p-진 m-수열과 $\frac{p^n+1}{p+1}+\frac{p^n-1}{2}$로 Decimation된 m-수열의 상호 상관 값 유도

*최성태O, * 임태형, *노종선, **정하봉
*서울대학교 전기컴퓨터공학부, 뉴미디어통신공동연구소
**홍익대학교 전자전기공학부
stchoi@ccl.snu.ac.kr, jayelish@gmail.com, jsno@snu.ac.kr, habchung@hongik.ac.kr

On the Cross-Correlation Function of a p-ary m-sequence and its Decimated Sequence by $\frac{p^n+1}{p+1}+\frac{p^n-1}{2}$

요약

본 논문에서는 소수 $p \equiv 1 \bmod 4$, 홀수 n, 그리고 $d = \frac{p^n+1}{p+1} + \frac{p^n-1}{2}$에 대해서 p-진 m-수열과 그의 decimation m-수열 $m(dt)$의 상호 상관 값을 유도한다. 상호 상관 값은 $\{-1, -1 \pm p^{n/2}, -1 + \frac{\pm 1 \pm \sqrt{p}}{2} p^{n/2}, -1 + \frac{p-1}{2} p^{n/2}, -1 + \frac{-p+1}{2} p^{n/2}\}$의 값들을 갖는 것을 보인다.

1. 개요

m-수열은 잘 알려진 이상적인 상관 특성을 갖는 수열이다. 지난 수십 년 동안, 이진이 아닌 p-진 m-수열 $m(t)$와 그의 decimation 수열 $m(dt)$의 상호 상관 값의 분포를 구하고 그를 수식적으로 보이는 연구가 진행되어 왔다. 특히 $\gcd(d, p^n - 1) = 1$인 경우에 대해서 Trachtenberg [1], Helleseth [2], 그리고 Dobbertin, Helleseth, Kumar, 그리고 Martinsen [3] 이 연구를 하였다.

Decimation 값 $d = \frac{p^n+1}{p+1} + \frac{p^n-1}{2}$에 대해, Muller [4] 그리고 Hu *et al.* [5]는 각각 $p = 3$ 그리고 홀수의 소수 $p \equiv 3 \mod 4$에 대해서 $m(t)$와 decimation 시퀀스들의 상호 상관 값의 크기의 상한 값을 구하였다. 그들의 경우에서는 $\gcd(d, p^n - 1) = 2$이기 때문에 decimation 수열이 $m(dt)$와 $m(dt+1)$가 존재한다.

본 논문에서는 같은 decimation 값인 $d = \frac{p^n+1}{p+1} + \frac{p^n-1}{2}$, 홀수인 소수 $p \equiv 1 \mod 4$, 그리고 홀수의 n에 대해서 $m(t)$와 $m(dt)$의 상호 상관 값들을 구하였다.

2. 사전 지식 및 기호

A. *Trace* 함수 및 상호 상관 함수

p는 소수이고 F_{p^n}은 원소의 개수가 p^n인 유한체라 하자. F_{p^n}에서 F_p로 가는 trace 함수 $\mathrm{tr}_k^n(\cdot)$는 다음과 같이 정의된다.

$$\mathrm{tr}_k^n(x) = \sum_{i=0}^{\frac{n}{k}-1} x^{p^{ki}}$$

여기서 $x \in F_{p^n}$ 이고 $k|n$이다.

α 는 F_{p^n}의 원시 원소일 때 주기 $p^n - 1$인 p-진 m-수열 $m(t)$는 다음과 같이 표현된다.

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

주기 N인 Z_q상의 수열 $s_1(t)$와 $s_2(t)$의 상호 상관 함수는 다음과 같이 정의된다.

$$C(\tau) = \sum_{t=0}^{N-1} \omega_q^{s_1(t+\tau) - s_2(t)} \quad (1)$$

여기서 τ는 수열의 이동 값이고 ω_q는 q차 복소 원시근이다.

