낮은 상관 특성과 큰 선형 복잡도를 갖는 새로운 p-진 수열군

*김영식, **정정수, **노종선, ***신동준
*삼성전자, **서울대학교 전기컴퓨터공학부, INMC,
***한양대학교 전자전기공학부

New Families of p-ary Sequences With Low Correlation and Large Linear Span

*Young-Sik Kim, **Jung-Soo Chung, **Jong-Seon No, and ***Dong-Joon Shin
*Samsung Electronics, Co., Ltd.
**Department of EECS, INMC, Seoul National University
***Division of Electronics and Computer Engineering, Hanyang University
{kingsi, integer}@ccl.snu.ac.kr, jsno@snu.ac.kr, djshin@hanyang.ac.kr

요약

최근에 홀수인 소수 p, $n = 4k$, 그리고 $d = ((p^{2k}+1)/2)^2$에 대해서 Seo, Kim, No, Shin [1]이 m-sequence와 d로 decimation한 부분 수열들 사이의 상관 분포를 유도하였다. 하지만 이러한 상관 분포로부터 수열군이 자명하게 결정되지는 않는다. 이 논문에서는 우선 위의 상관 특성을 유지하는 수열군을 선택하는 방법을 제시한다. 더 나아가서 이 수열군과 동일한 상관 특성을 가지면서도 더 큰 선형 복잡도를 갖는 수열군을 새롭게 생성할 것이다. 끝으로 3진 수열의 선형 복잡도를 특정 경우에 대해서 유도하고 이 경우 원래의 수열군보다 더 큰 선형 복잡도를 가짐을 보일 것이다.

1. 서론

오늘날 의사 불규칙 수열은 여러 가지 디지털 통신 시스템에서 많이 사용되고 있다. 이러한 수열들을 설계하는데 있어서 가장 중요한 요소는 수열들의 상관 특성이지만 이에 못지 않게 선형 복잡도를 높게 만드는 것도 매우 중요하다. 왜냐하면 선형 복잡도는 바로 수열을 분석하는 것이 얼마나 어려운지에 대한 정보를 제공해 주기 때문이다. 다시 말해 선형 복잡도가 크다는 것은 수열을 분석하고 다음 값을 예측하기 위해서 그만큼 더 많은 정보가 필요하다는 의미이다.

최근에 홀수인 소수 p, $n = 4k$, 그리고 $d = ((p^{2k}+1)/2)^2$에 대해서 Seo, Kim, No, Shin [1]이 m-sequence와 d로 decimation한 부분 수열들 사이의 상관 분포를 유도하였다. 하지만 이러한 상관 분포로 부터 수열군이 자명하게 결정되지는 않는다. 이 논문에서는 우선 위의 상관 특성을 유지하는 수열군을 선택하는 방법을 제시한다. 더 나아가서 이 수열군과 동일한 상관 특성을 가지면서도 더 큰 선형 복잡도를 갖는 수열군을 새롭게 생성할 것이다. 끝으로 3진 수열의 선형 복잡도를 특정 경우에 대해서 유도하고 이 경우 원래의 수열군보다 더 큰 선형 복잡도를 가짐을 보일 것이다.

2. 사전지식

p 가 홀수인 소수이고 F_{p^n} 가 p^n개의 원소를 갖는 유한체라 하자. 그러면 유한체 F_{p^n}에서 유한체 F_{p^m}로의 trace 함수 $\mathrm{tr}_m^n(\cdot)$는 $\mathrm{tr}_m^n(x) = \sum_{i=0}^{n/m-1} x^{p^{mi}}$로 정의된다. 여기서 $x \in F_{p^n}$이고 m은 n의 약수이다. α가 F_{p^n}의 원시원이라 하자. 그러면 주기가 $p^n - 1$인 p-진 m-sequence $s(t)$은 다음과 같이 trace 함수로 나타낼 수가 있다.

$$s(t) = \mathrm{tr}_1^n(\alpha^t).$$

이 논문에서는 다음의 정의들을 사용할 것이다.

- $D = (p^{2k}+1)/2$ 이고 $d = D^2 = ((p^{2k}+1)/2)^2$;
- r은 $1 \le r < p^{2k}-1$, $\gcd(r, p^{2k}-1) = 1$인 정수;
- κ는 F_{p^n}의 한 원시원;
- $\beta = \kappa^{(p^{2k}+1)/2}$ 이고 $\gamma = \kappa^{2(p^{2k}-1)}$.

