Some results on cross-correlation distribution between a p-ary m-sequence and its decimated sequences

Yongbo Xia

A joint work with Chunlei Li, Xiangyong Zeng, and Tor Helleseth

Selmer Center, University of Bergen

Sept. 5, 2014

Outline

Outline

Outline

1. Background and preliminaries
2. The exponential sum $S_d(u,v)$
3. Cross-correlation distribution

Outline

Notation

- p: an odd prime.
- m: a positive integer.
- $\mathbb{F}_{p^m}$: the finite field with p^m elements.
- α: a primitive element of $\mathbb{F}_{p^m}$.
- $\{s(t)\}_{t=0}^{p^m-2}$: a p-ary m-sequence of period $p^m - 1$.

The d-decimations of $\{s(t)\}$

- Trace representation (after suitable cyclic shift): $s(t) = \mathrm{Tr}_1^m(\alpha^t)$.
- The decimation exponent d.
- The l-th d-decimated sequence $\{s(dt+l)\}$ of $\{s(t)\}$:

$$s(dt+l) = \mathrm{Tr}_1^m(\alpha^{dt+l}),\ 0 \le l < \gcd(d, p^m - 1).$$

- $\{s(dt+l)\}$ has period $\frac{p^m-1}{\gcd(d,p^m-1)}$.

Cross-correlation function $C_{d,l}(\tau)$

- The cross-correlation function of $\{s(t)\}$ and $\{s(dt + l)\}$:

$$C_{d,l}(\tau) = \sum_{t=0}^{p^m-2} \omega_p^{\mathrm{Tr}_1^m(\alpha^t) - \mathrm{Tr}_1^m(\alpha^{d(t+\tau)+l})}.$$

- To determine $C_{d,l}(\tau)$, it suffices to investigate

$$C_d(\gamma) = \sum_{x \in \mathbb{F}_{p^m}} \omega_p^{\mathrm{Tr}_1^m(x+\gamma x^d)} - 1, \ \gamma \in \mathbb{F}_{p^m}^*. \qquad (1.1)$$

Cross-correlation distribution

Two important problems in sequence design.

- Find new decimation exponents d such that $\max_{\gamma \in \mathbb{F}_{p^m}^*} |C_d(\gamma)|$ is low.
- Determine the cross-correlation distribution, i.e., the multiset

$$\left\{ C_d(\gamma) \,|\, \gamma \in \mathbb{F}_{p^m}^* \right\}.$$

Exponential sums related to $C_d(\gamma)$

- Define

$$S_d(u,v) = \sum_{x\in\mathbb{F}_{p^m}} \omega_p^{\mathrm{Tr}_1^m\left(ux+vx^d\right)}. \tag{1.2}$$

- Then,

$$S_d(1,\gamma) = C_d(\gamma) + 1.$$

Some known results $(1/4)$

- odd prime p, $e = \gcd(k,m)$, $\frac{m}{e} \geq 3$ odd, $d = \frac{p^{2k}+1}{2}$ or $\frac{p^{3k}+1}{p^k+1}$, 3-valued, $p^{\frac{m+e}{2}} + 1$.
- $p^{\frac{m}{2}} \not\equiv 2 \pmod 3$, m even, $d = 2p^{\frac{m}{2}} - 1$, 4-valued, $2p^{\frac{m}{2}} - 1$.

T. Helleseth, "Some results about the cross-correlation function between two maximal linear sequences," *Discr. Math.*, 16: 209-232 (1976)

Some known results $(2/4)$

- $p=3$, m odd, $d=2\cdot 3^{\frac{m-1}{2}}+1$, 3-valued, $3^{\frac{m+1}{2}}+1$
- $p=3$, $m=3r$ $(r\geq 2)$, $d=3^r+2$ or $3^{2r}+2$, 4 or 6-valued, $3^{2r}-1$.

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*, 47(4): 1473-1481 (2001)

T. Zhang, S. Li, T. Feng and G. Ge, "Some new results on the cross correlation of m-sequences," *IEEE Trans. Inf. Theory*, 60(5): 3062-3068 (2014).

Y. Xia, T. Helleseth and G. Wu, "A note on cross-correlation distribution between a ternary m-sequence and its decimated sequence," to appear in SETA2014.

