Some Recent Progress in the Applications of Niho Exponents

Nian Li

Faculty of Mathematics and Statistics
Hubei University
Wuhan, China

July 5, 2017

Outline

Definition

Let p be a prime, $n = 2m$ a positive integer and $q = p^m$. Let $\mathbb{F}_q$ denote the finite field with q elements.

Niho Exponent

A positive integer d is called a Niho exponent (with respect to $\mathbb{F}_{q^2}$) if there exists some $0 \leq j \leq n-1$ such that

$$d \equiv p^j \pmod{q-1}$$

- Normalized form: $j = 0$, i.e., $d = (q-1)s + 1$.
- Generalized form: $d \equiv \Delta \pmod{q-1}$ for some integer Δ.

Cross Correlation Between an m-sequence and Its Decimation Sequence

The determination of the cross correlation between an m-sequence and its d-decimation sequence is a classic research problem.

Basic Notations:

- $\mathrm{Tr}(\cdot)$ is the trace function from $\mathbb{F}_q$ to $\mathbb{F}_p$.
- α is a primitive element of $\mathbb{F}_q$.
- ω is a p-th primitive root of unity.
- $s(t) = \mathrm{Tr}(\alpha^t)$ is an m-sequence of period $q - 1$.
- $s(dt) = \mathrm{Tr}(\alpha^{dt})$ is the d-decimation sequences of $s(t)$.

Correlation Function

Correlation Function

The periodic cross correlation function $C_d(\tau)$ between the sequences $s(t)$ and $s(dt)$ is defined for $\tau = 0, 1, 2, \cdots, q-2$ by

$$C_d(\tau) = \sum_{t=0}^{q-2} w^{s(t+\tau)-s(dt)} = \sum_{x\in\mathbb{F}_q} w^{\mathrm{Tr}(\alpha^\tau x - x^d)} - 1.$$

Main Research Problems

- Find decimation d such that $C_d(\tau)$ takes few values.
- Determine the value distribution of $C_d(\tau)$.

Correlation Function

Known 3-valued Correlation Function $C_d(\tau)$ over $\mathbb{F}_{2^n}$

No.	d-Decimation	Condition	Remarks
1	$2^k + 1$	$n/\gcd(n,k)$ odd	Gold, 1968
2	$2^{2k} - 2^k + 1$	$n/\gcd(n,k)$ odd	Kasami, 1971
3	$2^{n/2} - 2^{(n+2)/4} + 1$	$n \equiv 2 \pmod 4$	Cusick et al., 1996
4	$2^{n/2+1} + 3$	$n \equiv 2 \pmod 4$	Cusick et al., 1996
5	$2^{(n-1)/2} + 3$	n odd	Canteaut et al., 2000
6	$2^{(n-1)/2} + 2^{(n-1)/4} - 1$	$n \equiv 1 \pmod 4$	Hollmann et al., 2001
7	$2^{(n-1)/2} + 2^{(3n-1)/4} - 1$	$n \equiv 3 \pmod 4$	Hollmann et al., 2001

Remarks: (1) No. 5 is the Welch's conjecture; (2) Nos. 6 and 7 are the Niho's conjectures

Open Problem

Show that the table contains all decimations with 3-valued correlation function.

Correlation Function

Known 3-valued Correlation Function $C_d(\tau)$ over $\mathbb{F}_{p^n}$

No.	d-Decimation	Condition	Remarks
1	$(p^{2k}+1)/2$	$n/\gcd(n,k)$ odd	Trachtenberg, 1970
2	$p^{2k}-p^k+1$	$n/\gcd(n,k)$ odd	Trachtenberg, 1970
3	$2\cdot 3^{(n-1)/2}+1$	$n/\gcd(n,k)$ odd	Dobbertin et al., 2001
4	$2\cdot 3^k+1$	$n\|4k+1$, n odd	Katz and Langevin, 2015

Remarks: (1) Nos. 1 and 2 are due to Helleseth for even n; (2) The result obtained by Xia et al. (IEEE IT 60(11), 2014) is covered by No. 1

Open Problems

- Show that the table contains all decimations with 3-valued correlation function for $p > 3$.

