

# 낮은 상관 특성과 큰 선형 복잡도를 갖는 새로운 $p$ -진 수열군

정회원 김 영 식\*, 정 정 수\*\*, 종신회원 노 종 선\*\*, 신 동 준\*\*\*

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

Young-Sik Kim\*, Jung-Soo Chung\*\* *Regular Members*,  
Jong-Seon No\*\*, Dong-Joon Shin\*\*\* *Lifelong Members*

### 요 약

최근에 홀수인 소수  $p$ ,  $n = 4k$ , 그리고  $d = ((p^{2k} + 1)/2)^2$ 에 대해서 Seo, Kim, No, Shin<sup>[1]</sup>이  $m$ -sequence와  $d$ 로 decimation한 부분 수열들 사이의 상관 분포를 유도하였다. 하지만 이러한 상관 분포로부터 수열군이 자명하게 결정되지는 않는다. 본 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.

**Key Words :** Cross-correlation, Linear complexity, Linear span, Sequences

### ABSTRACT

For an odd prime  $p$ ,  $n = 4k$ , and  $d = ((p^{2k} + 1)/2)^2$ , Seo, Kim, No, and Shin<sup>[1]</sup> derived the correlation distribution of  $p$ -ary  $m$ -sequence of period  $p^n - 1$  and its decimated sequences by  $d$ . In this paper, two new families of  $p$ -ary sequences with family size  $p^{2k}$  and maximum correlation magnitude  $2\sqrt{p^n} - 1$  are constructed. The linear complexity of new  $p$ -ary sequences in the families are derived in the some cases and the upper and lower bounds of their linear complexity for general cases are presented.

### I. 서 론

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.

※ 본 논문은 교육과학기술부, 지식경제부, 노동부의 출연금으로 수행한 최우수실험실 지원 사업과 지식경제부 및 정보통신연구원진흥원의 IT핵심기술개발사업[2008-F-007-01, 3차원 환경에서의 지능형 무선 통신 시스템]에 의한 연구 결과입니다.

※ 본 논문은 2008 JCCI 우수논문으로 추천되었습니다.

\* 삼성전자(kingsi@ccl.snu.ac.kr), \*\* 서울대학교 전기·컴퓨터공학부 및 뉴미디어통신공동연구소(integer@ccl.snu.ac.kr, jsno@snu.ac.kr)

\*\*\* 한양대학교 전자전기공학부(djshin@hanyang.ac.kr)

논문번호 : KICS2008-05-240, 접수일자 : 2008년 5월 23일, 최종논문접수일자 : 2008년 7월 4일

최근에 홀수인 소수  $p$ ,  $n=4k$ , 그리고  $d = ((p^{2k}+1)/2)^2$ 에 대해서 Seo, Kim, No, Shin [1]이  $m$ -sequence와  $d$ 로 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.

## II. 사전지식

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

$$s(t) = tr_1^n(\alpha^t).$$

이 논문에서는 다음의 정의들을 사용할 것이다.

- $D = (p^{2k} + 1)/2$ 이고  $d = D^2 = ((p^{2k} + 1)/2)^2$ ;
- $r$ 은  $1 \leq r < p^{2k} - 1$ ,  $\gcd(r, p^{2k} - 1) = 1$ 인 정수;
- $\kappa$ 는  $F_{p^n}$ 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;
- $\beta^{2k} = -\beta$ 이고  $\beta^d = -\beta$ ;
- $\gamma^{2k} = \gamma^{-1}$  이고  $\gamma^d = 1$ .

$\gcd(p^n - 1, d) = \frac{p^{2k} + 1}{2}$  이므로 주기가  $2p^{2k} - 2$ 인

$(p^{2k} + 1)/2$ 개의 서로 다른 decimation 된 수열  $s(dt+l)$  ( $0 \leq l < (p^{2k} + 1)/2$ )가 존재한다. 그러면  $s(t)$ 와  $s(dt+l)$  사이의 상호 상관 함수는 다음과 같이 정의된다.

$$C_l(\tau) = \sum_{x \in F_p^*} \omega^{tr_1^n(ax - bx^d)}. \quad (1)$$

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

**정리 1.** (Seo, Kim, No, Shin [1])  $p$ 가 홀수인 소수이고,  $n = 4k$  그리고  $d = ((p^{2k} + 1)/2)^2$ 라 하자. 그러면  $p$ -진  $m$ -sequence  $s(t)$ 와 decimation된 수열  $s(dt+l)$  ( $0 \leq l < (p^{2k} + 1)/2$ )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  $\tau$ 는  $0 \leq \tau < p^n - 1$ 이다.  $\square$

