주기 $3^{4k+2}-1$의 3-진 m-수열과 $\frac{(3^{2k+1}+1)^2}{8}$로 Decimation된 수열의 상관 함수의 상한 값 유도

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

The Upper Bound of the Cross-Correlation of a Ternary m-sequence of Period $3^{4k+2}-1$ and Its Decimated Sequence by $\frac{(3^{2k+1}+1)^2}{8}$

*Sung-Tai ChoiO, *Jong-Seon No, and **Habong Chung
*Department of EECS, INMC, Seoul National University
**School of Electronics and Electrical Engineering, Hongik University,
stchoi@ccl.snu.ac.kr, jsno@snu.ac.kr, habchung@hongik.ac.kr

요약

본 논문에서는 주기 3^n-1인 3-진 m-수열 $m(t)$와 $d=\frac{(3^m+1)^2}{8}$로 decimation된 수열 $m(dt)$의 상호 상관 값을 유도한다. 여기서 $n=2m=4k+2$이다. 상호 상관 값 크기가 $2\sqrt{3^n}+1$로 상한 됨을 보인다.

1. 개요

p-진 m-수열 $s(t)$와 decimation된 수열 $s(dt)$의 상호 상관 값이 작은 d를 찾는 많은 연구가 진행되어 왔다. $\gcd(d,p^n-1)=1$을 만족하는 d 값은 Trachtenberg [1], Helleseth [2], 그리고 Dobbertin, Helleseth, Kumar, Martinsen [3]에 의해서 연구되었다.

Decimation 값 d가 p^n-1과 서로소가 아닌 경우에는 $s(dt)$는 $\frac{p^n-1}{\gcd(d,p^n-1)}$의 주기를 갖으며 두 수열간에 상호 상관 값에 대한 연구가 진행되어 왔다. 3-진 경우에 대해서 Ness, Helleseth, 그리고 Kholosha [4]는 $d=\frac{3^k+1}{2}$, $\gcd(k,n)=1$, 그리고 k는 홀수인 경우에 대해서 상호 상관 값의 분포를 유도하였다. 이 경우의 decimation 값은 Coulter-Matthews decimation로 잘 알려져 있다.

Muller [5]는 $d=\frac{3^n+1}{4}+\frac{3^n-1}{2}$ 이고 n은 홀수인 경우에 대해서 상호 상관 값의 크기가 $2\sqrt{3^n}+1$로 상한 됨을 보였다. Hu [6] 등은 Muller의 경우를 모든 홀수의 소수의 경우로 확장하여 $d=\frac{p^n+1}{p+1}+\frac{p^n-1}{2}$에 대해서 상호 상관 값의 크기가 $\frac{p+1}{2}\sqrt{p^n}$로 상한됨을 유도하였다. Seo, Kim, No, 그리고 Shin [7]는 $d=\frac{(p^{2k}+1)^2}{4}$, p는 홀수의 소수, 그리고 $n=4k$인 경우에 대해서 상호 상관 값의 분포를 구하였다.

2. 사전 지식

p는 홀수인 소수이고 F_{p^n}는 p^n개의 원소를 갖는 유한체이다. 유한체 F_{p^n}에서 유한체 F_{p^s}로 가는 trace 함수 $\mathrm{tr}_s^n(\cdot)$는 다음과 같이 정의된다.

$$\mathrm{tr}_s^n(x)=\sum_{i=0}^{\frac{n}{s}-1}x^{p^{si}}$$

여기서 $x\in F_{p^n}$이고 $s|n$이다. α는 F_{p^n} 상에서 원시근이라고 놓으면 주기 p^n-1의 p-진 m-수열 $s(t)$는 다음과 같이 표현할 수 있다.

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

본 논문에서 앞으로 쓰이게 될 기호들을 다음과 같이 정의한다.

- $n=2m$, m은 홀수;
- $d=\frac{(3^m+1)^2}{8}$;
- α는 F_{3^n}의 원시원;
- ω는 3차 복소근.

