# Decimation에 의해 생성된 $p$-진 m-시퀀스 군의 상호 상관 값의 분포

정회원 서 은 영*, 김 영 식**, 종신회원 노 종 선***, 신 동 준****

# Cross-Correlation Distribution of a $p$-ary m-Sequence Family Constructed by Decimation

Eun-Young Seo*, Young-Sik Kim** ***Regular Members,***
Jong-Seon No***, Dong-Joon Shin**** ***Lifelong Members***

요 약

홀수인 소수 $p$와 $n=4k$, 그리고 $d=((p^{2k}+1)/2)^2$에 대해서, 주기가 $p^n-1$인 $p$-진 m-수열 $s(t)$에 대해서 $(p^{2k}+1)/2$개의 서로 다른 decimated 수열들 $s(dt+l)$, $0\le l<(p^{2k}+1)/2$가 존재한다. 이 논문에서는 $s(t)$와 $s(dt+l)$, $0\le l<(p^{2k}+1)/2$ 사이의 상호상관 값이 $\{-1,-1\pm\sqrt{p^n},-1+2\sqrt{p^n}\}$과 같음을 보이고, 상호 상관 값의 분포를 유도하였다.

**Key Words :** Cross-correlation, Cross-correlation distribution, $p$-ary m-sequence, Decimation, Sequences

ABSTRACT

For an odd prime $p$, $n=4k$ and $d=((p^{2k}+1)/2)^2$, there are $(p^{2k}+1)/2$ distinct decimated sequences $s(dt+l)$, $0\le l<(p^{2k}+1)/2$, of a $p$-ary m-sequence $s(t)$ of period $p^n-1$. In this paper, it is shown that the cross-correlation function between $s(t)$ and $s(dt+l)$ takes the values in $\{-1,-1\pm\sqrt{p^n},-1+2\sqrt{p^n}\}$ and their cross-correlation distribution is also derived.

## Ⅰ. 서 론

낮은 상호상관 값을 갖는 수열 군에 대한 연구가 오랫동안 진행되었는데[1]-[4], 특히 주기가 $p^n-1$인 $p$-진 수열 군을 만들기 위해 $\gcd(d,p^n-1)=1$을 만족시키는 decimation 값 $d$에 관한 연구가 활발히 진행되었다[5]-[8]. 하지만 낮은 상호상관 값을 가지는 시퀀스 군을 만드는데 있어 decimation 값 $d$가 반드시 그런 성질을 만족 시킬 필요는 없으므로 주기 $p^n-1$과 서로소가 아닌 decimation 수 $d$를 이용한 수열 군에 대한 연구도 진행되었다[9].

홀수인 소수 $p$와 $n=4k$, 그리고 $d=((p^{2k}+1)/2)^2$에 대해서, $\gcd(d,p^n-1)=(p^{2k}+1)/2$이므로 주기가 $p^n-1$인 $p$-진 m-진 수열 $s(t)$에 대해서 $(p^{2k}+1)/2$개의 서로 다른 decimated 수열 $s(dt+l)$, $0\le l<(p^{2k}+1)/2$, 가 존재한다. 이 논문에서는 $s(t)$

※ 본 논문은 교육과학기술부, 지식경제부, 노동부의 출연금으로 수행한 최우수실험실 지원 사업과 지식경제부 및 정보통신연구진흥원의 IT핵심기술개발사업[2008-F-007-01, 3차원 환경에서의 지능형 무선 통신 시스템]에 의한 연구 결과입니다.
※ 본 논문은 2007 JCCI 우수논문으로 추천되었습니다.
* University of Maryland, 전기컴퓨터공학과 (eunyoung00@gmail.com), ** 삼성전자 (mypurist@gmail.com)
*** 서울대학교, 전기·컴퓨터공학부 및 뉴미디어통신공동연구소(jsno@snu.ac.kr)
**** 한양대학교, 전자전기공학부(djshin@hanyang.ac.kr)
논문번호 : KICS2007-06-263, 접수일자 : 2007년 6월 10일, 최종논문접수일자 : 2008년 8월 18일

와 $s(dt+l)$, $0 \le l < (p^{2k}+1)/2$ 사이의 상호상관 값이 집합 $\{-1, -1 \pm \sqrt{p^n}, -1+2\sqrt{p^n}\}$에서 값을 취함을 보이고, 상호상관 값의 분포를 구하였다.

## Ⅱ. 사전지식

$p$가 홀수인 소수이고 $F_{p^n}$는 $p^n$개의 원소를 갖는 유한체라 하자. 그러면 $F_{p^n}$에서 $F_{p^m}$으로의 trace 함수는 $x \in F_{p^n}$와 $m|n$에 대해서 다음과 같이 정의된다.

$$tr_m^n(x) = \sum_{i=0}^{n/m-1} x^{p^{im}}$$

$\alpha$가 $F_{p^n}$상의 원시원일 때 trace 함수를 이용해서 주기가 $p^n-1$인 $p$-진 m-수열 $s(t)$를 $tr_1^n(\alpha^t)$로 쓸 수 있다. 이 논문에서는 다음과 같은 표기들이 사용될 것이다.