또한 다음과 같은 관계식도 [1]에서 찾을 수 있다.

$$A(b) = \sum_{x \in F_p^*} \omega^{tr_1^n(bx^d)} = \begin{cases} \frac{p^n - p^{n/2}}{2} - 1, & \text{if } b = 1, l = 0 \\ -p^{n/2} - 1, & \text{otherwise.} \end{cases} \quad (2)$$

## III. 낮은 상관 특성을 갖는 수열군

정리 1로부터 주기가  $p^n - 1$ 인  $p$ -진 수열군을 생성할 수 있다.  $D = (p^{2k} + 1)/2$ 이고  $K$ 가  $\alpha^{Dl}$  ( $0 \leq l < 2(p^{2k} - 1)$ )의 집합이라 하자. 그러면  $K$ 는  $l$

이 짝수 또는 홀수일 때에 따라  $F_{p^*}$ 와  $K_2$ 로 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.

**증명** 정수  $l_1$ 과  $l_2$ 에 대해  $\alpha^{D(2l_1+1)}$ 와  $\alpha^{D(2l_2+1)} \in K_2 \cup \{0\}$ 는 다음과 같이 된다.

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

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

수열군  $S'$ 를 다음과 같이 정의하자.

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

수열군  $S'$ 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.

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

그러므로  $S'$ 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  $F_{p^*}$ 에서  $\beta_1 - \beta_2 \in K$ 를 만족하는 원소들을 배제해야만 한다. 이런 원소들의 집합을 찾는데 다음의 사전정리를 사용할 수 있다.

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

**증명**  $|K_2 \cup \{0\}| = p^{2k}$ 와  $|F_{p^*}| = p^{2k}$ 이기 때문에, 모든 원소  $x+y, x \in K_2 \cup \{0\}$  그리고  $y \in F_{p^*}$ 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  $y_i \in F_{p^*}$ 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. □

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

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

$$S = \{s_b(t) = \text{tr}_1^n(\alpha^t + b\alpha^{dt}) \mid b \in P, 0 \leq t < p^n - 1\}.$$

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  $p^{n/2}$ 이다. 여기서  $P = \{\zeta_i + \gamma_j \mid 0 \leq i \leq p^{2k} - 1\}$ 이다.

**증명**  $i \neq j$ 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  $\gamma \in F_{p^*}$ 이다. 그래서 사전정리 2와 사전정리 3으로부터  $\zeta + \gamma \notin K$ 을 어렵지 않게 보일 수 있다. □

위의  $P$ 는 필요조건인  $b_i - b_j \notin K, b_i, b_j \in P$ 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  $\alpha$ 가  $x^4 + x^3 + 2x^2 + 2x + 2 = 0$ 의 근이라 하자. 그러면 다음의 수열군  $S$ 는 상호 상관 값의 최대 크기로  $2\sqrt{3^4} - 1 = 17$ 를 갖는다.

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

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

#### IV. 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.

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

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

정리 1에서의 수열군을 사용하면 더 큰 선형 복

잡도를 갖는 새로운  $p$ -진 수열군이 다음의 정리에 서처럼 생성될 수 있다.

$$\begin{aligned} & tr_{2k}^n(\alpha^{t_2+\tau}) + tr_{2k}^n(b_1\alpha^{dt_2+\tau}) \\ &= tr_{2k}^n(\alpha^{t_2}) + tr_{2k}^n(b_2\alpha^{dt_2}). \end{aligned} \quad (5)$$

**정리 7.**  $n=4k$ 과  $(r, p^{2k}-1)=1, 1 \leq r \leq p^{2k}-2$ , 이라 하자. 그리고  $p$ 가 홀수인 소수라 하자.  $S_r$ 는 다음과 같이 정의되는  $p$ -진 수열이라 하자.

그러면 (4)는 다음과 같이 다시 쓸 수 있다.