다음 장에서 다음의 성질들을 이용할 것이다.

- $\beta\gamma$는 F_{p^n}의 원시원;
- $\beta^{p^{2k}} = -\beta$ 이고 $\beta^d = -\beta$;
- $\gamma^{p^{2k}} = \gamma^{-1}$ 이고 $\gamma^d = 1$.

$\gcd(p^n-1, d) = (p^{2k}+1)/2$이므로 주기가 $2(p^{2k}-1)$인 $(p^{2k}+1)/2$개의 서로 다른 decimation 된 수열 $s(dt+l)$ $(0 \le l < (p^{2k}+1)/2)$가 존재한다. 그러면 $s(t)$와 $s(dt+l)$ 사이의 상호 상관 함수는 다음과 같이 정의된다.

$$C_l(\tau) = \sum_{x \in F_{p^n}^*} \omega^{\mathrm{tr}_1^n(ax - bx^d)}. \quad (1)$$

여기서 ω는 1의 p-차 원시 복소 근이고, $a = \alpha^\tau$ 이고 $b = \alpha^l$이다. Seo, Kim, No, Shin은 다음 정리를 증명하였다.

정리 1 (Seo, Kim, No, Shin [1]) p가 홀수인 소수이고, $n = 4k$, 그리고 $d = ((p^{2k}+1)/2)^2$라 하자. 그러면 p-진 m-sequence $s(t)$와 decimation된 수열 $s(dt+l)$

$(0 \le l < (p^{2k}+1)/2)$의 상호 상관 분포는 다음과 같이 주어진다. $l = 0$ 일 때,

$$C_l(\tau) = \begin{cases} -1, & \frac{(\sqrt{p^n}+1)(5\sqrt{p^n}-9)}{8} \text{ times} \\ -1-\sqrt{p^n}, & \frac{p^n-1}{4} \text{ times} \\ -1+\sqrt{p^n}, & \frac{\sqrt{p^n}+1}{2} \text{ times} \\ -1+2\sqrt{p^n}, & \frac{p^n-1}{8} \text{ times.} \end{cases}$$

그렇지 않을 때,

$$C_l(\tau) = \begin{cases} -1, & \frac{3(p^n-1)}{8} \text{ times} \\ -1-\sqrt{p^n}, & \frac{(\sqrt{p^n}+1)(3\sqrt{p^n}-7)}{8} \text{ times} \\ -1+\sqrt{p^n}, & \frac{(\sqrt{p^n}+1)(\sqrt{p^n}+3)}{8} \text{ times} \\ -1+2\sqrt{p^n}, & \frac{p^n-1}{8} \text{ times.} \end{cases}$$

여기서 τ는 $0 \le \tau < p^n - 1$이다. □

또한 다음과 같은 관계식도 [1]에서 찾을 수 있다.

$$\begin{aligned} A(b) &= \sum_{x \in F_{p^n}^*} \omega^{-\mathrm{tr}_1^n(bx^d)} \\ &= \begin{cases} \frac{p^n - p^{\frac{n}{2}}}{2} - 1, & \text{if } b = 1,\ l = 0 \\ -p^{\frac{n}{2}} - 1, & \text{otherwise.} \end{cases} \end{aligned} \quad (2)$$

3. 낮은 상관 특성을 갖는 수열군

정리 1로부터 주기가 $p^n - 1$인 p-진 수열군을 생성할 수 있다. $D = (p^{2k}+1)/2$이고 K가 α^{Dl} $(0 \le l < 2(p^{2k}-1))$의 집합이라 하자. 그러면 K 는 l이 짝수 또는 홀수일 때에 따라 $F_{p^{2k}}^*$와 K_2로 나눌 수 있다. 다음의 사전정리는 집합 $K_2 \cup \{0\}$의 한 가지 성질을 보여준다.

사전정리 2 $K_2 \cup \{0\}$ 는 덧셈에 대해 닫혀 있다.