B. 이차 형식

F_{p^n} 상에서 이차 character는 다음과 같이 정의된다.

$$\eta(x) = \begin{cases} 1, & \text{if } x\text{가 } F_{p^n}^*\text{의 제곱원인 경우} \\ -1, & \text{if } x\text{가 } F_{p^n}^*\text{의 비제곱원인 경우} \\ 0, & \text{if } x = 0\text{인 경우.} \end{cases}$$

F_p 상에서 n 변수의 이차 형식은 차수가 2인 $F_p[x_1, x_2, \cdots, x_n]$에서의 동차 다항식이고 다음과 같이 표현된다.

$$f(x_1, x_2, \cdots, x_n) = \sum_{i,j \le n} a_{ij} x_i x_j \quad (2)$$

여기서 $a_{ij} \in F_p$이다.

$(F_p)^n$은 F_p상에서의 n-차원 벡터 공간이라 하자. 임의의 $b \in F_p$에 대해 이차 형식의 방정식 $f(x_1, x_2, \cdots, x_n) = b$을 만족시키는 해의 개수 $(x_1, x_2, \cdots, x_n) \in (F_p)^n$는 이차 형식 $f(x_1, x_2, \cdots, x_n)$의 rank로부터 결정된다. 이어지는 보조정리는 어떻게 이차 형식의 rank를 계산할 수 있는가 보여준다.

보조정리 1 ([4]): $f \in F_p[x_1, x_2, \cdots, x_n]$는 이차 형식일 때, 다음을 정의한다.

$$Z := \{\mathbf{z} \in (F_p)^n : f(\mathbf{x}+\mathbf{z}) - f(\mathbf{x}) = 0, \text{ for all } \mathbf{x} \in (F_p)^n\}. \tag{3}$$

그러면 Z는 $(F_p)^n$의 부분 공간이고 f의 rank는 $n - \dim(Z)$이다.

따름정리 1: F_{p^n}에서 F_p로 가는 이차 형식 $f(x)$에 대해 $p^{n-\rho}$는 $f(x+z) = f(x)$ 를 모든 $x \in F_{p^n}$에 대해 만족하는 해 $z \in F_{p^n}$의 개수이다. 이 때 이차 형식 f의 rank는 ρ와 같다.

(2)에서의 a_{ij}들로 (i,j)번째 원소가 a_{ij}인 $n \times n$ 행렬 A를 만들었을 때, 행렬 A의 행렬식 $\det(A)$를 이차 형식 f의 행렬식이라고 정의한다.

이어지는 보조정리에서는, rank k인 이차 형식 $f \in F_p[x_1, x_2, \cdots, x_k]$에 대해서, $f(x) = b$ in F_{p^n}을 만족하는 해의 개수 $x \in F_{p^k}$를 어떻게 계산하는지를 보여준다.

보조정리 2 ([6]): Rank k인 이차 형식 $f(x_1, x_2, \cdots, x_k)$에 대해 $f(\mathbf{x}) = b \in F_p$를 만족하는 해 $\mathbf{x} \in (F_p)^k$의 개수 $N(b)$는 다음과 같이 결정된다. 여기서 Δ는 f의 행렬식을 가리키고 η는 F_p에서의 이차 character이다.

Case 1) k는 짝수일 때;

$$N(b) = \begin{cases} p^{k-1} - \epsilon p^{\frac{k-2}{2}}, & \text{if } b \neq 0 \\ p^{k-1} + \epsilon(p-1)p^{\frac{k-2}{2}}, & \text{if } b = 0 \end{cases}$$

여기서 $\epsilon = \eta((-1)^{k/2}\Delta)$이다.

Case 2) k는 홀수일 때;

$$N(b) = \begin{cases} p^{k-1} + \epsilon\eta(b)p^{\frac{k-1}{2}}, & \text{if } b \neq 0 \\ p^{k-1}, & \text{if } b = 0 \end{cases}$$

여기서 $\epsilon = \eta((-1)^{(k-1)/2}\Delta)$이다.