Some known results $(3/4)$

- odd prime p, $e=\gcd(k,m)$, $\frac{m}{e}\geq 2$, $d=\frac{p^k+1}{2}$, $\frac{k}{e}$ odd , 9-valued, $\frac{p^e-1}{2}p^{\frac{m}{2}}+1$.
- odd prime p, $m=4k$, $d=(\frac{p^{2k}+1}{2})^2$, 4-valued, $2p^{\frac{m}{2}}-1$.

J. Luo and K. Feng, "Cyclic codes and sequence from generalized Coulter-Matthews functions," *IEEE Trans. Inf. Theory*, 54(12): 5345-5353 (2008)

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 $(\frac{p^{2k}+1}{2})^2$," *IEEE Trans. Inf. Theory*, 54(7): 3140-3149 (2008)

Some known results $(4/4)$

- $p \equiv 3 \pmod 4$, m odd, $e \mid m$, $\frac{m}{e} \geq 3$, $d = \frac{p^m+1}{p^e+1} \pm \frac{p^m-1}{2}$, $\gcd(d, p^m-1) = 2$, 9-valued, $\frac{p^e+1}{2} p^{\frac{m}{2}} + 1$.

E. N. Müller, "On the crosscorrelation of sequences over $\mathrm{GF}(p)$ with short periods," *IEEE Trans. Inf. Theory*, 45(1): 289-295 (1999)

Z. Hu, X. Li, D. Mills, E. N. Müller, W. Sun, W. Willems, Y. Yang and Z. Zhang, "On the crosscorrelation of sequences with the decimation factor $d = \frac{p^n+1}{p+1} - \frac{p^n-1}{2}$," *Appl. Algebra Eng. Commun. Comput.*, 12(3): 255-263 (2001)

Y. Xia, X. Zeng and L. Hu, "Further crosscorrelation properties of sequences with the decimation factor $d = \frac{p^n+1}{p+1} - \frac{p^n-1}{2}$," *Appl. Algebra Eng. Commun. Comput.*, 21(5): 329-342 (2010)

S. T. Choi, J. Y. Kim, and J. S. No, "On the cross-correlation of a p-ary m-sequence and its decimated sequences by $d = \frac{p^n+1}{p^k+1} + \frac{p^n-1}{2}$," *IEICE Trans. Commun.*, vol. E96-B(9): 2190-2197 (2013)

The topic of this talk

- An odd prime p and two positive integers m, k:

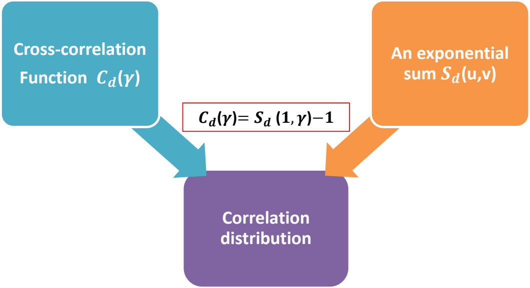
$$\frac{m}{\gcd(k,m)} \text{ is odd and } \frac{m}{\gcd(k,m)} > 1; \qquad (1.3)$$

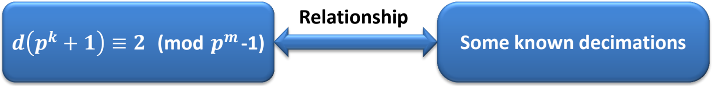
a decimation d:

$$d\left(p^k+1\right) \equiv 2 \pmod{p^m-1}. \qquad (1.4)$$

- The purpose is to determine the cross-correlation distribution for every decimation d satisfying Eq. (1.4).

$$d(p^k+1) \equiv 2 \pmod{p^m-1}$$





Some auxiliary results $(1/4)$

Lemma 1

For p, m and k satisfying (1.3), there are two distinct integers d_1, d_2 satisfying $d\left(p^k+1\right) \equiv 2 \pmod{p^m-1}$ in $\mathbb{Z}_{p^m-1}$. Then

(i) $d_1 \equiv 1 \pmod{p^e-1}$, and $d_2 \equiv 1 + \frac{p^e-1}{2} \pmod{p^e-1}$;

(ii) $\gcd(d_1, p^m-1) = 1$, and

$$\gcd(d_2, p^m-1) = \begin{cases} 1, & \text{if } p^e \equiv 1 \pmod 4, \\ 2, & \text{if } p^e \equiv 3 \pmod 4. \end{cases}$$

Some auxiliary results $(2/4)$

Let m, k be two positive integers satisfying (1.3). Define

$$Q_{u,v}(x) = \mathrm{Tr}_e^m\left(ux^{p^k+1} + vx^2\right), \ u, v \in \mathbb{F}_{p^m}. \qquad (1.5)$$