Proof: 정수 l_1과 l_2에 대해 $\alpha^{D(2l_1+1)}$와 $\alpha^{D(2l_2+1)} \in K_2 \cup \{0\}$는 다음과 같이 된다.

$$\alpha^{D(2l_1+1)} + \alpha^{D(2l_2+1)} = \alpha^D(\alpha^{D(2l_1)} + \alpha^{D(2l_2)}).$$

$\alpha^{D(2l_1)}, \alpha^{D(2l_2)} \in F_{p^{2k}}^*$이기 때문에 $\alpha^{D(2l_1)} + \alpha^{D(2l_2)} \in F_{p^{2k}}$ 과 $\alpha^{D(2l_1+1)} + \alpha^{D(2l_2+1)} \in K_2 \cup \{0\}$가 된다. □

수열군 $\mathcal{S}'$를 다음과 같이 정의하자.

$$\mathcal{S}' = \{s_\beta(t) = \mathrm{tr}_1^n(\alpha^t + \beta\alpha^{dt}) \mid \beta \in F_{p^n}, 0 \le t < p^n - 1\}.$$

수열군 $\mathcal{S}'$에 포함된 두 개의 수열 $s_{\beta_1}(t)$와 $s_{\beta_2}(t)$에 대해서 $\beta_1 - \beta_2 \in K$일 때 (2)를 사용해서 다음을 유도할 수 있다.

$$\begin{aligned} \sum_{x \in F_{p^n}^*} \omega^{\mathrm{tr}_1^n((\beta_1-\beta_2)x^d)} &= \sum_{x \in F_{p^n}^*} \omega^{\mathrm{tr}_1^n(\alpha^{Dl}x^d)} \\ &= \sum_{x \in F_{p^n}^*} \omega^{\mathrm{tr}_1^n(\alpha^{Dl}x^D)} = \sum_{x \in F_{p^n}^*} \omega^{\mathrm{tr}_1^n(x^D)} \\ &= A(1) = (p^n - p^{n/2})/2 - 1. \end{aligned}$$

그러므로 $\mathcal{S}'$에서의 두 개의 수열의 상호 상관 값의 최대 크기는 $2\sqrt{p^n} - 1$ 보다 더 커질 수 있다. 상호 상관 값의 최대 크기가 $2\sqrt{p^n} - 1$로 제한되는 수열군을 생성하기 위해서 F_{p^n}에서 $\beta_1 - \beta_2 \in K$를 만족하는 원소들을 배제해야만 한다. 이런 원소들의 집합을 찾는데 다음의 사전정리를 사용할 수 있다.

사전정리 3 $\{x + y \mid x \in K_2 \cup \{0\},\ y \in F_{p^{2k}}\} = F_{p^n}$.

Proof: $|K_2 \cup \{0\}| = p^{2k}$와 $|F_{p^{2k}}| = p^{2k}$이기 때문에, 모든 원소 $x + y, x \in K_2 \cup \{0\}$ 그리고 $y \in F_{p^{2k}}$가 서로 다른 것을 보이는 것으로 충분하다. $x_1 + y_1 = x_2 + y_2$라 가정하자. 여기서 $x_i \in K_2 \cup \{0\}$ 이고 $y_i \in F_{p^{2k}}$이다. 그러면 $x_1 - x_2 = y_2 - y_1$와 사전정리 2는 $x_1 - x_2 = y_2 - y_1 = 0$를 함축한다. 즉 $x_1 = x_2$와 $y_1 = y_2$이다. □

$b_i - b_j \notin K (i \ne j)$를 만족하는 집합 $\mathcal{Z} = \{b_0, b_1, ...\} \subseteq F_{p^n}$를 찾으면 상호 상관 값의 최대 값이 $2\sqrt{p^n} - 1$인 수열군 $\mathcal{S}$를 생성할 수 있다.

정리 4 $K_2 \cup \{0\} = \{\zeta_0 = 0, \zeta_1, \zeta_2, \ldots, \zeta_{p^{2k}-1}\}$와 $F_{p^{2k}} = \{\gamma_0 = 0, \gamma_1, \gamma_2, \ldots, \gamma_{p^{2k}-1}\}$라 하자. 그러면 수열군 $\mathcal{S}$는 다음과 같이 정의된다.

$$\mathcal{S} = \{s_b(t) = \mathrm{tr}_1^n(\alpha^t + b\alpha^{dt}) \mid b \in \mathcal{Z}, 0 \le t < p^n - 1\}.$$

그러면 이 수열군의 자기상관과 상호 상관 함수는 집합 $\{-1, -1-\sqrt{p^n}, -1+\sqrt{p^n}, -1+2\sqrt{p^n}\}$에 있는 값을 취하고 수열군의 크기는 $p^{\frac{n}{2}}$이다. 여기서 $\mathcal{Z} = \{\zeta_i + \gamma_i \mid 0 \le i \le p^{2k} - 1\}$이다.