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

$$S_r = \{s_b(t) = tr_1^{2k}([tr_{2k}^n(\alpha^t) + tr_{2k}^n(b\alpha^{dt})]^r) \mid b \in P, 0 \leq t < p^n - 1\}.$$

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

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

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

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

### V. 3진 수열군의 선형 복잡도

수열군  $S$ 에 속한 수열들의 선형 복잡도는 다음과 같다.

$$C_{b_1, b_2}(\tau) = \sum_{t=0}^{p^n-2} \omega^{tr_1^{2k}[tr_{2k}^n(\alpha^{t+\tau}) + tr_{2k}^n(b_1\alpha^{dt+\tau})]^r} \times \omega^{-[tr_{2k}^n(\alpha^t) + tr_{2k}^n(b_2\alpha^{dt})]^r}. \quad (3)$$

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

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

그러나  $S_r$ 에 속한 수열들의 선형 복잡도를 일반적으로 유도하는 것은 쉬운 일이 아니다. 다음 정리에서는 3진 수열군의 선형 복잡도를 특별한 경우에 대해서 유도할 것이다.

우선 지수  $r$ 는 다음과 같이  $p$ -진으로 확장할 수 있다.

$$\begin{aligned} & C_{b_1, b_2}(\tau) \\ &= \sum_{t_2=0}^{T-1} \sum_{t_1=0}^{p^{2k}-2} tr_1^{2k}(\alpha^{rT}([tr_{2k}^n(\alpha^{t_2+\tau}) + tr_{2k}^n(b_1\alpha^{dt_2+\tau})]^r)) \\ & \quad \times \omega^{tr_1^{2k}(\alpha^{rT}(-[tr_{2k}^n(\alpha^{t_2}) + tr_{2k}^n(b_2\alpha^{dt_2})]^r))} \\ &= -T + \sum_{t_2=0}^{T-1} \sum_{\beta \in F_{p^{2k}}} \omega^{tr_1^{2k}(\beta h_r(t_2, \tau, b_1, b_2))}. \end{aligned} \quad (4)$$

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

여기서

$$h_r(t_2, \tau, b_1, b_2) = [tr_{2k}^n(\alpha^{t_2+\tau}) + tr_{2k}^n(b_1\alpha^{dt_2+\tau})]^r - [tr_{2k}^n(\alpha^{t_2}) + tr_{2k}^n(b_2\alpha^{dt_2})]^r.$$

여기서 모든  $i$ 에 대해서  $l_i$ 는  $0 \leq l_i < 2k$ 에 속하는 서로 다른 정수들이다. 그리고  $w$ 는  $r$ 의 Hamming weight이다. 즉,  $r$ 의  $p$ -진 확장에서의 0이 아닌 자릿수의 개수이다. 일반성을 잃지 않고서  $0 = l_1 < l_2 < \dots < l_w < 2k$ 라 가정할 수 있다.

그러면 다음과 같이  $S_r$ 에 속한 3진 수열들의 선형 복잡도를 특별한 경우에 대해 유도할 수가 있다.

만일  $h_r(t_2, \tau, b_1, b_2) \neq 0$ 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  $t_2$ 의 개수를 계산하여야 한다.

**정리 8.** 만일  $l_{i+1} > l_i + 1$  또는  $l_{i+1} = l_i + 1$ 와  $2a_i < p$ 가 모든  $i$ 에 대해서 성립하면  $S_r$ 에 속한 수열  $s_{b(t)}$ 의 선형 복잡도는 다음과 같이 주어진다.

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

$$L = 2k \prod_{i=1}^w (4a_i - A_b(i))$$

여기서

$$A_b(i) = \begin{cases} 3a_i - 1, & \text{if } b = 0 \\ 1, & \text{if } (a_i, b^{2(3^{2k-1})}) = (2, 2) \\ & \text{or } (a_i, b^{3^{2k+1}}) = (2, 2) \\ 0, & \text{otherwise.} \end{cases}$$

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

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

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

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

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

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

그러면  $\beta^t = -\beta, \beta^{p^{2k}} = -\beta, \gamma^d = 1$ , 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. 즉  $y = cx^{(p^{2k}-1)/2}$ 로 나타낼 수 있다. 여기서  $c$ 는  $c^2 = (-1)^t$ 를 만족하는  $F_{p^{2k}}$ 에 속한 한 원소이다. 그러면  $S_r$ 에 속한 수열은 다음과 같이 쓸 수 있다.

$$s_b(t) = tr_1^{2k}(x^r [y^2 + B(t)y + (-1)^t]^r). \quad (10)$$

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

$$\begin{aligned} tr_1^{2k}(x^r [y^2 + B(t)y + (-1)^t]^r) \\ = \sum_{s=0}^{2k-1} x^r p^s [y^2 + B(t)y + (-1)^t]^r p^s. \end{aligned}$$

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

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

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  $l_1$ 와  $l_2$ , 그리고  $M$ 에 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  $0 < s = s_j - s_i \leq 2k - 1$ 이다.  $(r, (p^{2k}-1)/2) = 1$ 이므로 우변은  $(p^{2k}-1)/2$ 로 나뉘지 않지만 좌변은 나뉘진다. 따라서 모순이고 그러므로 중복되는 차수는 존재하지 않는다. 따라서 수열의 선형 복잡도는 (10)을 전개했을 때의 서로 다른  $x$ 의 항들의 개수의 정확히  $2k$ 배가 된다.