본 논문에서는 다음과 같이 정의된 기호들을 사용하고자 한다.

- $p \equiv 1 \bmod 4$는 홀수의 소수;
- n은 홀수;
- Decmation 값 $d = \frac{p^n+1}{p+1} + \frac{p^n-1}{2}$;
- α는 유한체 F_{p^n}의 원시 원소;
- ω는 p-차 복소 원시근;
- $F_{p^n}^*$는 $F_{p^n} \setminus \{0\}$이다.

3. 상호 상관 함수 계산

이동 값 τ에서의 $m(t)$와 $m(dt)$의 상호 상관 값 $C(\tau)$는 다음과 같이 쓸 수 있다.

$$\begin{aligned} C(\tau) &= \sum_{t=0}^{p^n-2} \omega^{m(t+\tau)-m(dt)} \\ &= \sum_{t=0}^{p^n-2} \omega^{\mathrm{tr}_1^n(\alpha^{t+\tau}-\alpha^{dt})} \\ &= \sum_{x \in F_{p^n}^*} \omega^{\mathrm{tr}_1^n(ax-x^d)} \end{aligned} \tag{4}$$

여기서 $a = \alpha^\tau$이다.

$S(a)$는 다음과 같이 정의된다.

$$S(a) = \sum_{x \in F_{p^n}} \omega^{\mathrm{tr}_1^n(ax-x^d)}. \tag{5}$$

상관 함수 $C(\tau)$는 $C(\tau) = S(a) - 1$과 같이 표현될 수 있다. $F_{p^n}^*$의 절반은 제곱원들이고 나머지 절반은 비제곱원들인 것은 자명하다. $\gcd(p+1, p^n-1) = 2$이므로 제곱원들은 $x = y^{p+1}$와 같이 표현할 수 있고 비제곱원들은 $x = ry^{p+1}$와 같이 표현할 수 있다. 여기서 $y \in F_{p^n}$이고 r은 F_p^*상에서 임의의 비제곱원이다. 즉, y가 F_{p^n}상에서 변함에 따라서 제곱원과 비제곱원은 각각 두 번씩 발생한다. 그러므로 $S(a)$는 다음과 같이 표현할 수 있다.

$$\begin{aligned} 2S(a) &= \sum_{y \in F_{p^n}} \omega^{\mathrm{tr}_1^n(ay^{p+1}-y^2)} + \sum_{y \in F_{p^n}} \omega^{\mathrm{tr}_1^n(ary^{p+1}-r^dy^2)} \\ &= \sum_{y \in F_{p^n}} \omega^{\mathrm{tr}_1^n(ay^{p+1}-y^2)} + \sum_{y \in F_{p^n}} \omega^{r\mathrm{tr}_1^n(ay^{p+1}+y^2)} \\ &= \sum_{y \in F_{p^n}} \omega^{g(y)} + \sum_{y \in F_{p^n}} \omega^{h(y)} \end{aligned} \tag{6}$$

여기서 $g(y) = \mathrm{tr}_1^n(ay^{p+1} - y^2)$ 이고 $h(y) = r\mathrm{tr}_1^n(ay^{p+1} + y^2)$이다.

$y \in F_{p^n}$을 F_p 상에서 F_{p^n}의 기저를 $\{\alpha_1, \alpha_2, \cdots, \alpha_n\}$로 표현을 하면 $y = \sum_{i=1}^n y_i\alpha_i$와 같이 표현할 수 있다. 여기서 $y_i \in F_p$이다. 이를 이용해 $g(y)$가 이차 형식인 것을 다음과 같이 보일 수 있다.