3. 상호 상관 함수의 이차 형식으로의 표현

두 수열 $s(t)$와 $s(dt)$의 상호 상관 값은 다음과 같이 정의된다.

$$C_d(\tau) = \sum_{t=0}^{3^n-2} \omega^{\mathrm{tr}_1^n(\alpha^{t+\tau}-\alpha^{dt})} = \sum_{x\in F_{3^n}^*} \omega^{\mathrm{tr}_1^n(ax-x^d)} \quad (1)$$

여기서 $x=\alpha^t$ 이고 $a=\alpha^\tau$이다.

함수 $C(a)$를 다음과 같이 정의한다.

$$C(a) = \sum_{x\in F_{3^n}} \omega^{\mathrm{tr}_1^n(ax-x^d)}. \quad (2)$$

그러면 상관 함수는 $C_d(\tau)=C(a)-1$로 표현된다.

$F_{3^n}^*$의 절반은 제곱원들이고 나머지 절반은 비제곱원들인 것은 자명하다. $\gcd(3^{m+1}+1, 3^n-1)=2$이기 때문에 제곱원들은 $x=y^{3^{m+1}+1}$와 같이 표현할 수 있고 비제곱원들은 $x=ry^{3^{m+1}+1}$와 같이 표현할 수 있다. 여기서 $y\in F_{3^n}^*$ 이고 r은 $F_{3^n}^*$상에서 임의의 비제곱원이다. 또한 y가 $F_{3^n}^*$ 상에서 변함에 따라서 $x\in F_{3^n}^*$는 두 번씩 발생한다. 그러므로 $C(a)$는 다음과 같이 표현할 수 있다.

$$\begin{aligned} 2C(a) = &\sum_{y\in F_{3^n}} \omega^{\mathrm{tr}_1^n(ay^{3^{m+1}+1}-y^{d(3^{m+1}+1)})} \\ &+ \sum_{y\in F_{3^n}} \omega^{\mathrm{tr}_1^n(ary^{3^{m+1}+1}-r^dy^{d(3^{m+1}+1)})}. \end{aligned}$$

$(3^{m+1}+1)d \equiv 3^m+1 \bmod 3^n-1$이므로,

$$\begin{aligned} 2C(a) = &\sum_{y\in F_{3^n}} \omega^{\mathrm{tr}_1^n(ay^{3^{m+1}+1}-y^{3^m+1})} \\ &+ \sum_{y\in F_{3^n}} \omega^{\mathrm{tr}_1^n(ary^{3^{m+1}+1}-r^dy^{3^m+1})}. \end{aligned} \quad (3)$$

함수 $g(y)$, $h(y)$를 다음과 같이 정의한다.

$$\begin{aligned} g(y) &= \mathrm{tr}_1^n(ay^{3^{m+1}+1}-y^{3^m+1}) \\ h(y) &= \mathrm{tr}_1^n(ary^{3^{m+1}+1}-r^dy^{3^m+1}). \end{aligned}$$

만약 y가 F_3 상에서 F_{3^n}의 기저 $\{\alpha_1,\alpha_2,\cdots,\alpha_n\}$에 의해 $y=\sum_{i=1}^n y_i\alpha_i$, $y_i\in F_3$로 표현되면, $g(y)$와 $h(y)$가 이차 형식으로 표현되는 것은 다음과 같이 확인할 수 있다.

$$\begin{aligned} &g(y) \\ =&\mathrm{tr}_1^n\Big(a(\sum_{i=1}^n y_i\alpha_i^{3^{m+1}})(\sum_{i=1}^n y_i\alpha_i) - (\sum_{i=1}^n y_i\alpha_i^{3^m})(\sum_{i=1}^n y_i\alpha_i)\Big) \\ =&\mathrm{tr}_1^n\Big(a\sum_{i=1}^n\sum_{j=1}^n (y_iy_j)(\alpha_i^{3^{m+1}}\alpha_j) - \sum_{i=1}^n\sum_{j=1}^n (y_iy_j)(\alpha_i^{3^m}\alpha_j)\Big) \\ =&\sum_{i=1}^n\sum_{j=1}^n (y_iy_j)\mathrm{tr}_1^n\Big(a(\alpha_i^{3^{m+1}}\alpha_j) - (\alpha_i^{3^m}\alpha_j)\Big) \\ =&\sum_{i=1}^n\sum_{j=1}^n (y_iy_j)a_{ij} \end{aligned}$$