Proof: $i \ne j$일 때 $\zeta_i + \gamma_i - (\zeta_j + \gamma_j) \notin K$임을 보이는 것으로 충분하다. 즉,

$$\zeta_i + \gamma_i - (\zeta_j + \gamma_j) = (\zeta_i - \zeta_j) + (\gamma_i - \gamma_j) = \zeta + \gamma$$

이다. 여기서 $\zeta \in K_2$이고 $\gamma \in F_{p^{2k}}^*$이다. 그래서 사전정리 2와 사전정리 3로부터 $\zeta + \gamma \notin K$을 어렵지 않게 보일 수 있다. □

위의 $\mathcal{Z}$는 필요 조건인 $b_i - b_j \notin K$, $b_i, b_j \in \mathcal{Z}$가 어느 원소라도 하나를 더 더하면 만족하지 않는다는 의미에서 최대의 집합이다. 이것은 사전정리 3로부터 쉽게 보일 수 있다.

예제 5 $p = 3$, $n = 4$이고 α가 $x^4 + x^3 + 2x^2 + 2x + 2 = 0$의 근이라 하자. 그러면 다음의 수열 군 $\mathcal{S}$는 상호 상관 값의 최대 크기로 $2\sqrt{3^4} - 1 = 17$를 갖는다.

$$\mathcal{S} = \{s_b(t) = \mathrm{tr}_1^4(\alpha^t + b\alpha^{25t}) \mid b \in \mathcal{Z}, 0 \le t < 80\}.$$

이 때 $\mathcal{Z} = \{0, \alpha^3, \alpha^{13}, \alpha^{23}, \alpha^{33}, \alpha^{43}, \alpha^{53}, \alpha^{63}, \alpha^{73}\}$이다.

4. 큰 선형 복잡도를 갖는 p-진 수열군

이제 Seo, Kim, No, Shin [1]과 동일한 decimation $d = ((p^{2k}+1)/2)^2$를 갖는 새로운 p-진 수열군을 유도하자. 우선 [2]에 나오는 사전정리 1의 p-진 형태인 다음의 사전정리를 유도하는 것은 어렵지 않다.

사전정리 6 $n = 4k$라 하자. 그리고 $\{s(t)\}$ 가 다음과 같이 정의되는 수열이라 하자.

$$s(t) = \mathrm{tr}_{2k}^n(\alpha^t).$$

그러면 $t = (2i+1)T$, $0 \le i < (p^{2k}-1)/2$, 일 때 $s(t) = 0$이고 그렇지 않으면 $s(t) \in F_{p^{2k}}^*$이다. □

정리 1에서의 수열군을 사용하면 더 큰 선형 복잡도를 갖는 새로운 p-진 수열군이 다음의 정리에서처럼 생성될 수 있다.

정리 7 $n=4k$과 $(r,p^{2k}-1)=1$, $1\le r\le p^{2k}-2$,이라 하자. 그리고 p가 홀수인 소수라 하자. $\mathcal{S}_r$는 다음과 같이 정의되는 p-진 수열이라 하자.

$$\mathcal{S}_r=\{s_b(t)=\mathrm{tr}_1^{2k}([\mathrm{tr}_{2k}^n(\alpha^t)+\mathrm{tr}_{2k}^n(b\alpha^{dt})]^r) \mid b\in\mathcal{Z}, 0\le t<p^n-1\}.$$

여기서 $\mathcal{Z}=\{\zeta_i+\gamma_i \mid 0\le i\le p^{2k}-1\}$이다. 그러면 수열군 $\mathcal{S}_r$에 속하는 수열들의 상관 함수는 집합 $\{-1,-1-\sqrt{p^n},-1+\sqrt{p^n},-1+2\sqrt{p^n}\}$에 있는 값을 취한다.