- $n=4k$, $k$: 양의 정수, $\delta$: $F_{p^n}$상의 원시원;
- $d=((p^{2k}+1)/2)^2$;
- $\beta=\delta^{((p^{2k}+1)/2)^2}$, $\gamma=\delta^{2(p^{2k}-1)}$, 그리고 $\alpha=\beta\gamma$.

또한 다음의 성질들을 사용할 것이다.

- $\gcd((p^{2k}+1)/2, 2(p^{2k}-1))=1$;
- $\gcd(p^n-1, ((p^{2k}+1)/2)^2)=(p^{2k}+1)/2$;
- $d=(\frac{p^{2k}+1}{2})^2=\begin{cases} p^{2k} \bmod 2(p^{2k}-1) \\ 0 \quad \bmod (p^{2k}+1)/2 \end{cases}$;
- $\beta^{p^{2k}}=-\beta$, $\beta^d=-\beta$, $\gamma^{p^{2k}}=\gamma^{-1}$, $\gamma^d=1$;
- 모든 양의 정수 $t$에 대해서 $\gamma^t \ne -1$.

$\gcd(p^n-1, d)=(p^{2k}+1)/2$이므로 서로 다른 decimated 수열 $s(dt+l)(0 \le l < (p^{2k}+1)/2)$가 $(p^{2k}+1)/2$개 존재하고 $tr_1^n(\alpha^{dt+l})$로 정의된다. 이 때 수열의 주기는 $2(p^{2k}-1)$이다. 그러면 $\omega$가 $p$차 복소근이고, $a=\alpha^\tau$, $b=\alpha^l$일 때, $s(t)$와 decimated 수열 $s(dt+l)$ 사이의 상호상관 값은 다음과 같다.

$$C_l(\tau)=\sum_{t=0}^{p^n-2}\omega^{tr_1^n(\alpha^{t+\tau}-\alpha^{dt+l})}=\sum_{x\in F_{p^n}^*}\omega^{tr_1^n(ax-bx^d)}. \quad (1)$$

## Ⅲ. 상호 상관 값의 계산

이 장에서는 (1)의 상호상관 값이 가질 수 있는 값을 구할 것이다. 다음의 보조정리는 Helleseth[6]에 증명된 것으로 앞으로의 정리를 증명하는데 사용할 것이다.

보조정리 1.[6] $p$가 홀수인 소수이고 $n$이 짝수인 정수일 때 다음이 성립한다.

$$\sum_{y\in F_{p^n}}\omega^{tr_1^n(ay^{p^{\frac{n}{2}}+1})}=\begin{cases} p^n, & \text{if} \quad a+a^{p^{\frac{n}{2}}}=0 \\ -p^{\frac{n}{2}}, & \text{if} \quad a+a^{p^{\frac{n}{2}}}\ne 0. \end{cases}$$

□

정리 2. (1)에서 주어진 $p$-진 m-수열 $s(t)$와 decimated 수열 $s(dt+l)(0 \le l < (p^{2k}+1)/2)$과의 상호 상관 값은 집합 $\{-1, -1 \pm \sqrt{p^n}, -1+2\sqrt{p^n}\}$에서 값을 취한다.

증명) Helleseth의[6] 정리 3.8의 증명과 비슷한 방법으로 정리 2를 증명할 수 있다. $x=\alpha^j y^{p^{2k}+1}$ $(0 \le j < p^{2k}+1)$라 하면 $y \in F_{p^n}$인 $y$에 대해서 $y^{(p^{2k}+1)d}=y^{p^{2k}+1}$이고 (1)은 다음과 같이 쓸 수 있다.

$$C_l(\tau)+1=\frac{1}{p^{2k}+1}\sum_{j=0}^{p^{2k}}\sum_{y\in F_{p^n}}\omega^{tr_1^n(y^{p^{2k}+1}(a\alpha^j-b\alpha^{dj}))}. \quad (2)$$

$K(a,b)$를 다음 식의 해 $j$의 개수라고 하자.

$$tr_{2k}^n(a\alpha^j-b\alpha^{dj})=(a\alpha^j-b\alpha^{dj})^{p^{2k}}+a\alpha^j-b\alpha^{dj}=0,$$
$$0 \le l < p^{2k}+1. \quad (3)$$

보조정리 1에 의해서 (2)는 다음과 같이 쓸 수 있다.

$$C_l(\tau)=-1+p^{2k}(K(a,b)-1).$$

또한 $\alpha=\beta\gamma$, $\beta^d=-\beta$, $\beta^{p^{2k}}=-\beta$, $\gamma^d=1$, $\gamma^{p^{2k}}=\gamma^{-1}$를 이용하면 (3)을 다음과 같이 나타낼 수 있다.

$$a\gamma^{2j}-b^{p^{2k}}\gamma^j-b(-1)^j\gamma^j+a^{p^{2k}}(-1)^j=0,$$
$$0 \le j < p^{2k}+1. \quad (4)$$

(4)의 해의 개수인 $K(a,b)$는 (4)를 $(-1)^j\gamma^j$에 대한 다음과 같은 두 가지 방정식으로 나타냄으로써 구할 수 있다.