J. Luo and K. Feng, "On the weight distribution of two classes of cyclic codes," *IEEE Trans. Inf. Theory*, 54(12): 5332-5344 (2008)

J. Luo and K. Feng, "Cyclic codes and sequence from generalized Coulter-Matthews functions," *IEEE Trans. Inf. Theory*, 54(12): 5345-5353 (2008)

S. T. Choi, J. Y. Kim, and J. S. No, "On the cross-correlation of a p-ary m-sequence and its decimated sequences by $d = \frac{p^n+1}{p^k+1} + \frac{p^n-1}{2}$," *IEICE Trans. Commun.*, vol. E96-B(9): 2190-2197 (2013)

Z. Zhou and C. Ding, "A class of three-weight cyclic codes," *Finite Fields Appl.*, 25: 79-93 (2014)

Some auxiliary results $(3/4)$

Lemma 2 (Luo and Feng, 2008; Choi et. al., 2013; Zhou and Ding, 2014)

Let $Q_{u,v}(x)$ be the quadratic form defined by (1.5), $(u,v) \in \mathbb{F}_{p^m}^2 \setminus \{(0,0)\}$ and $s = \frac{m}{e}$.

(i) The rank of $Q_{u,v}(x)$ is s, $s-1$ or $s-2$. Especially, both $Q_{u,0}(x)$ with $u \in \mathbb{F}_{p^m}^*$ and $Q_{0,v}(x)$ with $v \in \mathbb{F}_{p^m}^*$ have rank s.

(ii) For any given $(u,v) \in \mathbb{F}_{p^m}^2 \setminus \{(0,0)\}$, at least one of $Q_{u,v}(x)$ and $Q_{u,-v}(x)$ has rank s.

Some auxiliary results $(4/4)$

Lemma 3 (Luo and Feng, 2008)

$$T(u,v) = \sum_{x\in\mathbb{F}_{p^m}} \omega_p^{\mathrm{Tr}_1^e(Q_{u,v}(x))} \tag{1.6}$$

Table 1: Value distribution for $T(u,v)$

Value	Frequency (each)
p^m	1
$\pm\epsilon p^{\frac{m}{2}}$	$\frac{(p^m-1)p^{2e}(p^m-p^{m-e}-p^{m-2e}+1)}{2(p^{2e}-1)}$
$p^{\frac{m+e}{2}}$	$\frac{(p^m-1)(p^{m-e}+p^{\frac{m-e}{2}})}{2}$
$-p^{\frac{m+e}{2}}$	$\frac{(p^m-1)(p^{m-e}-p^{\frac{m-e}{2}})}{2}$
$\pm\epsilon p^{\frac{m+2e}{2}}$	$\frac{(p^m-1)(p^{m-e}-1)}{2(p^{2e}-1)}$

The Exponential sum $S_d(u,v)$

- d: $d\left(p^k+1\right) \equiv 2 \pmod{p^m-1}$.
- θ: a fixed nonsquare in $\mathbb{F}_{p^e}$.
- $\mathcal{S} = \left\{x^{p^k+1} : x \in \mathbb{F}_{p^m}^*\right\} = \left\{x^2 : x \in \mathbb{F}_{p^m}^*\right\}$. Then, $\mathbb{F}_{p^m}^* = \mathcal{S} \bigcup \theta\mathcal{S}$.

Then

$$\begin{aligned} & S_d(u,v) \\ = & \sum_{x\in\mathbb{F}_{p^m}} \omega_p^{\mathrm{Tr}_1^m\left(ux+vx^d\right)} \\ = & \frac{1}{2}\sum_{x\in\mathbb{F}_{p^m}} \left(\omega_p^{\mathrm{Tr}_1^m\left(ux^{p^k+1}+vx^2\right)} + \omega_p^{\mathrm{Tr}_1^m\left(u\theta x^{p^k+1}+v\theta^d x^2\right)}\right). \end{aligned}$$

A relation between $S_d(u,v)$ and $T(u,v)$

- If d satisfies $d \equiv 1 \pmod{p^e - 1}$, i.e., $\theta^d = \theta$,

$$\begin{aligned} & S_d(u,v) \\ = \ & \frac{1}{2} \sum_{x \in \mathbb{F}_{p^m}} \left(\omega_p^{\mathrm{Tr}_1^e(Q_{u,v}(x))} + \omega_p^{\mathrm{Tr}_1^e(\theta Q_{u,v}(x))} \right) \\ = \ & \frac{1}{2} \left(T(u,v) + T(u\theta, v\theta) \right). \end{aligned} \tag{2.1}$$

