도출하였다. 그리고 GMW 계열의 자기상관함수가 $\tau = 0 \bmod (2^M-1)$일 때 '2^M-1'이고, $\tau \neq 0 \bmod (2^M-1)$일 때 '-1'이 됨을 확인함으로서, 이상적인 자기상관특성을 가짐을 확인하였다. 그리고 GMW 계열의 생성기는 부계열을 생성하기 위한 부계열 생성 회로와 부계열에서 이진 계열로 사상하는 ROM 회로 또는 논리회로 부로 구성될 수 있음을 확인하였다. 또한 GMW 계열의 선형복잡도는 w가 r을 이진 표현했을 경우 '1'의 갯수인 경우, $L = J \cdot (M/J)^w$임을 알 수 있었다. 그리고 $N_p(J)$를 차수가 p차인 $GF(2^p)$의 Cyclotmic Coset의 갯수라고 하고, N_{GMW}를 서로 다른 GMW 계열의 갯수라고 가정하면, GMW 계열의 갯수는 $N_{GMW} = N_P(M) \cdot N_P(J)$임을 확인하였다. 본 고에서는 참고문헌 [9]에서 제시된 GMW 계열의 특성을 자세히 분석함으로서 추후의 2레벨 GMW 계열[8]의 특성을 분석하기 위한 바탕 이론을 제시하였다. 또한 GMW 계열은 참고문헌 [11]에서와 같이 선형

표 4 $J=7$인 경우의 설계 변수

w	$\binom{J}{w}/J$	$M=14$		$M=28$	
		L	$N_{GMW}(W)$	L	$N_{GMW}(W)$
1	1	14	756	28	4,741,632
2	3	28	2,268	112	14,224,896
3	5	56	3,780	448	23,708,160
4	5	112	3,780	1,792	23,708,160
5	3	224	2,268	7,168	14,224,896
6	1	448	756	28,672	4,731,632

복잡도가 우수한 비선형 난수 계열을 생성하기 위한 바탕 계열로 이용될 수 있을 것이다.

참 고 문 헌

[1] S.W. Golomb, Shift Register Sequences, Hoden-day, 1982.

[2] R.A.Rueppel, Analysis and Design of Stream Ciphers, Springer-Verlag, 1986.

[3] J.L. Massey, Coding and Cryptography, Advanced Technology Seminars, 1985.

[4] M.Y.Rhee, Cryptography and Secure Communications, McGraw-Hill, New-York, 1993.

[5] J.L. Massey, "Shift-Register Synthesis and BCH Decoding", IEEE Tr. on Inform. Theory, Vol.IT-15, No.1, Jan. 1969, pp.122-127

[6] E.L. Key "An Analysis of the Structure and Complexity of Non-linear Binary Sequence Generator", IEEE Transactions on Information Theory, Vol.IT-22, No.6, pp.732-736, 1976.

[7] T.Siegenthaler, "Design of Combiners to Prevent Divide and Conquer Attacks", Proceedings of Crypto'85, Santa Barbara, August 18-22, 1985.

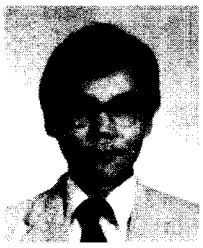
[8] M.Antweiler, L.Bomer, "Complex Sequences over GF(P^M) with a Two-level Autocorrelation Function and Large Linear Span", IEEE Tr. on Inform. Theory, Vol.IT-38, No.1, pp.120-130, Jan. 1992.

[9] R.A. Scholtz, L.R.Welch, "GMW Sequences", IEEE Tr. on Inform. Theory, Vol.IT-30, No.3, pp.548-553, May 1984.

[10] R.A.Rueppel, O.J.Staffelbach, "Products of Linear Recurring Sequences with Maximum Complexity", IEEE Tr. on Inform. Theory, Vol.IT-33, No.2, pp.122-131, Jan. 1987.

[11] Heung Youl Youm and Man Young Rhee, "Correlation-immune Random Sequence Generator Using GMW Sequences", Proceeding of Joint Workshop on Information Security and Cryptography' 95, Japan, 1995.

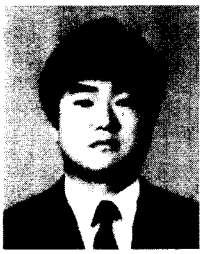
□ 著者紹介



염 홍 열(종신회원)

1981년 漢陽大學校 電子工學科 卒業(學士)
1983년 漢陽大學校 大學院 電子工學科 卒業(工學碩士)
1990년 漢陽大學校 大學院 電子工學科 卒業(工學博士)
1982년 12월 ~ 1990년 9월 韓國電子通信研究所 先任研究員
1990년 3월 ~ 현재 順天鄕大學校 工科大學 電子工學科 助教授

※ 관심분야 : 암호이론, 부호이론, 이동통신 분야



김 춘 수

1987년 2월 숭실대학교 공과대학 전기공학과 졸업(공학사)
1989년 2월 숭실대학교 대학원 전기공학과 졸업(공학석사)
1990년 2월 ~ 현재 한국전자통신연구소 부호4실 선임연구원

이 홍 섭(종신회원)

통신정보보호학회지 제3권 제4호 참조