여기서 $a_{ij}=\mathrm{tr}_1^n\Big(a(\alpha_i^{3^{m+1}}\alpha_j)-(\alpha_i^{3^m}\alpha_j)\Big)$이다. $h(y)$의 경우는 위의 과정에서 a가 ar로 바뀐 형태이므로 위와 비슷하게 확인할 수 있다.

모든 이차 형식은 표준 형태로 가역 변환에 의해서 변환 가능하다. 그리고 임의의 $c\in F_p$에 대해서 이차식 $f(x)=c$를 만족하는 해 $x\in F_{p^n}$의 개수는 이차 형식 $f(x)$의 rank를 구함으로써 결정할 수 있다. 이차 형식 $f(x)$의 rank ρ는 함수의 독립적인 coordinates의 개수를 찾아서 결정할 수 있다. 다시 말해서, 이차 형식 $g(x)$의 경우, 모든 $y\in F_{p^n}$에 대해서 $g(y+z)=g(y)$를 만족하는 해 $z\in F_{p^n}$의 개수는 $p^{n-\rho}$과 같다. 이 내용은 다음 사전정리를 통해서 기술된다.

사전정리 1: [5]

$$f\in F_p[x_1,\cdots,x_n]$$

를 이차 형식으로 놓자. 또한

$$Y := \{\mathbf{y}\in(F_p)^n : f(\mathbf{x}+\mathbf{y})-f(\mathbf{x})=0 \text{ for all } \mathbf{x}\in(F_p)^n\}.$$

라 정의한다. 그러면 Y는 $(F_p)^n$의 부분집합이고 $\mathrm{rank}(f)=n-\dim(Y)$이다.

□

$C(a)$의 값을 유도하기 위해서 이차 형식 $g(y)$와 $h(y)$의 rank를 구해야 한다. 다시 말해서, 모든 $y\in F_{3^n}$에 대해서 이차식 $g(y+z)=g(y)$와 $h(y+z)=h(y)$를 만족하는 해 $z\in F_{3^n}$의 개수를 찾아야 한다. 해의 개수를 구하는 문제는 다음 사전정리를 통해서 단순화시킬 수 있다.

사전정리 2: 모든 $y\in F_{3^n}$에 대해서 $g(y+z)=g(y)$를 만족하는 $z\in F_{3^n}$의 개수는 다음 방정식을 만족하는 $z\in F_{3^n}$의 개수와 같다.

$$a^{3^{m+1}}z^{3^2}+z^3+az=0 \quad (4)$$

모든 $y\in F_{3^n}$에 대해서 $h(y+z)=h(y)$를 만족하는 $z\in F_{3^n}$의 개수는 다음 방정식을 만족하는 $z\in F_{3^n}$의 개수와 같다.

$$(ar)^{3^{m+1}}z^{3^2}-(r^{3d}+r^{d3^{m+1}})z^3+az=0 \quad (5)$$

여기서 r은 $F_{3^n}^*$에서의 비제곱원이다.