- If d satisfies $d \equiv 1 + \frac{p^e-1}{2} \pmod{p^e - 1}$, i.e., $\theta^d = -\theta$,

$$\begin{aligned} & S_d(u,v) \\ = \ & \frac{1}{2} \sum_{x \in \mathbb{F}_{p^m}} \left(\omega_p^{\mathrm{Tr}_1^e(Q_{u,v}(x))} + \omega_p^{\mathrm{Tr}_1^e(\theta Q_{u,-v}(x))} \right) \\ = \ & \frac{1}{2} \left(T(u,v) + T(u\theta, -v\theta) \right). \end{aligned} \tag{2.2}$$

The definition of $\widehat{T}(u, v)$

- Define

$$\widehat{T}(u, v) = (T(u, v), T(u\theta, -v\theta)) \tag{2.3}$$

- Denote $c_i = \begin{cases} \epsilon p^{\frac{m+ie}{2}}, & i = 0, 2, \\ p^{\frac{m+ie}{2}}, & i = 1, \end{cases}$ where $\epsilon = \sqrt{\eta_e(-1)}$.
- $T(u, v), T(u\theta, -v\theta) \in \{\varepsilon c_i \mid \varepsilon = \pm 1, i = 0, 1, 2\}$.
- $\widehat{T}(u, v) \in \{(\varepsilon_1 c_{i_1}, \varepsilon_2 c_{i_2}) \mid \varepsilon_1, \varepsilon_2 \in \{\pm 1\}, i_1, i_2 \in \{0, 1, 2\}\}$. (36 possible values!)

A characterization of $\widehat{T}(u, v)$

- Define two sets

$$N_{\varepsilon,i} = \left\{(u, v) \in \mathbb{F}_{p^m}^2 \,|\, T(u, v) = \varepsilon c_i\right\},$$
$$M_{\varepsilon,i} = \left\{(u, v) \in \mathbb{F}_{p^m}^2 \,|\, T(u\theta, -v\theta) = \varepsilon c_i\right\}, \tag{2.4}$$

where $\varepsilon \in \{\pm 1\}$ and $i \in \{0, 1, 2\}$.

- Then,

$$\widehat{T}(u, v) = (\varepsilon_1 c_{i_1}, \varepsilon_2 c_{i_2}) \Leftrightarrow (u, v) \in N_{\varepsilon_1,i_1} \cap M_{\varepsilon_2,i_2},$$

where $\varepsilon_1, \varepsilon_2 \in \{\pm 1\}$ and $i_1, i_2 \in \{0, 1, 2\}$.

Some properties of $N_{\varepsilon,i}$ and $M_{\varepsilon,i}$

Let $\mathcal{A}$ be a set of $\mathbb{F}_{p^m}^2$, and define

$$(\theta, -\theta)\mathcal{A} = \{(\theta, -\theta)(a, b) \mid (a, b) \in \mathcal{A}\} = \{(a\theta, -b\theta) \mid (a, b) \in \mathcal{A}\}$$

and

$$\theta\mathcal{A} = \{(a\theta, b\theta) \mid (a, b) \in \mathcal{A}\}.$$

Lemma 4

Let $N_{\varepsilon,i}$ and $M_{\varepsilon,i}$ be the sets defined in (2.4). Then,

(i) for any $\varepsilon \in \{\pm 1\}$ and any $i \in \{0, 1, 2\}$, $(\theta, -\theta)N_{\varepsilon,i} = M_{\varepsilon,i}$, $N_{\varepsilon,i} = (\theta, -\theta)M_{\varepsilon,i}$;

(ii) for any $\varepsilon \in \{\pm 1\}$ and any $i \in \{0, 2\}$, $\theta N_{\varepsilon,i} = N_{-\varepsilon,i}$, $\theta M_{\varepsilon,i} = M_{-\varepsilon,i}$;

(iii) for any $\varepsilon \in \{\pm 1\}$, $\theta N_{\varepsilon,1} = N_{\varepsilon,1}, \theta M_{\varepsilon,1} = M_{\varepsilon,1}$.