Correlation Function

Known 4-valued Correlation Function $C_d(\tau)$ over $\mathbb{F}_{2^n}$

No.	d-Decimation	Condition	Remarks
1	$2^{n/2+1}-1$	$n \equiv 0 \pmod 4$	Niho, 1972
2	$(2^{n/2}+1)(2^{n/4}-1)+2$	$n \equiv 0 \pmod 4$	Niho, 1972
3	$\frac{2^{(n/2+1)r}-1}{2^r-1}$	$n \equiv 0 \pmod 4$	Dobbertin, 1998
4	$\frac{2^n+2^{s+1}-2^{n/2+1}-1}{2^s-1}$	$n \equiv 0 \pmod 4$	Helleseth et al., 2005
5	$(2^{n/2}-1)\frac{2^r}{2^r\pm1}+1$	$n \equiv 0 \pmod 4$	Dobbertin et al., 2006

Remarks: (1) All are the Niho type decimations; (2) No. 5 covers previous four cases.

Conjecture (Dobbertin, Helleseth et al., 2006)

No. 5 covers all 4-valued cross correlation for Niho type decimation.

Correlation Function

Known 4-valued Correlation Function $C_d(\tau)$ over $\mathbb{F}_{p^n}$

No.	d-Decimation	Condition	Remarks
1	$2 \cdot p^{n/2} - 1$	$p^{n/2} \not\equiv 2 \pmod 3$	Helleseth, 1976
2	$3^k + 1$	$n = 3k, k$ odd	Zhang et al., 2013
3	$3^{2k} + 2$	$n = 3k, k$ odd	Zhang et al., 2013

Remarks: (1) No. 1 is a Niho type decimation; (2) Nos. 2 and 3 are due to Zhang et al. if $\gcd(k, 3) = 1$ and due to Xia et al. if $\gcd(k, 3) = 3$.

Open Problem

Find new 4-valued $C_d(\tau)$ for any prime p.

Correlation Function

Known 5 or 6-valued Correlation Function $C_d(\tau)$ over $\mathbb{F}_{2^n}$

No.	d-Decimation	Condition	Remarks
1	$2^{n/2}+3$	$n \equiv 0 \pmod 2$	Helleseth, 1976
2	$2^{n/2}-2^{n/4}+1$	$n \equiv 0 \pmod 8$	Helleseth, 1976
3	$\frac{2^n-1}{3}+2^i$	$n \equiv 0 \pmod 2$	Helleseth, 1976
4	$2^{n/2}+2^{n/4}+1$	$n \equiv 0 \pmod 4$	Dobbertin, 1998

Remarks: (1) No. 1 was conjectured by Niho; (2) No. 3 is of Niho type if $n/2$ is odd.

Open Problem (Dobbertin, Helleseth et al., 2006)

Determine the cross correlation distribution of $C_d(\tau)$ for the Niho type decimation $d = 3 \cdot (2^{n/2}-1)+1$.

Correlation Function

Known 5 or 6-valued Correlation Function $C_d(\tau)$ over $\mathbb{F}_{p^n}$

No.	d-Decimation	Condition	Remarks
1	$(p^n-1)/2+p^i$	$p^n \equiv 1 \pmod 4$	Helleseth, 1976
2	$(p^n-1)/3+p^i$	$p \equiv 2 \pmod 3$	Helleseth, 1976
3	$p^{n/2}-p^{n/4}+1$	$p^{n/4} \not\equiv 2 \pmod 3$	Helleseth, 1976
4	3^k+1	$n=3k, k$ even	Zhang et al., 2013
5	$3^{2k}+2$	$n=3k, k$ even	Zhang et al., 2013

Remarks: (1) No. 1 is of Niho type if $n/2$ is odd; (2) Nos. 4 and 5 are due to Zhang et al. if $\gcd(k,3)=1$ and due to Xia et al. if $\gcd(k,3)=3$.

Open Problem (Dobbertin, Helleseth and Martinsen, 1999)

Determine the cross correlation distribution of $C_d(\tau)$ for the Niho type decimation $d = 3\cdot(3^{n/2}-1)+1$.

Correlation Function: Recent Results

Let k be a positive integer and N_k denote the number of solutions to

$$\begin{aligned} x_1 + x_2 + \cdots + x_k &= 0, \\ x_1^d + x_2^d + \cdots + x_k^d &= 0. \end{aligned}$$

Question: How to determine the values of N_k?

Open Problem (Dobbertin, Helleseth et al., 2006)

Determine the cross correlation distribution of $C_d(\tau)$ for the Niho type decimation $d = 3 \cdot (2^{n/2} - 1) + 1$.

Solved! (surprising connection with the Zetterberg code) by Xia, L., Zeng and Helleseth 2016 (IEEE IT, 62(12), 2016)

Correlation Function: Recent Results

Open Problem (Dobbertin, Helleseth and Martinsen, 1999)

Determine the cross correlation distribution of $C_d(\tau)$ for the Niho type decimation $d = 3 \cdot (3^{n/2} - 1) + 1$.