1) $j$가 짝수 일 때;

$$a((-1)^j\gamma^j)^2-(b+b^{p^{2k}})(-1)^j\gamma^j+a^{p^{2k}}=0 \quad (5)$$

2) $j$가 홀수일 때:

$$a((-1)^j\gamma^j)^2+(b-b^{p^{2k}})(-1)^j\gamma^j-a^{p^{2k}}=0. \quad (6)$$

(5)와 (6)의 방정식은 $(-1)^j\gamma^j$에 대한 이차방정식이므로 각각 두 개씩 $K(a,b)$의 값은 최대 4이다. 하지

만 (5)가 두 개의 서로 다른 근을 가지면 (6)은 두 개의 서로 다른 근을 가질 수 없고, 역도 마찬가지임을 근과 계수의 관계를 이용하여 어렵지 않게 보일 수 있으므로 $K(a,b)$는 0, 1, 2, 3만 가능하다. 그러므로 가능한 $C_l(\tau)$의 값은 $-1, -1\pm p^{2k}, -1+2p^{2k}$이다.

□

## Ⅳ. 상호 상관 값의 분포

이 장에서는 (1)번에서 정의된 수열의 상호상관 값의 분포, 다시 말해 각각의 상호 상관 값의 발생 회수를 구할 것이다. 이를 위해서 먼저 $\sum C_l(\tau)$, $\sum C_l^2(\tau)$, $\sum C_l^3(\tau)$의 값을 구할 것이다.

정리 3. $\sum C_l(\tau)$는 다음과 같이 구할 수 있다.

$$\sum_{\tau=0}^{p^n-2} C_l(\tau)=\begin{cases}\dfrac{-p^n+p^{\frac{n}{2}}}{2}+1, & \text{if } l=0\\ p^{\frac{n}{2}}+1, & \text{otherwise.}\end{cases}$$

증명) (1)에 의해서 $\sum C_l(\tau)$는 다음과 같이 표현된다.

$$\sum_{\tau=0}^{p^n-2} C_{l(\tau)}=\sum_{a\in F_{p^n}^*}\sum_{x\in F_{p^n}^*}\omega^{tr_1^n(ax-bx^d)}=-\sum_{x\in F_{p^n}^*}\omega^{tr_1^n(bx^d)}.$$

$d$가 홀수이고, $\gcd((p^{2k}+1)/2, 2(p^{2k}-1))=1$이므로 $\sum_{x\in F_{p^n}^*}\omega^{tr_1^n(bx^d)}=\sum_{x\in F_{p^n}^*}\omega^{tr_1^n(bx^{(p^{2k}+1)/2})}$이다. Square $x$에 대해서는 $x=y^2$, nonsquare $x$에 대해서는 nonsquare $z$를 이용하여 $x=zy^2$라 두면 다음과 같다.

$$2(1-\sum_{\tau=0}^{p^n-2} C_{l(\tau)})=\sum_{y\in F_{p^n}}\omega^{tr_1^n(by^{p^{2k}+1})}+\sum_{y\in F_{p^n}}\omega^{tr_1^n(bz^{\frac{p^{2k}+1}{2}}y^{p^{2k}+1})}. \quad (7)$$

보조정리 1에서, 모든 $b=\alpha^l, 0\le l<(p^{2k}+1)/2$, 에 대해서 $b+b^{p^{2k}}$는 0이 아니기 때문에 첫 번째 합 부분은 다음과 같다.

$$\sum_{y\in F_{p^n}}\omega^{tr_1^n(by^{p^{2k}+1})}=-p^{\frac{n}{2}} \quad (8)$$

두 번째 합 부분에서, $z^{p^{2k}(p^{2k}+1)/2}=-z^{(p^{2k}+1)/2}$를 이용하면 $bz^{\frac{p^{2k}+1}{2}}+(bz^{\frac{p^{2k}+1}{2}})^{p^{2k}}=0$는 $b^{p^{2k}-1}=1$이고, 즉 $b$는 1이므로 두 번째 합 부분은 다음과 같다.

$$\sum_{y\in F_{p^n}}\omega^{tr_1^n(bz^{\frac{p^{2k}+1}{2}}y^{p^{2k}+1})}=\begin{cases}p^n, & \text{if } b=1,\ i.e.,\ l=0\\ -p^{\frac{n}{2}}, & \text{otherwise.}\end{cases} \quad (9)$$

(8)과 (9)를 (7)에 대입하면 $\sum C_l(\tau)$를 구할 수 있다.