$$\begin{aligned} g(y) &= \mathrm{tr}_1^n\Big(a(\sum_{i=1}^n y_i\alpha_i^p)(\sum_{i=1}^n y_i\alpha_i) - (\sum_{i=1}^n y_i\alpha_i)^2\Big) \\ &= \mathrm{tr}_1^n\Big(a\sum_{i=1}^n\sum_{j=1}^n (y_iy_j)(\alpha_i^p\alpha_j) - \sum_{i=1}^n\sum_{j=1}^n (y_iy_j)(\alpha_i\alpha_j)\Big) \\ &= \sum_{i=1}^n\sum_{j=1}^n y_iy_j\mathrm{tr}_1^n(a\alpha_i^p\alpha_j - \alpha_i\alpha_j) \\ &= \sum_{i=1}^n\sum_{j=1}^n y_iy_jg_{ij} \end{aligned}$$

여기서 $g_{ij} = \mathrm{tr}_1^n(a\alpha_i^p\alpha_j - \alpha_i\alpha_j)$.

비슷한 방법으로 $h(y)$가 이차 형식인 것도 보일 수 있다. $g(y)$와 $h(y)$가 이차 형식이기 때문에 $S(a)$의 값을 구하기 위해서는 각 이차 형식의 rank를 구해야 한다. 따름정리 1로부터 모든 $y \in F_{p^n}$에 대해서 $g(y+z) = g(y)$와 $h(y+z) = h(y)$를 만족하는 해 $z \in F_{p^n}$의 개수를 구해야 한다.

보조정리 3: 모든 y에 대해 $g(y+z) = g(y)$를 만족하는 해의 개수 $z \in F_{p^n}$의 개수는 다음 방정식을 만족하는 해의 개수와 같다.

$$L_g(z) = a^pz^{p^2} - 2z^p + az = 0 \tag{7}$$

그리고 모든 y에 대해 $h(y+z)=h(y)$를 만족하는 해의 개수 $z\in F_{p^n}$의 개수는 다음 방정식을 만족하는 해의 개수와 같다.

$$L_h(z)=a^pz^{p^2}+2z^p+az=0. \tag{8}$$

Proof: 방정식 $g(y+z)=g(y)$은 다음과 같이 쓸 수 있다.

$$\mathrm{tr}_1^n(a(y+z)^{p+1}-(y+z)^2)=\mathrm{tr}_1^n(ay^{p+1}-y^2). \tag{9}$$

(9)를 다시 쓰면

$$\mathrm{tr}_1^n(y^p(a^pz^{p^2}-2z^p+az)+az^{p+1}-z^2)=0. \tag{10}$$

그러므로 (10)이 모든 $y\in F_{p^n}$에 대해 성립하는 것과

$$\mathrm{tr}_1^n(az^{p+1}-z^2)=0 \tag{11}$$

과 (7)이 동시에 성립하는 것은 동치이다. 그러므로 (9)를 만족하는 해 $z\in F_{p^n}$의 개수는 (7)와 (11)를 동시에 만족하는 해 $z\in F_{p^n}$의 개수와 같다.

이제는 (7)를 만족하는 해는 (11) 역시 만족함을 보이도록 하자. (7)로부터

$$2z^p=a^pz^{p^2}+az$$

이다. 양변에 p^{i-1} 승을 하고 z^{p^i}를 곱해주면

$$2z^{2p^i}=a^{p^i}z^{p^{i+1}+p^i}+a^{p^{i-1}}z^{p^i+p^{i-1}} \tag{12}$$

이다. (12)로부터, (11)는 다음과 같이 전개할 수 있다.

$$\begin{aligned}&\mathrm{tr}_1^n(az^{p+1}-z^2)\\&=\sum_{i=0}^{n-1}(a^{p^i}z^{p^{i+1}+p^i}-z^{2p^i})\\&=\sum_{i=0}^{n-1}\left(a^{p^i}z^{p^{i+1}+p^i}-2^{-1}(a^{p^i}z^{p^{i+1}+p^i}+a^{p^{i-1}}z^{p^i+p^{i-1}})\right)\\&=0.\end{aligned}$$