이제 다음의 두 가지 경우를 생각해 보자.

Case 1)  $b$ 가 0인 경우:

$g(y)$ 가 다음과 같이 정의된다.

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

(7)를 사용하면,  $g(y)$ 는 다음과 같이 된다.

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

이 때  $z = y^{p^i}$ 라 하면

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

가 되고  $1 \leq a_i \leq p-1$ 이기 때문에  $\binom{a_i}{u}$ 는  $0 \leq u \leq a_i$ 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.

Case 2)  $b$ 가 0이 아닌 경우:

$g(y)$ 는 다음과 같이 된다.

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

여기서  $g_i(y)$ 는 다음과 같다.

$$g_i(z) = [z^2 + B(t)^{p^i}z + (-1)^t]^{a_i}.$$

$a_i = 1$ 일 때,  $B(t)$ 가 두 개의 항으로 구성되어 있으므로  $g_i(z)$ 는 항이 4개이다.  $a_i = 2$ 일 때,  $g_i(z) = z^4 - B(t)z^3 + (B(t)^2 - 1)z^2 - (-1)^t B(t)z + 1$ 이다. 그러면  $B(t)$ 가 두 개의 항으로 구성되어 있으므로 일반적으로는 8개의 항을 갖는다. 그러나 가운데  $B(t)^2 = 1$ 로부터  $b^{2(3^{2k-1})} = 2$  또는  $b^{3^{2k+1}} = 2$ 가 성립

할 때 항수가 하나 더 줄어들게 된다. 따라서 증명이 완료된다. □

### VI. 결 론

이 논문에서는 Seo, Kim, No, Shin[1]의 논문에 대한 보충으로서 수열군을 생성하는 방법을 제시하였고 그 선형 복잡도도 유도하였다. 또한 더 큰 선형 복잡도를 갖는 새로운 수열군을 생성하는 방법을 제시하였고 3진 수열의 특정 조건에 대해서 선형 복잡도를 유도하였다. 후자의 수열군은 전자의 경우를  $r=1$ 인 특별한 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.

### 참 고 문 헌

- [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.

김 영 식 (Young-Sik Kim)

정회원



2001년 2월 서울대학교 전기공학부 공학사

2003년 2월 서울대학교 전기컴퓨터공학부 석사

2007년 2월 서울대학교 전기컴퓨터공학부 박사

2007년 3월~현재 삼성전자

<관심분야> 시퀀스, 암호학, 오류정정부호, 디지털통신

정 정 수 (Jung-Soo Chung)

정회원



2003년 2월 서울대학교 전기공학부 공학사

2003년 3월~현재 서울대학교 대학원 전기·컴퓨터공학부 석·박사 통합과정

<관심분야> 시퀀스, 오류정정부호, 디지털통신

노 종 선 (Jong-Seon No)

종신회원



1981년 2월 서울대학교 전자공학과 공학사

1984년 2월 서울대학교 대학원 전자공학과 석사

1988년 5월 Univ. of Southern California, 전기공학과 공학박사

1988년 2월~1990년 7월 Hughes Network Systems, Senior MTS

1990년 9월~1999년 7월 건국대학교 전자공학과 부교수

1999년 8월~현재 서울대학교 전기컴퓨터공학부 교수

<관심분야> 시퀀스, 시공간부호, LDPC 부호, OFDM, 이동통신, 암호학

신 동 준 (Dong-Joon Shin)

종신회원



1990년 2월 서울대학교 전자공학과 공학사

1991년 Northwestern Univ. 공학 석사

1998년 5월 Univ. of Southern California, 전기공학과 공학박사

1999년 4월~2000년 8월 Member

Technical Staff at Hughes Network Systems

2000년 9월~현재 한양대학교 전자통신컴퓨터 부교수

<관심분야> 부호이론, 시퀀스, 이산수학, 디지털통신