□

정리 4. $\sum C_l^2(\tau)$는 다음과 같이 주어진다.

$$\sum_{\tau=0}^{p^n-2} C_l^2(\tau)=\begin{cases}\dfrac{3p^{2n}+2p^{\frac{3n}{2}}-p^n-4p^{\frac{n}{2}}}{4}-1, & \text{if } l=0\\ p^{2n}-2p^n-2p^{\frac{n}{2}}-1, & \text{otherwise.}\end{cases}$$

증명) $\sum C_l^2(\tau)$는 다음과 같이 표현된다.

$$\begin{aligned}\sum_{\tau=0}^{p^n-2} C_l^2(\tau)&=\sum_{x_1,x_2\in F_{p^n}^*}\omega^{-tr_1^n(b(x_1^d+x_2^d))}\sum_{a\in F_{p^n}^*}\omega^{tr_1^n(a(x_1+x_2))}\\&=(p^n-1)^2-\sum_{x_1\in F_{p^n}^*}\sum_{\substack{x_2\in F_{p^n}^*\\ x_2\ne -x_1}}\omega^{-tr_1^n(b(x_1^d+x_2^d))}.\end{aligned}$$

정리 3을 이용하면 $\sum C_l^2(\tau)$는 다음과 같이 계산된다.

$$\sum_{\tau=0}^{p^n-2} C_l^2(\tau)=p^{2n}-p^n-(\sum_{\tau=0}^{p^n-2} C_l(\tau))^2.$$

□

원시원 $\delta$와 $\beta=\delta^{(p^{2k}+1)/2}$, $\gamma=\delta^{2(p^{2k}-1)}$을 이용하여, $\sum C_l^3(\tau)$의 값을 구하는 정리 9에 사용될 보조정리와 정리들을 유도할 것이다.

보조정리 5. $F_{p^n}^*$상에서 정의된 $(p^{2k}+1)/2$ to 1 함수 $f: x\to x^d$는 다음과 같은 성질들을 가진다.

1) $f(\beta^{2u}\gamma^t)=\beta^{2u}$;

2) $f(\beta^{2u+1}\gamma^t)=-\beta^{2u+1}$,

$$0\le u<p^{2k}-1,\ 0\le t<(p^{2k}+1)/2.$$

증명) $\beta^d=-\beta$와 $\gamma^d=1$을 이용하면 위의 성질을 어렵지 않게 이끌어 낼 수 있다.

□

보조정리 6. 아래 방정식의 모든 해는 $F_{p^n}$상에 있는 $p^{2k}$개의 모든 원소이다.

$$1+x^d-(1+x)^d=0,\quad x\in F_{p^n} \quad (10)$$

증명) $x=-1$이 (10)의 해가 되는 것은 자명한데, $x\neq-1$이라 가정하면 수식 (10)은 $1+x^d=(1+x)^d=\beta^{2u}$로 쓸 수 있다. 보조정리 5로부터 (10)의 해는 어떤 정수 $t_1$과 $t_2$에 대해서 다음을 만족해야한다.

$$x=(\beta^{2u}-1)\gamma^{t_1}=\beta^{2u}\gamma^{t_2}-1. \tag{11}$$

$t_1\neq t_2$이면, (11)은 다음과 같다.

$$\beta^{2u}=\frac{1-\gamma^{t_1}}{\gamma^{t_2}-\gamma^{t_1}}. \tag{12}$$

$\beta^{2u}$는 $F^*_{p^{2k}}$상의 원소이고, $\gamma^{p^{2k}}=\gamma^{-1}$이므로, (12)의 양변에 $(p^{2k}-1)$승을 하면 $1=\gamma^{t_2}$를 얻을 수 있다. (11)과 $t_2=0$으로부터 $t_1=t_2=0$이 되는데 이것은 $t_1\neq t_2$라는 가정에 위배된다. 그러므로 $t_1=t_2=0$이고, $x=\beta^{2u}-1$이 된다. 그러므로 $x=-1$을 포함하면 (11)의 해는 $F_{p^{2k}}$상의 $p^{2k}$개의 원소가 된다. □

보조정리 7. $0\le e<p^{2k}-1$라 하면 모든 각각의 $i$ $(1\le i<(p^{2k}+1)/2)$에 대해서, $1+\beta^{2e+1}=\beta^u\alpha^i$을 만족시키는 해 $e$가 $e_1$, $p^{2k}-2-e_1$의 쌍으로 두 개씩 존재한다. 여기서 $\alpha$는 $F_{p^n}$상의 원시원이고, $u$는 $0\le u<2(p^{2k}-1)$ 사이의 어떤 정수이다.