Solved!

by Xia, L., Zeng and Helleseth 2017 (it is available on arXiv).

Future Work

Determine the cross correlation distribution of $C_d(\tau)$ for the Niho type decimation $d = 3 \cdot (p^{n/2} - 1) + 1$ for $p > 3$.

This case is much more complicated!

Bent Functions From Niho Exponents

Bent functions have significant applications in cryptography and coding theory.

Walsh Transform

Let $f(x)$ be a function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$. The Walsh transform of $f(x)$ is defined by

$$\widehat{f}(\lambda) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x)+\mathrm{Tr}(\lambda x)}, \lambda \in \mathbb{F}_{2^n}.$$

Bent Function

A function $f(x)$ from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$ is called Bent if $|\widehat{f}(\lambda)| = 2^{n/2}$ for any $\lambda \in \mathbb{F}_{2^n}$.

Bent Functions From Niho Exponents

Problem Description

Let $f(x)$ be a function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$ defined by

$$f(x) = \sum_{i=1}^{2^n-2} \mathrm{Tr}(a_i x^i), a_i \in \mathbb{F}_{2^n}.$$

Then how to choose a_i and i such that $f(x)$ is Bent?

Remarks

Known infinite classes of Boolean Bent functions:

1. Monomial Bent: only 5 classes
2. Binomial Bent: only about 6 classes
3. Polynomial form: quadratic form, Dillon type and Niho type

Constructions of Bent Functions of Niho Type

Known Constructions of Niho Bent Functions

Table: Known Niho Bent Functions

No.	Class of Functions	Authors	Year
1	$\mathrm{Tr}_1^n(ax^{(2^m-1)\frac{1}{2}+1})$	–	–
2	$\mathrm{Tr}_1^n(ax^{(2^m-1)\frac{1}{2}+1} + bx^{(2^m-1)3+1})$	Dobbertin et al.	2006
3	$\mathrm{Tr}_1^n(ax^{(2^m-1)\frac{1}{2}+1} + bx^{(2^m-1)\frac{1}{4}+1})$	Dobbertin et al.	2006
4	$\mathrm{Tr}_1^n(ax^{(2^m-1)\frac{1}{2}+1} + bx^{(2^m-1)\frac{1}{6}+1})$	Dobbertin et al.	2006
5	$\mathrm{Tr}_1^n(ax^{(2^m-1)\frac{1}{2}+1} + \sum_{i=1}^{2^{r-1}-1} x^{(2^m-1)\frac{i}{2^r}+1})$	Leander, Kholosha	2006

Remarks: (1) No. 1 is trivial; (2) No. 3 is covered by No. 5

Niho Type Bent Functions: Some Recent Results

Let $n = 2m$, p be a prime and $q = p^m$. Define

$$f(x) = \sum_{i=1}^{p^r-1} \mathrm{Tr}_1^n(ax^{(ip^{m-r}+1)(q-1)+1})$$

Theorem (L., Helleseth, Kholosha and Tang, 2013)

1. $f(x)$ is Bent if $p = 2$ and $\gcd(r, m) = 1$ (4-valued otherwise), and it is equivalent to the Leander-Kholosha's Bent functions.
2. The proof (based on quadratic form) is self-contained and much simpler than the original one (by using Dickson polynomials and complicated techniques over finite fields).

Niho Type Bent Functions: Some Recent Results

Let $n = 2m$ and $0 < r < m$. Define

$$f(x) = \mathrm{Tr}\left(a_{2^r-1}x^{2^m+1} + \sum_{i=1}^{2^{r-1}-1} a_i x^{(2^m-1)(2^{m-r}i+1)+1}\right)$$

Theorem (Budaghyan, Kholosha, Carlet, Helleseth, 2014/2016)

1. Up to EA-equivalence, any Niho Bent function has the above form.
2. New Niho Bent functions obtained from quadratic and cubic o-polynomials.

Challenging problems: Determine the coefficients for o-polynomials of higher degree; or find new Niho Bent functions from other approach?

Cyclic Codes with Niho Type Zeros

Let α be a primitive element of $\mathbb{F}_{p^n}$ and $m_{\alpha^i}(x)$ denote the minimal polynomial of α^i over $\mathbb{F}_p$ for $1 \le i \le p^n - 1$. Define

$$\mathcal{C}_{(d_1, d_2, \cdots, d_k)} = \langle m_{\alpha^{d_1}}(x) m_{\alpha^{d_2}}(x) \cdots m_{\alpha^{d_k}}(x) \rangle,$$

i.e., cyclic codes with generator polynomial $m_{\alpha^{d_1}}(x) m_{\alpha^{d_2}}(x) \cdots m_{\alpha^{d_k}}(x)$.