그리므로 $g(y+z)=g(y)$를 만족하는 해의 개수는 (7)의 해의 개수와 같음을 증명할 수 있다. ■

위의 보조정리를 통해서 $g(y)$와 $h(y)$의 rank를 결정하기 위해서 각각 (7)와 (8)를 만족하는 해의 개수를 구해야 함을 알 수 있다. $L_g(z)$와 $L_h(z)$의 해의 집합은 벡터공간을 이루고 차수는 p^2이기 때문에 가질 수 있는 해의 개수는 1, p, 또는 p^2개이다. 또한 두 식 중 적어도 한 식의 근의 개수는 1개여야 함을 다음 보조정리로부터 보일 수 있다.

보조정리 4: n_g와 n_h는 각각 $L_g(z)=0$와 $L_h(z)=0$를 만족하는 해의 개수라고 놓자. 그러면 n_g와 n_h 중 적어도 하나는 1이다.

Proof: $L_g(z)=0$와 $L_h(z)=0$가 각각 0이 아닌 해 z_1와 z_2를 갖는다고 가정하자. $L_g(z_1)=0$와 $L_h(z_2)=0$를 다시 쓰면 다음과 같다.

$$a^pz_1^{p^2-p}+az_1^{1-p}=2$$

$$a^pz_2^{p^2-p}+az_2^{1-p}=-2$$

그러므로 두 식으로부터,

$$a^p(z_1^{p^2-p}+z_2^{p^2-p})+a(z_1^{1-p}+z_2^{1-p})=0.$$

$z_1^{1-p}+z_2^{1-p}\neq 0$를 이용하여 위 식을 다시 쓰면,

$$\begin{aligned}&a^{p-1}\frac{z_1^{p^2-p}+z_2^{p^2-p}}{z_1^{1-p}+z_2^{1-p}}\\&=a^{p-1}(z_1z_2)^{p-1}(z_1^{p-1}+z_2^{p-1})^{p-1}\\&=-1\end{aligned}$$

이는 -1이 원시 원소의 $p-1$승의 형태로 나타날 수 없기 때문에 모순이다. 그러므로 두 식 중 적어도 하나는 근을 $z=0$만 갖는다. ■

위의 보조정리로부터 가능한 해의 개수 (n_g,n_h)는 $(1,1)$, $(1,p)$, $(1,p^2)$, $(p,1)$, 그리고 $(p^2,1)$이다. 이로부터 이어지는 따름정리를 쉽게 유도 가능하다.

따름정리 2: r_g와 r_h은 각각 이차 형식 $g(y)$와 $h(y)$의 rank를 의미한다. 가능한 rank (r_g,r_h)는 (n,n), $(n,n-1)$, $(n,n-2)$, $(n-1,n)$, 또는 $(n-2,n)$이다.

이어지는 정리는 보조정리 5의 증명을 위해 필요하다.

정리 1 ([6]): p는 홀수의 소수이고 η는 F_p의 이차 character라 하자.

$$\sum_{i=1}^{p-1}\eta(i)\omega^i=\begin{cases}p^{\frac{1}{2}}, & \text{if } p\equiv 1 \bmod 4\\ ip^{\frac{1}{2}}, & \text{if } p\equiv 3 \bmod 4\end{cases}$$

여기서 ω는 p-차 복소 원시근이다.

정리 2 ([6]): $f\in F_{p^n}[x]$는 차수 s가 $s\geq 1$이고 $\gcd(s,p^n)=1$인 다항식이다. χ는 F_{p^n}에서의 nontrivial additive character이다.

$$|\sum_{c\in F_{p^n}}\chi(f(c))|\leq(s-1)p^{n/2}.$$

보조정리 5: (6)에서 정의된 $S(a)$의 크기는 다음과 같이 상한 된다.

$$|S(a)|\leq\frac{p-1}{2}p^{\frac{n}{2}}.$$

Proof: (6)으로부터, 다음을 보여야 한다.

$$\Big|\sum_{y\in F_{p^n}}\omega^{\mathrm{tr}_1^n(ay^{p+1}-y^2)}+\sum_{y\in F_{p^n}}\omega^{r\mathrm{tr}_1^n(ay^{p+1}+y^2)}\Big|\leq(p-1)p^{\frac{n}{2}}. \tag{13}$$

$r=\alpha^{\frac{p^n-1}{p-1}}$은 F_{p^n}에서의 비제곱원이고 F_p의 원시 원소이다.