증명) 모든 $e$에 대해서 $i\neq0$임은 어렵지 않게 알 수 있다. 같은 $i$에 대해서 다음을 가정하자.

$$1+\beta^{2e_1+1}=\beta^{u_1}\alpha^i,\ 1+\beta^{2e_2+1}=\beta^{u_2}\alpha^i,$$
$$0\le e_1\neq e_2<p^{2k}-1.$$

위 두 식에 각각 $2(p^{2k}-1)$승을 한 후 각각의 식을 나눈 후 $\beta^{p^{2k}-1}=-1$의 성질을 이용하면 $e_1$과 $e_2$사이의 관계식을 아래와 같이 얻을 수 있다.

$$\beta^{2e_2}-\beta^{2e_1}=\beta^{2(e_1+e_2+1)}(\beta^{2e_2}-\beta^{2e_1}).$$

여기서 $e_1\neq e_2$이기 때문에 $e_1+e_2+1=0\bmod(p^{2k}-1)$가 된다. 그러므로 고정된 $i$에 대해서 $e_1$과 $p^{2k}-2-e_1$이 동시에 $1+\beta^{2e+1}=\beta^u\alpha^i$에서 해 $e$가 됨을 알 수 있다. 여기서 $e$는 $p^{2k}-1$개의 서로 다른 값을 가질 수 있고 $i$는 0을 제외하고 $(p^{2k}-1)/2$개의 서로 다른 값을 가질 수 있으므로 각각의 $i$에 대해서 위와 같은 두 개의 해가 존재함을 알 수 있다. □

다음의 정리 8에서는 $1+x^d-(1+x)^d=\beta^u\alpha^i$을 만족시키는 $x$의 개수를 구할 것이다.

정리 8. $0\le u<2(p^{2k}-1)$와 $0\le i<(p^{2k}+1)/2$인 $u$와 $i$에 대해 아래 식의 해는 다음과 같다.

$$1+x^d-(1+x)^d=\beta^u\alpha^i,\ x\in F^*_{p^n} \tag{13}$$

$i=0$을 만족하는 $x$는 $(p^{2k}-1)(p^{2k}+3)/4$개 존재하고, 0이 아닌 각각의 $i$에 대해서는 각각 $3(p^{2k}-1)/2$개의 해 $x$가 존재한다.

증명) 증명은 크게 $i$가 0인 경우와 0이 아닌 경우로 나눈 뒤 그 아래 각각 $x$에 따라 네 가지 경우로 나누어서 생각할 것이다.

경우 **1)** $i=0$:

이 경우에 있어 총 $(p^{2k}-1)(p^{2k}+3)/4$개의 (13)을 만족하는 해 $x$가 존재함을 증명할 것이다.

경우 **1-1)** $x$: square, $1+x$: square;

차수가 2인 원분수(cyclotomic number)의 성질로부터 [13] $x$는 square이고 동시에 $1+x$는 nonsquare인 $x$는 $(p^n-1)/4$개 존재한다. 이 경우에 있어 $1+x^d$과 $(1+x)^d$ 모두 $F^*_{p^{2k}}$상의 원소이고, 그러므로 (13)의 오른쪽 식은 $\beta^u$형태가 된다. 보조정리 6에 의해서 $1+x^d-(1+x)^d=0$이 되는 해를 제외하면 (13)의 해 $x$는 다음과 같다.

$$\frac{p^{4k}-1}{4}-(p^{2k}-1)=\frac{(p^{2k}-1)(p^{2k}-3)}{4}$$

경우 **1-2)** $x$: square, $1+x$: nonsqurae;

먼저 이 경우에 있어 $1+x^d=0\Leftrightarrow i=0$이라는 것을 보일 것이다. 여기서 보조정리 5에 의해서 $(1+x)^d=-\beta^{2u_1+1}$이므로 $1+x^d=0$이면 $i=0$이여야 한다. 역을 증명하기 위해서 $1+x^d\neq0$이면 $i\neq0$임을 모순을 통해 보일 수 있다. 다음으로 $1+x^d=0$을 만족하는 $x$는 모두 nonsquare임을 보일 것이다. 보조정리 5에 의해서 $x^d=-1$을 만족하는 $x$는 $-\gamma^{t_1}$으로 나타낼 수 있고, 그러므로 square임을 알 수 있다. 이 때 $1+x$가 square라 가정하면 $1+x$는 $\beta^{2u}\gamma^{t_2}$로 표현할 수 있고, $-\gamma^{t_1}=\beta^{2u}\gamma^{t_2}-1$를 얻을 수 있는데, 이 식은 다시 $\beta^{2u}=(1-\gamma^{t_1})\gamma^{-t_2}$로 쓸 수 있다. 여기서 양변에 $(p^{2k}-1)$승을 하게 되면 $1=-\gamma^{2t_2-t_1}$을 얻게 된다. 하지만 $\gamma$의 성질상 어떤 $t_1$과 $t_2$를 대입하더라도 이 식을 만족 시킬 수는 없고 따라서 $1+x$는 nonsquare가 된다. 여기서 $1+x^d=0$을 만족시키는 $F^*_{p^n}$상의 해 $x$는 $-1$을 제외하고 $(p^{2k}-1)/2$개가 됨을 알 수 있다.