증명: 방정식 $g(y+z)=g(y)$은 다음과 같이 쓸 수 있다.

$$\mathrm{tr}_1^n(a(y+z)^{3^{m+1}+1}-(y+z)^{3^m+1}) = \mathrm{tr}_1^n(ay^{3^{m+1}+1}-y^{3^m+1}). \quad (6)$$

(6)은 다음과 같이 다시 쓸 수 있다.

$$\mathrm{tr}_1^n(y^{3^{m+1}}(a^{3^{m+1}}z^{3^2}+z^3+az)+az^{3^{m+1}}-z^{3^m+1})=0. \quad (7)$$

식 (7)이 모든 $y\in F_{3^n}$에 대해서 성립하는 것과 다음 식들이 동시에 성립하는 것은 필요충분조건이다.

$$a^{3^{m+1}}z^{3^2}+z^3+az = 0 \quad (8)$$
$$\mathrm{tr}_1^n(az^{3^{m+1}}-z^{3^m+1}) = 0 \quad (9)$$

그러므로 (6)을 만족하는 해 $z \in F_{3^n}$의 개수는 (8)과 (9)을 동시에 만족하는 해 $z \in F_{3^n}$의 개수를 구함으로써 결정할 수 있다.

지금부터, (8)을 만족하는 해 $z \in F_{p^n}$는 (9) 또한 만족하는 것을 보일 것이다. 식 (8)로부터,

$$-z^3 = a^{3^{m+1}}z^{3^2}+az$$

를 얻을 수 있고 양변에 3^{i-1}승을 해주면 다음을 얻을 수 있다.

$$-z^{3^i} = a^{3^{m+i}}z^{3^{i+1}}+a^{3^{i-1}}z^{3^{i-1}}. \quad (10)$$

식 (10)을 대입해서, (9)는 다음과 같이 다시 쓸 수 있다.

$$\begin{aligned}
&\mathrm{tr}_1^n(az^{3^{m+1}+1}-z^{3^m+1})\\
&=\sum_{i=1}^{n}a^{3^i}(z^{3^{m+1}+1})^{3^i}-\sum_{i=1}^{n}(z^{3^m+1})^{3^i}\\
&=\sum_{i=1}^{n}a^{3^i}(z^{3^{m+i+1}+3^i})-\sum_{i=1}^{n}(z^{3^{m+i}+3^i})\\
&=\sum_{i=1}^{n}a^{3^i}(z^{3^{m+i+1}+3^i})+\sum_{i=1}^{n}(-z^{3^i}z^{3^{m+i}})\\
&=\sum_{i=1}^{n}a^{3^i}(z^{3^{m+i+1}+3^i})\\
&\quad+\sum_{i=1}^{n}((a^{3^{m+i}}z^{3^{i+1}}+a^{3^{i-1}}z^{3^{i-1}})z^{3^{m+i}})\\
&=\sum_{i=1}^{n}a^{3^i}(z^{3^{m+i+1}+3^i})\\
&\quad+\sum_{i=1}^{n}((a^{3^{m+i}}z^{3^{i+1}+3^{m+i}}+a^{3^{i-1}}z^{3^{i-1}+3^{m+i}}))\\
&=3\sum_{i=1}^{n}a^{3^i}(z^{3^{m+i+1}+3^i})=0.
\end{aligned}$$

따라서 (7)의 해의 집합은 (8)의 해의 집합과 동일함을 증명할 수 있다.

$h(y)$의 경우도 위의 경우와 비슷하게 증명할 수 있다. □

사전정리 2로부터 $g(y)$와 $h(y)$의 rank를 결정하기 위해서 (4)와 (5)을 만족하는 해 $z \in F_{3^n}$의 개수를 구해야 함을 알 수 있다. 두 방정식의 차수가 모두 9이고 모두 선형화된 식의 형태이기 때문에, F_{3^n} 안에서 가능한 해의 개수는 두식 모두 $1, 3$, 또는 9개이다.

다음 사전정리를 통해서 $h(y)$는 F_{3^n}상에서 $z = 0$을 유일한 해로 갖음을 보일 것이다.

사전정리 3: 방정식

$$(ar)^{3^{m+1}}z^9-(r^{3d}+r^{d3^{m+1}})z^3+az = 0 \quad (11)$$

는 $z = 0$을 F_{3^n}상에서 유일한 해로 갖는다. 여기서 r은 $F_{3^n}^*$에서 비제곱원이다.