Proof: $s_{b_1}(t)$와 $s_{b_2}(t)$의 상관 함수는 다음과 같이 쓸 수 있다.

$$C_{b_1,b_2}(\tau)=\sum_{t=0}^{p^n-2}\omega^{\mathrm{tr}_1^{2k}[\mathrm{tr}_{2k}^n(\alpha^{t+\tau})+\mathrm{tr}_{2k}^n(b_1\alpha^{dt+\tau})]^r} \times\omega^{-[\mathrm{tr}_{2k}^n(\alpha^t)+\mathrm{tr}_{2k}^n(b_2\alpha^{dt})]^r}. \quad (3)$$

$T=p^{2k}+1$이고 t_1과 t_2가 $t(0\le t\le p^n-2)$를 T를 기저로 정리했을 때의 각 자릿수라 하자. 즉, $t=t_1T+t_2$이다. 여기서 $0\le t_1\le p^n-2$이고 $0\le t_2\le T-1$이다. 그러면 $p^{2k}+3=0 \bmod 4$이기 때문에 $dT=T \bmod p^n-1$임이 쉽게 유도된다. 그러면 (3)은 다음과 같이 다시 정리할 수 있다.

$$\begin{aligned}&C_{b_1,b_2}(\tau)\\&=\sum_{t_2=0}^{T-1}\sum_{t_1=0}^{p^{2k}-2}\omega^{\mathrm{tr}_1^{2k}\left(\alpha^{rTt_1}\left([\mathrm{tr}_{2k}^n(\alpha^{t_2+\tau})+\mathrm{tr}_{2k}^n(b_1\alpha^{dt_2+\tau})]^r\right)\right)}\\&\quad\times\omega^{\mathrm{tr}_1^{2k}\left(\alpha^{rTt_1}\left(-[\mathrm{tr}_{2k}^n(\alpha^{t_2})+\mathrm{tr}_{2k}^n(b_2\alpha^{dt_2})]^r\right)\right)}\\&=-T+\sum_{t_2=0}^{T-1}\sum_{\beta\in F_{p^{2k}}}\omega^{\mathrm{tr}_1^{2k}(\beta h_r(t_2,\tau,b_1,b_2))}. \quad (4)\end{aligned}$$

여기서 $h_r(t_2,\tau,b_1,b_2)=[\mathrm{tr}_{2k}^n(\alpha^{t_2+\tau})+\mathrm{tr}_{2k}^n(b_1\alpha^{dt_2+\tau})]^r-[\mathrm{tr}_{2k}^n(\alpha^{t_2})+\mathrm{tr}_{2k}^n(b_2\alpha^{dt_2})]^r$이다. 만일 $h_r(t_2,\tau,b_1,b_2)\ne 0$라면, 안쪽에 있는 합은 0이 된다. 그렇지 않은 경우에는 안쪽의 합이 p^{2k}가 된다. 그래서 우리는 $h_r(t_2,\tau,b_1,b_2)=0$를 만족하는 t_2의 개수를 계산하여야 한다.

이제 $K_r(\tau,b_1,b_2)$가 $h_r(t_2,\tau,b_1,b_2)=0$를 만족하는 t_2, $0\le t_2\le T-1$,의 개수라 하자. $(r,p^{2k}-1)=1$이므로, $K_r(\tau,b_1,b_2)$는 다음을 만족하는 t_2의 개수와 같다.

$$\mathrm{tr}_{2k}^n(\alpha^{t_2+\tau})+\mathrm{tr}_{2k}^n(b_1\alpha^{dt_2+\tau})=\mathrm{tr}_{2k}^n(\alpha^{t_2})+\mathrm{tr}_{2k}^n(b_2\alpha^{dt_2}). \quad (5)$$

그러면 (4)는 다음과 같이 다시 쓸 수 있다.

$$C_{b_1,b_2}(\tau)=(K_1(\tau,b_1,b_2)-1)p^{2k}-1. \quad (6)$$

[1]에 있는 정리 2로부터, $K_1(\tau,b_1,b_2)$의 값은 이미 0, 1, 2, 3 중 하나를 취한다는 것이 증명되었다. 그래서 상관 함수는 다음의 집합에서 값을 취한다.

$$\{-1,-1-\sqrt{p^n},-1+\sqrt{p^n},-1+2\sqrt{p^n}\}.$$

□

5. 3진 수열군의 선형 복잡도

수열군 $\mathcal{S}$의 선형 복잡도는 다음 정리에서 유도한다.