**경우 1-3)** $x$: nonsquare, $1+x$: square;

경우 1-2)와 비슷한 방법으로 $x$와 $1+x$의 역할을 반대로 생각하면 이 경우에도 역시 (13)의 해 $x$는 $(p^{2k}-1)/2$개 임을 알 수 있다.

**경우 1-4)** $x$: nonsquare, $1+x$: nonsquare;

이 경우에 있어 먼저, $x^d-(1+x)^d=0 \Leftrightarrow i=0$임을 보일 것이다. 순방향의 증명은 자명하고, 역방향의 증명은 $x^d-(1+x)^d \neq 0 \Rightarrow i \neq 0$임을 모순을 유도하여 보일 수 있다. 다음으로 $x$와 $1+x$가 모두 nonsquare일 때 $x^d=(1+x)^d$을 만족하는 $x$의 개수를 구할 것이다. $x^d=(1+x)^d=-\beta^{2u_1+1}$이라고 둘 수 있고, 보조정리 5에 의해서 이식은 $\gamma^{t_1}\beta^{2u_1+1}=\gamma^{t_2}\beta^{2u_1+1}-1$로 쓸 수 있다. 이것은 다시 아래와 같이 나타낼 수 있다.

$$\beta^{2u_1+1}=\frac{1}{\gamma^{t_2}-\gamma^{t_1}}. \tag{14}$$

(14)의 양변에 $(p^{2k}-1)$승을 하게 되면, $-1=-\gamma^{t_1+t_2}$을 얻을 수 있는데, 이것은 $t_1=-t_2$를 의미한다. 또한 (14)를 만족하는 $u_1$은 각각의 다른 $t_1$과 $t_2=-t_1$을 만족하는 $t_2$ 순서쌍에 대해서, 다른 값을 가짐을 보일 것이다. 같은 $u_1$을 가지면서 (14)를 만족하는 서로 다른 $t_1$과 $t_1'$이 있다고 가정하면 $\gamma^{t_1}-\gamma^{t_1'}=\gamma^{t_1'}-\gamma^{t_1}$을 만족해야 하는데, $\gamma^{(t_1+t_1')}\neq -1$이므로 이것은 불가능하다. 이 경우에 있어, $t_1$은 $1\le t_1<(p^{2k}+1)/2$이므로, (13)을 만족하는 nonsquare $x$의 개수는 총 $(p^{2k}-1)/2$개 임을 알 수 있다.

**경우 2)** $i\neq 0$: 0이 아닌 각각의 $i$에 대해서 아래 네 가지 경우를 고려할 때 (13)을 만족하는 $x$의 개수는 $3(p^{2k}-1)/2$개씩 있음을 보일 것이다.

**경우 2-1)** $x$: square, $1+x$: square;

경우 1-1)에서 보였듯이 이 경우에는 (13)을 만족하는 해가 없음을 알 수 있다.

**경우 2-2)** $x$: square, $1+x$: nonsquare;

보조정리 5 로부터 square $x$와 nonsquare $1+x$에 대해서 아래 식을 만족하는 $u_1$, $u_2$가 존재한다. 여기서 $0\le u_1$, $u_2<p^{2k}-1$이다.

$$1+x^d=\beta^{2u_1},\ (1+x)^d=-\beta^{2u_2+1}. \tag{15}$$

이것은 다음을 만족시켜야 한다.

$$\beta^{2u_1}+\beta^{2u_2+1}=\beta^u\alpha^i. \tag{16}$$

여기서 각각의 $i(1\le i<(p^{2k}+1)/2)$에 대해서 (13)식을 만족시키는 해 $x$의 개수가 $(p^{2k}-1)/2$임을 다음의 과정을 통해 증명할 수 있다. 증명 과정은 생략하도록 하겠다.

- 과정1: (15)에서 $x$로부터 $(u_1,u_2)$으로의 mapping이 1-1 이다.
- 과정2: 각각의 $i$에 대해서 (15)와 (16)식을 만족시키는 가능한 $(u_1,u_2)$의 순서쌍이 $(p^{2k}+1)/2$개 있다.
- 과정3: 각각의 $i$에 대해서 과정2에서 구한 가능한 해 중 딱 하나만이 해가 아니다.

**경우 2-3)** 그 이외의 경우;

경우 2-2)와 비슷한 증명과정으로 각각의 $i$에 대해서 (13)을 만족하는 nonsquare $x$가 $(p^{2k}-1)/2$개씩 있음을 보일 수 있다. □

보조정리 6과 정리 8을 이용하여 다음의 정리 9에서 $\sum C_l^3(\tau)$를 구할 수 있다.