증명: 먼저,

$$r^{3d}+r^{d3^{m+1}} = 0 \quad (12)$$

이 $F_{3^n}^*$에서 모든 비제곱원 r에 대해서 성립함을 보일 것이다. 식 (12)는 다음과 같이 쓸 수 있다.

$$r^{3d}(1+r^{3d(3^m-1)}) = 0.$$

따라서,

$$r^{3d(3^m-1)} = -1. \quad (13)$$

이로부터,

$$3d(3^m-1) = \frac{3(3^m+1)(3^{2m}-1)}{8},$$

이고 $3^m+1 \equiv 4 \mod 8$이기 때문에, 모든 비제곱원 r은 (13)을 만족함을 알 수 있다.

$r^{3d}+r^{d3^{m+1}} = 0$로부터, (11)는 다음과 같이 쓸 수 있다.

$$arz\Big((ar)^{3^{m+1}-1}z^8+1\Big) = 0.$$

$8|3^{m+1}-1$이므로, 어떤 $u \in F_{3^n}$에 대해서 $(ar)^{3^{m+1}-1}z^8 = u^8$이다. 그러나 F_{3^n}에는 16차 복소근이 존재하지 않는다. 따라서 $u^8 \neq -1$이므로 (11)의 유일한 해는 $z = 0$이다. □

위의 사전정리로부터, $g(y)$의 가능한 rank는 n, $n-1$, 또는 $n-2$이고 $h(y)$의 가능한 rank는 n뿐임을 알 수 있다.

4. 상관함수 값의 상한 값

이번 장에서는, 3-진 m-수열 $m(t)$와 그의 decimated 수열 $m(dt)$의 상관 함수 $C_d(\tau)$ 값의 크기에 대한 상한 값을 유도할 것이다.

먼저, F_{p^n}상에서 이차 character를 다음과 같이 정의한다.

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

본 논문의 상관함수의 상한 값에 대한 정리를 증명하기 위해 다음의 사전정리들을 사용할 것이다.

사전정리 4: [8] η는 F_p에서 이차 character라 놓자. $f(x)$가 t개의 변수를 갖고 Δ의 행렬식을 갖는 이차 형식일 때, $f(y) = c$를 만족하는 해의 개수 $N(c)$는 다음과 같이 정해진다.

경우 1) t는 짝수;

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

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

경우 2) t는 홀수;

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

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

□

$p = 3$이기 때문에 사전정리 4로부터 다음의 사전정리를 쉽게 유도할 수 있다. 다음 사전정리의 결과는 상관함수의 값을 유도하는데 쓰일 것이다.

사전정리 5: [4] η를 F_3에서 이차 character라 놓자. (다시 말해서, $\eta(0) = 0$, $\eta(1) = 1$, 이고 $\eta(2) = -1$). $f(x)$를 t개의 변수를 갖고 Δ를 행렬식으로 갖는 nondegenerate 이차 형식이라 놓으면,

$$S = \sum_{x \in F_{3^n}} \omega^{f(x)}$$

은 다음과 같이 결정된다.

$$S = \begin{cases} \epsilon 3^{t/2}, & \text{if } t \text{ is even} \\ \epsilon i 3^{t/2}, & \text{if } t \text{ is odd} \end{cases}$$

여기서 t가 짝수인 경우는 $\epsilon = \eta((-1)^{t/2}\Delta)$, 홀수인 경우는 $\epsilon = \eta((-1)^{(t-1)/2}\Delta)$이다.

□

사전정리 5를 사용해서, (1)의 상관 함수 $C_d(\tau)$의 크기에 대한 상한 값을 다음 정리에서 유도할 것이다.