(13)에서의 첫 번째 항은 다음과 같다.

$$\sum_{y\in F_{p^n}}\omega^{\mathrm{tr}_1^n(ay^{p+1}-y^2)}=1+2\sum_{z\in C_0}\omega^{\mathrm{tr}_1^n(az^{\frac{p+1}{2}}-z)}$$

여기서 $z=y^2$ and $C_0=\{x^2|x\in F_{p^n}\}$.

-1은 F_{p^n} 상에서 비제곱원이고 $r^{\frac{p+1}{2}} = -r$이기 때문에 다음과 같이 쓸 수 있다.

$$\begin{aligned}\sum_{z\in C_0}\omega^{\mathrm{tr}_1^n(az^{\frac{p+1}{2}}-z)} &= \sum_{u\in C_1}\omega^{\mathrm{tr}_1^n\left(a(ru)^{\frac{p+1}{2}}-ru\right)}\\ &= \sum_{u\in C_1}\omega^{r\mathrm{tr}_1^n(-au^{\frac{p+1}{2}}-u)}\\ &= \sum_{v\in C_1}\omega^{r\mathrm{tr}_1^n(av^{\frac{p+1}{2}}+v)}\end{aligned}$$

여기서 $z = ru$이고 $v = -u$이다. 그러므로 (13)의 첫 번째 항을 다시 쓰면,

$$\sum_{y\in F_{p^n}}\omega^{\mathrm{tr}_1^n(ay^{p+1}-y^2)} = 1 + \sum_{z\in C_0}\omega^{\mathrm{tr}_1^n(az^{\frac{p+1}{2}}-z)} + \sum_{z\in C_1}\omega^{r\mathrm{tr}_1^n(az^{\frac{p+1}{2}}+z)}. \tag{14}$$

(13)의 두 번째 항을 다시 쓰면,

$$\sum_{y\in F_{p^n}}\omega^{r\cdot\mathrm{tr}_1^n(ay^{p+1}+y^2)} = 1 + 2\sum_{z\in C_0}\omega^{r\cdot\mathrm{tr}_1^n(az^{\frac{p+1}{2}}+z)}$$

여기서 $z = y^2$이다.

위 식의 두 번째 항은 다음과 같이 다시 쓸 수 있다.

$$\begin{aligned}\sum_{z\in C_0}\omega^{r\mathrm{tr}_1^n(az^{\frac{p+1}{2}}+z)} &= \sum_{u\in C_1}\omega^{r\mathrm{tr}_1^n\left(a(ru)^{\frac{p+1}{2}}+ru\right)}\\ &= \sum_{u\in C_1}\omega^{\mathrm{tr}_1^n(-ar^2u^{\frac{p+1}{2}}+r^2u)}\\ &= \sum_{u\in C_1}\omega^{\mathrm{tr}_1^n(-ar^{p+1}u^{\frac{p+1}{2}}+r^2u)}\\ &= \sum_{v\in C_1}\omega^{\mathrm{tr}_1^n(av^{\frac{p+1}{2}}-v)}\end{aligned}$$

여기서 $z = ru$이고 $v = -r^2u$이다. 그러므로 (13)의 두 번째 항을 다시 쓰면,

$$\sum_{y\in F_{p^n}}\omega^{r\mathrm{tr}_1^n(ay^{p+1}+y^2)} = 1 + \sum_{z\in C_0}\omega^{r\mathrm{tr}_1^n(az^{\frac{p+1}{2}}+z)} + \sum_{z\in C_1}\omega^{\mathrm{tr}_1^n(az^{\frac{p+1}{2}}-z)}. \tag{15}$$