정리 9. $\sum C_l^3(\tau)$는 다음과 같이 주어진다.

$$\sum_{\tau=0}^{p^n-2} C_l^3(\tau)=\begin{cases}\frac{3}{4}p^{2n+2k}-\frac{7}{4}p^{2n}-\frac{7}{4}p^{n+2k} \\ \qquad +\frac{5}{4}p^n+\frac{3}{2}p^{2k}+1, & \text{if } l=0 \\ \frac{3}{4}p^{2n+2k}-2p^{2n}+\frac{1}{4}p^{n+2k} \\ \qquad +5p^{n+3p^{2k}}+1, & \text{otherwise.}\end{cases}$$

증명) $\sum C_l^3(\tau)$는 다음과 같이 전개 할 수 있다.

$$\sum_{\tau=0}^{p^n-2} C_l^3(\tau)=(p^n-1)\sum_{\substack{x_1,x_2,x_3\in F_{p^n}^* \\ x_1+x_2+x_3=0}}\omega^{-tr_1^n(b(x_1^d+x_2^d+x_3^d))} - \sum_{\substack{x_1,x_2,x_3\in F_{p^n}^* \\ x_1+x_2+x_3\neq 0}}\omega^{-tr_1^n(b(x_1^d+x_2^d+x_3^d))}.$$

위 식의 첫 번째 합은 다음과 같이 정리된다.

$$(p^n-1)\sum_{\substack{x_1,x_2,x_3\in F_{p^n}^* \\ x_1+x_2+x_3=0}}\omega^{-tr_1^n(b(x_1^d+x_2^d+x_3^d))}$$
$$=(p^n-1)[\sum_{x_1,x_2\in F_{p^n}^*}\omega^{tr_1^n(b(x_1^d+x_2^d-(x_1+x_2)^d))}-(p^n-1)].$$

두 번째 합은 다음과 같이 정리된다.

$$
\begin{aligned}
&-\sum_{x_1,x_2\in F_{p^n}^*} \omega^{-tr_1^n(b(x_1^d+x_2^d)} \sum_{\substack{x_3\in F_{p^n}^* \\ x_3\neq -(x_1+x_2)}} \omega^{-tr_1^n(bx_3^d)} \\
&\quad =-\sum_{x_1,x_2\in F_{p^n}^*} \omega^{-tr_1^n(b(x_1^d+x_2^d))}\Big[\sum_{x_3\in F_{p^n}^*}\omega^{-tr_1^n(bx_3^d)} \\
&\qquad -\omega^{tr_1^n(b(x_1+x_2)^d)}\Big]-\sum_{x_1\in F_{p^n}^*}\omega^{-tr_1^n(bx_1^d)}\omega^{tr_1^n(bx_1^d)}.
\end{aligned}
$$

그러므로 $y=x_2/x_1$일 때, 상호상관 값의 세제곱의 합은 다음과 같이 정리할 수 있다.

$$
\begin{aligned}
\sum_{\tau=0}^{p^n-2} C_l^3(\tau) &= p^n \sum_{x_1,y\in F_{p^n}^*} \omega^{-tr_1^n(bx_1^d(1+y^d-(1+y)^d))} \\
&\quad +\Big(\sum_{\tau=0}^{p^n-2} C_l(\tau)\Big)^3-(p^{2n}-p^n).
\end{aligned}
$$

보조정리 6과 정리 8로부터 $x$가 $F_{p^n}^*$상에서 변할 때, 다음의 사실을 알고 있다.

$$
1+x^d-(1+x)^d
=\begin{cases}
0, & p^{2k}-1 \text{ times} \\
\beta^u, & \dfrac{(p^{2k}-1)(p^{2k}+3)}{4} \text{ times} \\
\beta^u\alpha^i, & \dfrac{3(p^{2k}-1)}{2} \text{ times for each nonzero } i.
\end{cases}
$$

여기서 $i$는 $1\le i<(p^{2k}+1)/2$이고, $u$는 $0\le u<2(p^{2k}-1)$ 사이의 어떤 정수이다. 그러면 위의 사실로부터 $\sum C_l^3(\tau)$을 아래와 같이 구할 수 있다.

$$
\sum_{\tau=0}^{p^n-2} C_l^3(\tau)=
\begin{cases}
p^n\Big[(p^{2k}-1)(p^n-1)+\dfrac{(p^{2k}-1)(p^{2k}+3)}{4}A_0 \\
\quad +\dfrac{3(p^{2k}-1)^2}{4}A_1\Big]-A_0^3-(p^{2n}-p^n), & \text{if } l=0 \\
p^n\Big[(p^{2k}-1)(p^n-1)+\dfrac{3(p^{2k}-1)}{2}A_0+ \\
\dfrac{(p^{2k}-1)(2p^{2k}-3)}{2}A_1\Big]-A_1^3-(p^{2n}-p^n), & \text{otherwise.}
\end{cases}
$$

여기서 $A_0=(p^n-p^{2k}-2)/2$이고, $A_1=-p^{2k}-1$이다. □

정리 2, 3, 4, 9를 이용하여 $s(t)$와 $s(dt+l)$사이의 상호상관 값의 분포는 다음 정리 10에서 구할 수 있다.