Some properties of $T(u, v)$

Lemma 5

Let $T(u, v)$ be the exponential sum defined in (1.6) and $\mathcal{N}$ be the number given in Lemma 6. Then

(i) $$\sum_{(u,v)\in\mathbb{F}_{p^m}^2} T(u,v)T(u\theta,-v\theta) = p^{2m};$$

(ii) $$\sum_{(u,v)\in\mathbb{F}_{p^m}^2} T^3(u,v)T(u\theta,-v\theta) = p^{2m}\mathcal{N}.$$

The number of solutions to a system of equations

Lemma 6

With the notation above, let $\mathcal{N}$ denote the number of solutions of

$$\begin{cases} x^2+y^2+z^2-\theta w^2=0, \\ x^{p^k+1}+y^{p^k+1}+z^{p^k+1}+\theta w^{p^k+1}=0, \end{cases}$$

where $(x,y,z,w)\in\mathbb{F}_{p^m}^4$ and θ is a fixed nonsquare in $\mathbb{F}_{p^e}$. Then

$$\mathcal{N}=\begin{cases} p^{m+e}+p^m-p^e, & \text{if } p^e\equiv 1 \pmod 4, \\ 2p^{2m}-p^{m+e}-p^m+p^e, & \text{if } p^e\equiv 3 \pmod 4. \end{cases}$$

Proof sketch of Lemma 6

- $\mathcal{N}_1(a,b)$: the number of solutions to

$$\begin{cases} x^2 + y^2 = a, \\ x^{p^{k+1}} + y^{p^{k+1}} = b. \end{cases}$$

- $\mathcal{N}_2(a,b)$: the number of solutions to

$$\begin{cases} z^2 - \theta w^2 = -a, \\ z^{p^{k+1}} + \theta w^{p^{k+1}} = -b. \end{cases}$$

- $\mathcal{N}$: the number of solutions to the system in Lemma 5

$$\mathcal{N} = \sum_{(a,b)\in\mathbb{F}_{p^m}^2} \mathcal{N}_1(a,b)\mathcal{N}_2(a,b).$$

Value distribution of $\widehat{T}(u,v)$

Theorem 1

Let $\widehat{T}(u,v)$ be the function defined by (2.3). Then, the value distribution of $\widehat{T}(u,v)$ as (u,v) runs through $\mathbb{F}_{p^m}^2$ is given in Table 2 if $p^e \equiv 1 \pmod 4$ and in Table 3 if $p^e \equiv 3 \pmod 4$, where c_i, $i = 0, 1, 2$, are defined by (20).

Table 2: Value distribution of $\widehat{T}(u,v)$ if $p^e \equiv 1 \pmod 4$

Value	Frequency (each)
(p^m, p^m)	1
(c_0, c_0) $(-c_0, -c_0)$	$\frac{(p^{2m}-1)(p^e-1)}{4(p^e+1)}$
$(-c_0, c_0)$, $(c_0, -c_0)$	$\frac{(p^m-1)[(p^m+1)(p^e-3)+4]}{4(p^e-1)}$
(c_0, c_1), (c_1, c_0) $(-c_0, c_1)$, $(c_1, -c_0)$	$\frac{(p^m-1)(p^{m-e}+p^{\frac{m-e}{2}})}{4}$
$(-c_0, -c_1)$, $(-c_1, -c_0)$ $(c_0, -c_1)$, $(-c_1, c_0)$	$\frac{(p^m-1)(p^{m-e}-p^{\frac{m-e}{2}})}{4}$
(c_0, c_2), (c_2, c_0) $(-c_0, -c_2)$, $(-c_2, -c_0)$	0
$(-c_0, c_2)$, $(c_2, -c_0)$ $(c_0, -c_2)$, $(-c_2, c_0)$	$\frac{(p^m-1)(p^{m-e}-1)}{2(p^{2e}-1)}$

Table 3: Value distribution of $\widehat{T}(u,v)$ if $p^e \equiv 3 \pmod 4$

Value	Frequency (each)
(p^m, p^m)	1
(c_0, c_0) $(-c_0, -c_0)$	$\frac{(p^m-1)[(p^m+1)(p^e-3)+4]}{4(p^e-1)}$
$(-c_0, c_0)$, $(c_0, -c_0)$	$\frac{(p^{2m}-1)(p^e-1)}{4(p^e+1)}$
(c_0, c_1), (c_1, c_0) $(-c_0, c_1)$, $(c_1, -c_0)$	$\frac{(p^m-1)(p^{m-e}+p^{\frac{m-e}{2}})}{4}$
$(-c_0, -c_1)$, $(-c_1, -c_0)$ $(c_0, -c_1)$, $(-c_1, c_0)$	$\frac{(p^m-1)(p^{m-e}-p^{\frac{m-e}{2}})}{4}$
(c_0, c_2), (c_2, c_0) $(-c_0, -c_2)$, $(-c_2, -c_0)$	$\frac{(p^m-1)(p^{m-e}-1)}{2(p^{2e}-1)}$
$(-c_0, c_2)$, $(c_2, -c_0)$ $(c_0, -c_2)$, $(-c_2, c_0)$	0