정리 8 $\mathcal{S}$에 속한 수열들의 선형 복잡도 L'는 다음과 같이 주어진다.

$$L'=\begin{cases}4k=n, & \text{if } b=0\\ 6k=\frac{3n}{2}, & \text{otherwise.}\end{cases}$$

Proof: $b=0$이면 trace 함수의 성질로부터 자명하게 도출된다. $b\ne 0$일 때 $\mathcal{S}$에 속한 수열들을 다음과 같이 표현할 수 있다.

$$\begin{aligned}s_b(t)&=\mathrm{tr}_1^{2k}\left[\alpha^t+\alpha^{p^{2k}t}+b\alpha^{dt}+b^{p^{2k}}\alpha^{dp^{2k}t}\right]\\&=\sum_{i=0}^{2k-1}\left[\alpha^{p^it}+\alpha^{p^{2k+i}t}+(b^{p^i}+(-1)^tb^{p^{2k+i}})\alpha^{dp^it}\right].\end{aligned}$$

그래서 선형 복잡도는 $L'=2k\times 3=3n/2$가 된다. □

그러나 $\mathcal{S}_r$에 속한 수열들의 선형 복잡도를 일반적으로 유도하는 것은 쉬운 일이 아니다. 다음 정리에서는 3진 수열군의 선형 복잡도를 특별한 경우에 대해서 유도할 것이다.

우선 지수 r는 다음과 같이 p-진으로 확장할 수 있다.

$$r=\sum_{i=1}^{w}a_ip^{l_i},\qquad 1\le a_i\le p-1. \quad (7)$$

여기서 모든 i에 대해서 l_i는 $0\le l_i<2k$에 속하는 서로 다른 정수들이다. 그리고 w는 r의 Hamming weight이다. 즉, r의 p-진 확장에서의 0이 아닌 자릿수의 개수이다. 일반성을 잃지 않고서 $0=l_1<l_2<\cdots<l_w<2k$라 가정할 수 있다.

그러면 다음과 같이 $\mathcal{S}_r$에 속한 3진 수열들의 선형 복잡도를 특별한 경우에 대해 유도할 수가 있다.

정리 9 만일 $l_{i+1}>l_i+1$ 또는 $l_{i+1}=l_i+1$와 $2a_i<p$가 모든 i에 대해서 성립하면 $\mathcal{S}_r$에 속한 수열 $s_b(t)$의 선형 복잡도는 다음과 같이 주어진다.

$$L=\begin{cases}2k\prod_{i=1}^{w}(a_i+1), & \text{if } b=0\\ 2k\prod_{i=1}^{w}(a_i+2), & \text{if } \mathrm{tr}_{2k}^n(b)=\pm 1\\ 2k\prod_{i=1}^{w}(2a_i+1), & \text{otherwise.}\end{cases}$$

Proof: 수열 $s_b(t)$의 선형 복잡도는 다음과 같은 식에서 0이 아닌 항의 개수와 같다는 것이 잘 알려져 있다 [3].

$$s_b(t)=\sum_{j=0}^{p^n-2}c_j\alpha^{jt},\quad c_j\in F_p.$$

정의에 의해 다음과 같이 $s_b(t)$의 안쪽 trace 함수를 전개할 수 있다.

$$\mathrm{tr}_{2k}^n(\alpha^t+b\alpha^{dt})=(\alpha^t+b\alpha^{dt})^{p^{2k}}+\alpha^t+b\alpha^{dt}. \quad (8)$$

$\beta=\kappa^{(p^{2k}+1)/2}$와 $\gamma=\kappa^{2(p^{2k}-1)}$일 때 $\alpha=\beta\gamma$로 부터, (8)의 우변은 다음과 같이 쓸 수 있다.

$$(\beta\gamma)^{p^{2k}t}+b^{p^{2k}}(\beta\gamma)^{dp^{2k}t}+(\beta\gamma)^t+b(\beta\gamma)^{dt}. \quad (9)$$

그러면 $\beta^d = -\beta$, $\beta^{p^{2k}} = -\beta$, $\gamma^d = 1$, 그리고 $\gamma^{p^{2k}} = \gamma^{-1}$를 사용하면, (9)는 다음과 같이 된다.

$$\beta^t\gamma^{-t}(\gamma^{2t} + b^{p^{2k}}\gamma^t + b(-1)^t\gamma^t + (-1)^t).$$