(14)와 (15)로부터, $S(a)$는 다음과 같이 쓸 수 있다.

$$\begin{aligned}S(a) &= \sum_{y\in F_{p^n}}\omega^{\mathrm{tr}_1^n(ay^{p+1}-y^2)} + \sum_{y\in F_{p^n}}\omega^{r\mathrm{tr}_1^n(ay^{p+1}+y^2)}\\ &= 1 + \sum_{z\in C_0}\omega^{\mathrm{tr}_1^n(az^{\frac{p+1}{2}}-z)} + \sum_{z\in C_1}\omega^{r\mathrm{tr}_1^n(az^{\frac{p+1}{2}}+z)}\\ &\quad + 1 + \sum_{z\in C_0}\omega^{r\mathrm{tr}_1^n(az^{\frac{p+1}{2}}+z)} + \sum_{z\in C_1}\omega^{\mathrm{tr}_1^n(az^{\frac{p+1}{2}}-z)}\\ &= \sum_{z\in F_{p^n}}\omega^{\mathrm{tr}_1^n(az^{\frac{p+1}{2}}-z)} + \sum_{z\in F_{p^n}}\omega^{r\mathrm{tr}_1^n(az^{\frac{p+1}{2}}+z)}.\end{aligned} \tag{16}$$

정리 2로부터, (16)의 각 항의 크기는 다음과 같이 상한 된다.

$$\Big|\sum_{z\in F_{p^n}}\omega^{\mathrm{tr}_1^n(az^{\frac{p+1}{2}}-z)}\Big| \le \frac{p-1}{2}p^{\frac{n}{2}}$$

$$\Big|\sum_{z\in F_{p^n}}\omega^{r\mathrm{tr}_1^n(az^{\frac{p+1}{2}}+z)}\Big| \le \frac{p-1}{2}p^{\frac{n}{2}}.$$

그러므로 증명을 마칠 수 있다. ■

정리 3: p-진 m-수열 $m(t)$와 decimated 수열 $m(dt)$의 상관 함수의 값은 $\{-1, -1\pm p^{n/2}, -1+\frac{\pm\sqrt{p}\pm1}{2}p^{n/2}, -1+\frac{p-1}{2}p^{n/2}, -1+\frac{-p+1}{2}p^{n/2}\}$이다.

Proof: (4)로부터 상관 함수는 $S(a)$로 다음과 같이 표현할 수 있다.

$$C(\tau) = -1 + S(a) = -1 + \frac{1}{2}\Big(\sum_{y\in F_{p^n}}\omega^{g(y)} + \sum_{y\in F_{p^n}}\omega^{h(y)}\Big)$$

여기서 $g(y) = \mathrm{tr}_1^n(ay^{p+1}-y^2)$이고 $h(y) = r\mathrm{tr}_1^n(ay^{p+1}+y^2)$이다.

두 이차 형식의 rank에 따라서 다음과 같이 상관 함수 값을 구할 수 있다.

경우 1) $g(y)$의 rank$= n-2$이고 $h(y)$의 rank$= n$ (또는 $g(y)$의 rank$= n$이고 $h(y)$의 rank$= n-2$);

보조정리 2와 정리 1로부터,

$$\begin{aligned}2S(a) &= \sum_{y\in F_{p^n}}\omega^{g(y)} + \sum_{y\in F_{p^n}}\omega^{h(y)}\\ &= p^2\Big(p^{n-3} + \sum_{i=1}^{p-1}\big((p^{n-3}+\epsilon_g\eta(i)p^{\frac{n-3}{2}})\omega^i\big)\Big)\\ &\quad + \Big(p^{n-1} + \sum_{i=1}^{p-1}\big((p^{n-1}+\epsilon_h\eta(i)p^{\frac{n-1}{2}})\omega^i\big)\Big)\\ &= p^{\frac{n+1}{2}}\epsilon_g\sum_{i=1}^{p-1}\eta(i)\omega^i + p^{\frac{n-1}{2}}\epsilon_h\sum_{i=1}^{p-1}\eta(i)\omega^i\\ &= p^{\frac{n}{2}}(p\epsilon_g+\epsilon_h).\end{aligned}$$