Value distribution of $S_d(u,v)$

Theorem 2

Let $S_d(u,v)$ be the exponential sum defined by (1.2).

(i) When $d \equiv 1 \pmod{p^e - 1}$, the value distribution of $S_d(u,v)$ is given in Table 4;

(ii) When $d \equiv 1 + \frac{p^e-1}{2} \pmod{p^e - 1}$, the value distribution of $S_d(u,v)$ is given in Table 5 if $p^e \equiv 1 \pmod 4$ and in Table 6 if $p^e \equiv 3 \pmod 4$.

Table 4: Value distribution of $S_d(u,v)$ when $d \equiv 1 \pmod{p^e - 1}$

Value	Frequency (each)
p^m	1
0	$(p^m - 1)(p^m - p^{m-e} + 1)$
$p^{\frac{m+e}{2}}$	$\frac{(p^m-1)(p^{m-e}+p^{\frac{m-e}{2}})}{2}$
$-p^{\frac{m+e}{2}}$	$\frac{(p^m-1)(p^{m-e}-p^{\frac{m-e}{2}})}{2}$

Table 5: Value distribution of $S_d(u,v)$ when $d \equiv 1 + \frac{p^e-1}{2} \pmod{p^e-1}$ and $p^e \equiv 1 \pmod 4$

Value	Frequency (each)
p^m	1
$\pm p^{\frac{m}{2}}$	$\frac{(p^{2m}-1)(p^e-1)}{4(p^e+1)}$
0	$\frac{(p^m-1)[(p^m+1)(p^e-3)+4]}{2(p^e-1)}$
$\frac{\pm 1+\sqrt{p^e}}{2} p^{\frac{m}{2}}$	$\frac{(p^m-1)(p^{m-e}+p^{\frac{m-e}{2}})}{2}$
$\frac{\pm 1-\sqrt{p^e}}{2} p^{\frac{m}{2}}$	$\frac{(p^m-1)(p^{m-e}-p^{\frac{m-e}{2}})}{2}$
$\pm \frac{p^e-1}{2} p^{\frac{m}{2}}$	$\frac{(p^m-1)(p^{m-e}-1)}{(p^{2e}-1)}$

Table 6: Value distribution of $S_d(u, v)$ when $d \equiv 1 + \frac{p^e-1}{2} \pmod{p^e - 1}$ and $p^e \equiv 3 \pmod 4$

Value	Frequency (each)
p^m	1
$\pm p^{\frac{m}{2}}\sqrt{-1}$	$\frac{(p^m-1)[(p^m+1)(p^e-3)+4]}{4(p^e-1)}$
0	$\frac{(p^{2m}-1)(p^e-1)}{2(p^e+1)}$
$\frac{\pm\sqrt{-1}+\sqrt{p^e}}{2}p^{\frac{m}{2}}$	$\frac{(p^m-1)(p^{m-e}+p^{\frac{m-e}{2}})}{2}$
$\frac{\pm\sqrt{-1}-\sqrt{p^e}}{2}p^{\frac{m}{2}}$	$\frac{(p^m-1)(p^{m-e}-p^{\frac{m-e}{2}})}{2}$
$\pm\frac{p^e+1}{2}p^{\frac{m}{2}}\sqrt{-1}$	$\frac{(p^m-1)(p^{m-e}-1)}{(p^{2e}-1)}$

Recall some facts

- $d\left(p^k+1\right) \equiv 2 \pmod{p^m-1}$;
- $S_d(u,v) = \sum_{x \in \mathbb{F}_{p^m}} \omega_p^{\mathrm{Tr}_1^m\left(ux+vx^d\right)}$;
- $C_d(\gamma) = \sum_{x \in \mathbb{F}_{p^m}} \omega_p^{\mathrm{Tr}_1^m(x+\gamma x^d)} - 1 = S_d(1,\gamma) - 1.$

Some properties of $S_d(u,v)$

Lemma 7

Let $S_d(u,v)$ be the exponential sum given in (1.2).