정리 10. $p$는 홀수인 소수이고, $n=4k$, $d=((p^{2k}+1)/2)^2$일 때 $p$-진 m-수열 $s(t)$와 그것의 decimated 수열 $s(dt+l)$, $0\le l<(p^{2k}+1)/2$, 사이의 상호상관 값의 분포는 다음과 같다.

1) $l=0$;

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

otherwise:

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

여기서 $\tau$는 $0\le\tau<p^n-1$이다. □

## 참 고 문 헌


〔1〕 R. Gold, Maximal recursive sequences with 3-valued recursive cross-correlation functions, *IEEE Trans. Inf. Theory*, Vol.14, pp.154-156, Jan. 1968.

〔2〕 T. Kasami, Weight distribution formula for some class of cyclic codes, Coordinated Sci. Lab., Univ. Illinois, Urbana-Champaign, Tech. Rep. R-285 (AD 632574), 1996.

〔3〕 J.-S. No and P. V. Kumar, A new family of binary pseudorandom sequences having optimal periodic correlation properties and large linear span, *IEEE Trans. Inf. Theory*, Vol.35, No.2, pp.371-379, Mar. 1989.

〔4〕 J.-W. Jang, Y.-S. Kim, J.-S. No, and T. Helleseth, New family of p-ary sequences with optimal correlation property and large linear span, *IEEE Trans. Inf. Theory*, Vol.50, No.8, pp.1839-1844, Aug. 2004.

〔5〕 H. M. Trachtenberg, On the c'ross- correlation functions of maximal recurring sequences, Ph.D. dissertation, Univ. of Southern California, Los Angeles, CA, 1970.

〔6〕 T. Helleseth, Some results about the cross- correlation function between two maximal linear sequences, *Discrete Math.*, Vol.16, pp.209-232, 1976.

〔7〕 P. V. Kumar and O. Moreno, Prime-phase sequences with periodic correlation properties better than binary sequences, *IEEE Trans. Inf. Theory*, Vol.37, No.3, pp.603-616, May 1991.

〔8〕 H. Dobbertin, T. Helleseth, P. V. Kumar, and H. Martinsen, Ternary m-sequences with three-valued cross-correlation function: new decimations of Welch and Niho type, *IEEE Trans. Inf. Theory*, Vol.47, No.4, pp.1473-1481, May 2001.

〔9〕 G. J. Ness, T. Helleseth, and A. Kholosha, On the correlation distribution of the Coulter-Matthews decimation, *IEEE Trans. Inf. Theory*, Vol.52, No.5, pp.2241-2247, May 2006.

〔10〕 T. Storer, Cyclotomy and Difference Sets, Lectures in Advanced Mathematics. Chicago, IL: Markham, 1967.



**서 은 영** (Eun-Young Seo) 정회원

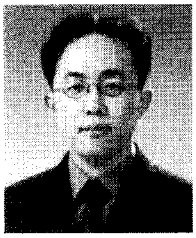
2005년 2월 서울대학교 전기컴퓨터공학부 공학사

2007년 2월 서울대학교 전기컴퓨터공학부 공학석사

2007년 8월~현재 University of Maryland, 전기컴퓨터공학과 박사과정

<관심분야> 시퀀스, Network Capacity

**김 영 식** (Young-Sik Kim) 정회원



2001년 2월 서울대학교 전기공학부 공학사

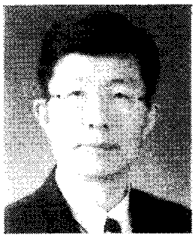
2003년 2월 서울대학교 전기컴퓨터공학부 공학석사

2007년 2월 서울대학교 전기컴퓨터공학부 박사

2007년 3월~현재 삼성전자

<관심분야> 시퀀스, 오류정정부호, 디지털통신, 암호학

**노 종 선** (Jong-Seon No) 종신회원



1981년 2월 서울대학교 전자공학과 공학사

1984년 2월 서울대학교 대학원 전자공학과 공학석사

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 12월 Northwestern Univ., 전기공학과 공학석사

1998년 12월 USC, 전기공학과 공학박사

1999년 1월~1999년 4월 Research Associate (USC)

1999년 4월~2000년 8월 Hughes Network Systems, MTS

2000년 9월~현재 한양대학교 전자통신컴퓨터공학부 부교수

<관심분야> 디지털통신, 이산수학, 시퀀스, 오류정정부호, 암호학