그러므로,

$$C(\tau) = -1 + \frac{p\epsilon_g+\epsilon_h}{2}p^{\frac{n}{2}}.$$

ϵ_g와 ϵ_h는 ±1 값을 갖기 때문에, 위 식으로부터 가능한 상관 값은 4개이다. 그러나 $\epsilon_g = \epsilon_h$인 경우는 Lemma 5에 제시된 상관 값을 넘기 때문에 모순이다. 그러므로 이 경우에 상관 값은 다음과 같다.

$$\Big\{-1+\frac{p-1}{2}p^{n/2}, -1+\frac{-p+1}{2}p^{n/2}\Big\}.$$

경우 2) $g(y)$의 rank$= n-1$이고 $h(y)$의 rank$= n$ (또는 $g(y)$의 rank$= n$이고 $h(y)$의 rank$= n-1$);

같은 방식으로 계산하면 다음과 같다.

$$2S(a) = \sum_{y\in F_{p^n}}\omega^{g(y)} + \sum_{y\in F_{p^n}}\omega^{h(y)}$$

$$= p\Big(p^{n-2} + \epsilon_g(p-1)p^{\frac{n-3}{2}} + \sum_{i=1}^{p-1}\big((p^{n-2} - \epsilon_g p^{\frac{n-3}{2}})\omega^i\big)\Big) + p^{\frac{n}{2}}\epsilon_h$$
$$= p^{\frac{n}{2}}(\sqrt{p}\epsilon_g + \epsilon_h).$$

그러므로,

$$C(\tau) = -1 + \frac{\sqrt{p}\epsilon_g + \epsilon_h}{2}p^{\frac{n}{2}}.$$

이 경우에 상관 값은 다음과 같다.

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

경우 3) $g(y)$의 rank$= n$ and $h(y)$의 rank$= n$;

같은 방식으로 계산하면 다음과 같다.

$$C(\tau) = -1 + \frac{\epsilon_g + \epsilon_h}{2}p^{\frac{n}{2}}.$$

이 경우에 상관 값은 다음과 같다.

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

■

4. 감사의 글

본 연구는 방송통신위원회의 차세대통신네트워크 원천기술개발사업(KCA-2011-08913-04003)과 2011년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임 (No. 2011-0000328).

5. 참고문헌

[1] H. M. Trachtenberg, "On the cross-correlation functions of maximal recurring sequences,"*Ph.D. dissertation*, Univ. of Southern California, Los Angeles, CA, 1970.

[2] T. Helleseth, "Some results about the cross-correlation function between two maximal linear sequences,"*Discrete Math.*, vol. 16, pp. 209–232, 1976.

[3] 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.

[4] E. N. Müller, "On the cross-correlation of sequences over $GF(p)$ with short periods," *IEEE Trans. Inf. Theory*, vol. 45, no. 1, pp. 289–295, Jan. 1999.

[5] Z. Hu, X. Li, D. Mills, E. Müller, W. Sun, W. Williems, Y. Yang, and Z. Zhang, "On the cross-correlation of sequences with the decimation factor $d = \frac{p^n+1}{p+1} - \frac{p^n-1}{2}$," *Applicable Algebra in Engineering, Communication and Computing*, vol. 12, pp. 255-263, 2001.

[6] R. Lidl and H. Niederreiter, *Finite Fields*, vol. 20 of *Encyclopedia of Mathematics and Its Applications*. Reading, MA: Addison-Wesley, 1983.