정리 1: $n = 2m$이고 $d = \frac{(3^m+1)^2}{8}$라 놓자. 여기서 m은 홀수이다. 그러면 (1)의 $C_d(\tau)$의 크기는 다음과 같이 상한된다.

$$|C_d(\tau)| \leq 2 \cdot 3^{\frac{n}{2}} + 1.$$

증명: 먼저, $C(a)$의 크기의 상한 값을 유도할 것이다. (3)는 $g(y)$와 $h(y)$를 사용하여 다음과 같이 쓸 수 있다.

$$2C(a) = \sum_{y \in F_{3^n}} \omega^{g(y)} + \sum_{y \in F_{3^n}} \omega^{h(y)}$$

여기서 $g(y) = \text{tr}_1^n(ay^{3^{m+1}+1} - y^{3^m+1})$와 $h(y) = \text{tr}_1^n(ary^{3^{m+1}+1} - r^d y^{3^m+1})$은 모두 이차 형식을 갖고 r $F_{3^n}^*$에서 비제곱원이다. ϵ_g과 ϵ_h은 사전정리 5에 정의된 값이고 각각 이차 형식 $g(y)$와 $h(y)$에 대응한다. 이차 형식의 rank가 n보다 작으면, 대응하는 지수 합은 $3^{n-\rho}$를 곱해줘서 계산해야 한다.

사전정리 2로부터 이차 형식 $g(y)$와 $h(y)$의 가능한 rank 조합은 (n, n), $(n-1, n)$, 그리고 $(n-2, n)$임을 알 수 있다. 그러므로 $C(a)$의 값을 결정하기 위해서 다음의 세가지 경우만 고려하면 될 것이다.

경우 1) Rank of $g(y) = n$이고 rank of $h(y) = n$;
사전정리 5로부터,

$$\begin{aligned} 2C(a) &= \textstyle\sum_{y \in F_{3^n}} \omega^{g(y)} + \sum_{y \in F_{3^n}} \omega^{h(y)} \\ &= (\epsilon_g + \epsilon_h) 3^{\frac{n}{2}}. \end{aligned}$$

위로부터, $|C_d(\tau)| = |-1 + C(a)| \leq 3^{\frac{n}{2}} + 1$.

경우 2) Rank of $g(y) = n-1$이고 rank of $h(y) = n$;
사전정리 5로부터,

$$\begin{aligned} 2C(a) &= \textstyle\sum_{y \in F_{3^n}} \omega^{g(y)} + \sum_{y \in F_{3^n}} \omega^{h(y)} \\ &= (\sqrt{3}i\epsilon_g + \epsilon_h) 3^{\frac{n}{2}}. \end{aligned}$$

위로부터, $|C_d(\tau)| = |-1 + C(a)| \leq 3^{\frac{n}{2}} + 1$.

경우 3) Rank of $g(y) = n-2$이고 rank of $h(y) = n$;
사전정리 5로부터,

$$\begin{aligned} 2C(a) &= \textstyle\sum_{y \in F_{3^n}} \omega^{g(y)} + \sum_{y \in F_{3^n}} \omega^{h(y)} \\ &= (3\epsilon_g + \epsilon_h) 3^{\frac{n}{2}}. \end{aligned}$$

위로부터, $|C_d(\tau)| = |-1 + C(a)| \leq 2 \cdot 3^{\frac{n}{2}} + 1$.
따라서 $C_d(\tau)$의 크기는 $2 \cdot 3^{\frac{n}{2}} + 1$로 상한된다.

□

5. 감사의 글

본 연구는 지식경제부 및 한국산업기술평가관리원의 IT산업원천기술개발사업[2008-F-007-02, 3차원 환경에서의 지능형 무선 통신 시스템]과 2009년도 정부(교육과학기술부)의 재원으로 한국과학재단의 지원을 받아 수행된 연구임(No. 2009-0081441)."

6. 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] 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.

[5] 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.

[6] Z. Hu, X. Li, D. Mills, E. Muller, 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.

[7] Eun-Young Seo, Young-Sik Kim, Jong-Seon No, and Dong-Joon Shin,"Cross-correlation distribution of p-ary m-sequence of period p^{4k}??1 and its decimated sequences by $(\frac{p^{2k}+1}{2})^2$," *IEEE Transactions on Information Theory*, vol. 54, no. 7, pp. 3140-3149, Jul. 2008.

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