(i) $S_d(u,0)=0$ for any $u\in\mathbb{F}_{p^m}^*$;

(ii) When $d\equiv 1 \pmod{p^e-1}$, or $d\equiv 1+\frac{p^e-1}{2} \pmod{p^e-1}$ and $p^e\equiv 1 \pmod 4$, $S_d(0,v)=0$ for any $v\in\mathbb{F}_{p^m}^*$;

(iii) When $d\equiv 1+\frac{p^e-1}{2} \pmod{p^e-1}$ and $p^e\equiv 3 \pmod 4$, $S_d(0,v)\in\left\{\pm p^{\frac{m}{2}}\sqrt{-1}\right\}$ for any $v\in\mathbb{F}_{p^m}^*$ and each value occurs $\frac{p^m-1}{2}$ times as v runs through $\mathbb{F}_{p^m}^*$;

(iv) For any given $u\in\mathbb{F}_{p^m}^*$, as v runs through $\mathbb{F}_{p^m}^*$, $S_d(u,v)$ and $S_d(1,v)$ have the same value distribution.

Cross-correlation distribution for d

Theorem 3

Let p, m and k satisfy Eq. (1.3), and d satisfy Eq. (1.4).

(i) When $\gcd(d, p^m - 1) = 1$, the value distribution of $C_d(\gamma)$ is given in Table 7 if $d \equiv 1 \pmod{p^e - 1}$, and in Table 8 if $d \equiv 1 + \frac{p^e-1}{2} \pmod{p^e - 1}$ and $p^e \equiv 1 \pmod 4$.

(ii) When $\gcd(d, p^m - 1) = 2$, i.e., $d \equiv 1 + \frac{p^e-1}{2} \pmod{p^e - 1}$ and $p^e \equiv 3 \pmod 4$, the value distribution of $C_d(\gamma)$ is given in Table 9.

Table 7: Cross-correlation distribution for $d \equiv 1 \pmod{p^e - 1}$

Value	Frequency (each)
-1	$(p^m - p^{m-e} - 1)$
$p^{\frac{m+e}{2}} - 1$	$\frac{(p^{m-e}+p^{\frac{m-e}{2}})}{2}$
$-p^{\frac{m+e}{2}} - 1$	$\frac{(p^{m-e}-p^{\frac{m-e}{2}})}{2}$

Table 8: Cross-correlation distribution for $d \equiv 1 + \frac{p^e-1}{2} \pmod{p^e-1}$ and $p^e \equiv 1 \pmod 4$

Value	Frequency (each)
-1	$\frac{(p^{m+e}-3p^m-3p^e+5)}{2(p^e-1)}$
$\pm p^{\frac{m}{2}}-1$	$\frac{(p^m+1)(p^e-1)}{4(p^e+1)}$
$\frac{\pm 1+\sqrt{p^e}}{2}p^{\frac{m}{2}}-1$	$\frac{(p^{m-e}+p^{\frac{m-e}{2}})}{2}$
$\frac{\pm 1-\sqrt{p^e}}{2}p^{\frac{m}{2}}-1$	$\frac{(p^{m-e}-p^{\frac{m-e}{2}})}{2}$
$\pm\frac{p^e-1}{2}p^{\frac{m}{2}}-1$	$\frac{p^{m-e}-1}{p^{2e}-1}$

Table 9: Cross-correlation distribution for $d \equiv 1 + \frac{p^e-1}{2} \pmod{p^e-1}$ and $p^e \equiv 3 \pmod 4$

Value	Frequency (each)
-1	$\frac{p^{m+e}-p^m-p^e-3}{2(p^e+1)}$
$\pm p^{\frac{m}{2}}\sqrt{-1}-1$	$\frac{p^{m+e}-3p^m-p^e+3}{4(p^e-1)}$
$\frac{\pm\sqrt{-1}+\sqrt{p^e}}{2}p^{\frac{m}{2}}-1$	$\frac{(p^{m-e}+p^{\frac{m-e}{2}})}{2}$
$\frac{\pm\sqrt{-1}-\sqrt{p^e}}{2}p^{\frac{m}{2}}-1$	$\frac{(p^{m-e}-p^{\frac{m-e}{2}})}{2}$
$\pm\frac{p^e+1}{2}p^{\frac{m}{2}}\sqrt{-1}-1$	$\frac{p^{m-e}-1}{p^{2e}-1}$