이 방정식은 $(-1)^t\gamma^t$의 이차 방정식으로 볼 수 있다. $y = (-1)^t\gamma^t$와 $x = \beta^t\gamma^{-t}$라 하자. 그러면 $y^2 = (-1)^t x^{p^{2k}-1}$가 성립한다. 다시 말해 y는 $y = cx^{(p^{2k}-1)/2}$로 나타낼 수 있다. 여기서 c는 $c^2 = (-1)^t$를 만족하는 $F_{p^{2k}}$에 속한 한 원소이다. 그러면 $\mathcal{S}_r$에 속한 수열은 다음과 같이 쓸 수 있다.

$$s_b(t) = \mathrm{tr}_1^{2k}(x^r[y^2 + B(t)y + (-1)^t]^r). \quad (10)$$

여기서 $B(t) = b + (-1)^t b^{p^{2k}}$이다. 그러면 (10)은 다음과 같이 전개된다.

$$\mathrm{tr}_1^{2k}(x^r[y^2 + B(t)y + (-1)^t]^r) = \sum_{s=0}^{2k-1} x^{rp^s}[y^2 + B(t)y + (-1)^t]^{rp^s}.$$

$y = cx^{(p^{2k}-1)/2}$로부터, 다음 식이 성립한다.

$$x^r[y^2 + B(t)y + (-1)^t]^r = \sum_{l=0}^{2r} c_l x^{(p^{2k}-1)l/2+r}.$$

이제 $s_j > s_i$일 때 위의 식을 각각 p^{s_i}와 p^{s_j}로 지수를 올렸을 때, 동일한 차수의 항이 없음을 보이자. 만일 동일한 차수의 항이 있다면, 어떤 정수 l_1와 l_2, 그리고 M에 대해서 다음 식이 성립된다.

$$\frac{p^{2k}-1}{2}(l_1 p^s - l_2) + M(p^n - 1) = -(p^s - 1)r. \quad (11)$$

여기서 $0 < s = s_j - s_i \le 2k-1$이다. $(r, (p^{2k}-1)/2) = 1$이므로 우변은 $(p^{2k}-1)/2$로 나눠지지 않지만 좌변은 나눠진다. 따라서 모순이고 그러므로 중복되는 차수는 존재하지 않는다. 따라서 수열의 선형 복잡도는 (10)를 전개했을 때의 서로 다른 x의 항들의 개수의 정확히 $2k$배가 된다.

이제 다음의 두 가지 경우를 생각해 보자.

Case 1) t가 짝수일 경우:
$B_1 = \mathrm{tr}_{2k}^n(b) \in F_{p^{2k}}$라 하고 $g(y)$ 가 다음과 같이 정의된다.

$$g(y) = [1 + B_1 y + y^2]^r. \quad (12)$$

(7)를 사용하면, $g(y)$ 는 다음과 같이 된다.

$$g(y) = \prod_{i=1}^{w}[1 + (B_1 y)^{p^{l_i}} + (y^2)^{p^{l_i}}]^{a_i} = \prod_{i=1}^{w} g_i(y).$$

여기서 $g_i(y)$에 있는 y의 0이 아닌 지수들은 모두 p^{l_i}의 배수이고 p^{l_i}와 $2a_i p^{l_i} \le 2(p-1)p^{l_i}$사이의 값을 갖는다.

여기서는 $l_{i+1} > l_i + 1$ 또는 모든 i에 대해 $l_{i+1} = l_i + 1$와 $2a_i < p$가 성립하는 경우만 살펴보기 때문에 전체 항의 개수는 각각의 다항식 $g_i(y)$의 항의 개수를 셈으로써 구할 수 있다.

이제 다시 다음의 두 가지 경우를 나눠 보자.

Subcase 1-1) $B_1 = 0$;
$z = y^{p^{l_i}}$라 하면

$$g_i(z) = [1 + z^2]^{a_i} = \sum_{u=0}^{a_i}\binom{a_i}{u} z^{2u}.$$

$1 \le a_i \le p-1$이기 때문에 $\binom{a_i}{u}$는 $0 \le u \le a_i$에 대해 0이 아니다. 따라서 $g_i(y)$의 항의 개수는 $a_i + 1$개이다. 이 경우 선형 복잡도는 $2k\prod_{i=1}^{w}(a_i+1)$이다.