Type 1

- Type 1: odd prime p, $\frac{m}{e} \geq 3$ odd, $e = \gcd(k, m)$, $d(p^k + 1) \equiv 2(\bmod\, p^m - 1)$, $d \equiv 1(\bmod\, p^e - 1)$, 3-valued, $p^{\frac{m+e}{2}} + 1$.
- (Helleseth, 1976): odd prime p, $\frac{m}{e} \geq 3$ odd, $e = \gcd(k, m)$, $d = \frac{p^k+1}{2}$, $\frac{k}{e}$ even, 3-valued, $p^{\frac{m+e}{2}} + 1$. (Inverse is covered by Type 1.)

T. Helleseth, "Some results about the cross-correlation function between two maximal linear sequences," *Discr. Math.*, 16: 209-232 (1976)

- Recently, Ding *et al.* reported three new decimations for ternary m-sequences that give a three-valued cross-correlation function:
  - $\frac{3^{m+1}-1}{3^h+1} + \frac{3^m-1}{2}$, $m \geq 3$ odd, $\frac{m+1}{h}$ even
  - $\left(3^{\frac{m+1}{8}} - 1\right)\left(3^{\frac{m+1}{4}} + 1\right)\left(3^{\frac{m+1}{2}} + 1\right) + \frac{3^m-1}{2}$, $m \equiv 7 \pmod 8$
  - $\left(3^{\frac{m+1}{4}} - 1\right)\left(3^{\frac{m+1}{2}} + 1\right) + \frac{3^m-1}{2}$, $m \equiv 3 \pmod 4$
- These decimations are of Type 1.

C. Ding, Y. Gao and Z. Zhou, "Five families of three-weight ternary cyclic codes and their duals," *IEEE Trans. Inf. Theory*, 59(12): 7940-7946(2013)

Type 2

- Type 2: odd prime p, $p^e \equiv 1 \pmod 4$, $\frac{m}{e} \geq 3$ odd, $e = \gcd(k,m)$, $d(p^k+1) \equiv 2 (\text{mod}\, p^m - 1)$, $d \equiv 1 + \frac{p^e-1}{2} (\text{mod}\, p^e - 1)$, 9-valued, $\frac{p^e-1}{2} p^{\frac{m}{2}} + 1$.
- (Luo and Feng, 2008): odd prime p, $p^e \equiv 1 \pmod 4$, $e = \gcd(k,m)$, $\frac{m}{e} \geq 3$ odd, $d = \frac{p^k+1}{2}$, $\frac{k}{e}$ odd, 9-valued, $\frac{p^e-1}{2} p^{\frac{m}{2}} + 1$. (Inverse is covered by Type 2.)

J. Luo and K. Feng, "Cyclic codes and sequence from generalized Coulter-Matthews functions," *IEEE Trans. Inf. Theory*, 54(12): 5345-5353 (2008)

Type 3

- Type 3: odd prime p, $p^e \equiv 3 \pmod 4$, $\frac{m}{e} \geq 3$ odd, $e = \gcd(k,m)$, $d(p^k+1) \equiv 2 (\bmod\, p^m - 1)$, $d \equiv 1 + \frac{p^e-1}{2} (\bmod\, p^e - 1)$, $\gcd(d, p^m-1) = 2$, 9-valued, $\frac{p^e+1}{2} p^{\frac{m}{2}} + 1$.
- (Xia et. al, 2010, and Choi et. al, 2013): $p \equiv 3 \pmod 4$, m odd, $e \mid m$, $\frac{m}{e} \geq 3$, $d = \frac{p^m+1}{p^e+1} \pm \frac{p^m-1}{2}$, $\gcd(d, p^m-1) = 2$, 9-valued, $\frac{p^e+1}{2} p^{\frac{m}{2}} + 1$. (Special cases of Type 3.)

Y. Xia, X. Zeng and L. Hu, "Further crosscorrelation properties of sequences with the decimation factor $d = \frac{p^n+1}{p+1} - \frac{p^n-1}{2}$," *Appl. Algebra Eng. Commun. Comput.*, 21(5): 329-342 (2010)

S. T. Choi, J. Y. Kim, and J. S. No, "On the cross-correlation of a p-ary m-sequence and its decimated sequences by $d = \frac{p^n+1}{p^k+1} + \frac{p^n-1}{2}$," *IEICE Trans. Commun.*, vol. E96-B(9): 2190-2197 (2013)

Thank you!