Subcase 1-2) $B_1 \neq 0$;
$z = y^{p^{l_i}}$라 하면

$$g_i(z) = [1 + B_1^{p^{l_i}} z + z^2]^{a_i}. \quad (13)$$

만일 $a_i = 1$라면, $g_i(z)$는 항이 3개이다. 만일 $a_i = 2$라면, $g_i(z) = z^4 - B_1 z^3 + (B_1^2 - 1)z^2 - B_1 z + 1$이다. 그러면 $B_1 = \mathrm{tr}_{2k}^n(b) = \pm 1$일 때 항의 개수는 4개이고 그렇지 않은 경우에는 항의 개수가 5개이다. 따라서 t가 짝수 일 때 $s_b(t)$의 선형 복잡도는 다음과 같이 주어진다.

$$L = \begin{cases} 2k\prod_{i=1}^{w}(a_i+2), & \text{if } \mathrm{tr}_{2k}^n(b) = \pm 1 \\ 2k\prod_{i=1}^{w}(2a_i+1), & \text{otherwise.} \end{cases}$$

Case 2) t가 음수:
이 경우에 $B_2 = b - b^{p^{2k}}$라 하면 다음 식을 얻는다.

$$\mathrm{tr}_1^{2k}([(y^2 + B_2 y - 1)]^r) = \sum_{s=0}^{2k-1}[(y^2 + B_2 y - 1)]^{rp^s}.$$

이 때 $B_2 = 0$이면, t가 짝수일 때와 동일하게 선형 복잡도는 $2k\prod_{i=1}^{w}(a_i+1)$이다. 만일 $B_2 \neq 0$이면, 다음과 같은 식을 얻는다.

$$g_i(z) = [z^2 + B_2^{p^{l_i}} z - 1]^{a_i}. \quad (14)$$

마찬가지로 만일 $a_i = 1$이면 $g_i(z)$의 항은 3개이다. 만일 $a_i = 2$라면 $g_i(z) = z^4 - B_2 z^3 + (B_2^2 + 1)z^2 + B_2 z + 1$이다. B_2^2는 $F_{p^{2k}}$에서 이차 비잉여(quadratic non-residue)이지만 F_p상의 원소는 $F_{p^{2k}}$에서 이차 잉여(quadratic residue)이므로 언제나 $B_2^2 \neq 1$가 된다. 따라서 t가 홀수일 때의 선형 복잡도는 다음과 같다.

$$L = 2k\prod_{i=1}^{w}(2a_i+1). \quad (15)$$

t가 짝수일 때와 t가 홀수 일 때 중 최소의 선형 복잡도가 실제 수열의 선형 복잡도가 되기 때문에 증명이 완료된다. □

6. 결론

이 논문에서는 Seo, Kim, No, Shin [1]의 논문에 대한 보충으로서 수열군을 생성하는 방법을 제시하였고 그 선형 복잡도도 유도하였다. 또한 더 큰 선형 복잡도

를 갖는 새로운 수열군을 생성하는 방법을 제시하였고 3진 수열의 특정 조건에 대해서 선형 복잡도를 유도하였다. 후자의 수열군은 전자의 경우를 $r = 1$인 특별 경우로 포함하고 있으며 $r \neq 1$인 경우 일반적으로 선형 복잡도는 크게 증가하게 된다. 따라서 전자의 수열군과 동일한 상관 특성을 가지면서도 더 높은 보안성을 제공해 줄 수 있다.

7. 감사의 글

본 연구는 교육과학기술부, 지식경제부, 노동부의 출연금으로 수행한 최우수실험실 지원 사업에 의한 연구 결과입니다.

참고 문헌

[1] E.-Y. Seo, Y.-S. Kim, J.-S. No, and D.-J. Shin, "Cross-correlation distribution of p-ary m-sequence of period $p^{4k} - 1$ and its decimated sequences by $((p^2k + 1)/2)^2$," in *Proc. IEEE Int. Symp. Information Theory (ISIT2007)*, Nice, France, Jun. 24-29, 2007, pp. 2516-2520.

[2] R. A. Scholtz and L. R. Welch, "GMW sequences," *IEEE Trans. Inf. Theory*, vol. IT-30, no. 3, pp. 548–553, May 1984.

[3] R. E. Blahut, "Transform techniques for error control codes," *IBM J. Res. Develop.*, vol. 23, pp. 299–315, 1979.