Research Topics

1. Find $\mathcal{C}_{(d_1, d_2, \cdots, d_k)}$ with optimal or good parameters;
2. Determine the weight distribution of its dual.

Remark: Normally both of them are difficult when $k \ge 3$.

Some Known Results on $\mathcal{C}_{(1,e)}$

For $k = 2$, cyclic code $\mathcal{C}_{(1,e)}$ has been well investigated:

Known Results about $\mathcal{C}_{(1,e)}$

1. $p = 2$: $\mathcal{C}_{(1,e)}$ is optimal if and only if x^e is APN
   - proved by Carlet, Charpin and Zinoviev in 1998
   - subcode $\mathcal{C}_{(0,1,e)}$ was investigated by Carlet, Ding and Yuan in 2005
2. $p > 3$: $\mathcal{C}_{(1,e)}$ cannot be optimal (minimal distance ≤ 3)
   - weight distribution if x^e is PN (Yuan, Carlet and Ding, 2006)
3. Connection with the correlation distribution between m-sequences
   - proved by Katz in 2012

Some Known Results on $\mathcal{C}_{(1,e)}$

For $p = 3$, $\mathcal{C}_{(1,e)}$ is optimal if it has parameters $[3^m - 1, 3^m - 1 - 2m, 4]$.

Known Results about $\mathcal{C}_{(1,e)}$ for $p = 3$

- $\mathcal{C}_{(1,e)}$, $\mathcal{C}_{(0,1,e)}$ are optimal if x^e is PN (Carlet, Ding and Yuan, 2005)
- $\mathcal{C}_{(1,e)}$ is optimal if x^e is APN (Ding and Helleseth, 2013)
- $\mathcal{C}_{(1,e,\frac{3^m-1}{2})}$ is optimal for some e (L.,Li,Helleseth,Ding and Tang,2014)
- weight distribution if x^e is PN (Yuan, Carlet and Ding, 2006)
- weight distributions if x^e is APN (Li, L., Helleseth and Ding, 2014)

Weight distribution of $\mathcal{C}_{(d_1,d_2,\cdots,d_k)}$ with Niho Exponents

A cyclic code $\mathcal{C}$ is said to have t nonzeros if its parity-check polynomial has t irreducible factors over $\mathbb{F}_p$.

Theorem (Li, Zeng and Hu, 2010)

Let $n = 2m$ and $d_i = s_i(2^m - 1) + 1$ for $i = 1, 2, 3$. Then the weight distribution of the dual of $\mathcal{C}_{(d_1,d_2,d_3)}$ is determined for the following cases:

- $(s_1, s_2, s_3) = (\frac{1}{2}, 1, 2^{m-1})$.
- $(s_1, s_2, s_3) = (\frac{1}{2}, 1, 2^{m-2} + 1)$.

Remark: it has 3 Niho type nonzeros.

Weight distribution of $\mathcal{C}_{(d_1,d_2,\cdots,d_k)}$ with Niho Exponents

Theorem (Li, Feng and Ge, 2013)

Let $n = 2m$ and $d_i = s_i(p^m - 1) + 1$ for $i = 1, 2$. Then the weight distribution of the dual of $\mathcal{C}_{(d_1,d_2)}$ is determined for the following cases:

1. $p = 2$
   - $(s_1, s_2) = (\frac{1}{2}, s_2)$. $s_2 \neq \frac{1}{2}$.
   - $(s_1, s_2) = (2^{k-1}t - \frac{t-1}{2}, 2^{k-1}t + \frac{t+1}{2})$, $k|m+1$, or $(k, 2m) = 1$.
2. $p > 2$
   - $(s_1, s_2) = (\frac{t+2}{4}, \frac{3t+2}{4})$, $t \equiv 2 \pmod 4$.

Remark: it has 2 Niho type nonzeros and some of their results are not new!

Weight distribution of $\mathcal{C}_{(i_1,i_2,\cdots,i_k)}$ with Niho Exponents

Recent Result (Xiong and L., 2015)

Let $n = 2m$, h, f be integers and q be a prime power. Then the weight distribution of the dual of $\mathcal{C}_{(\cdots,d_i,\cdots)}$ is determined for the following cases:

- $d_i = (ih + f)(q - 1) + 2f$, $i = 0, 1, 2, \cdots, t$
- $d_i = (ih + \frac{f-h}{2})(q - 1) + f$, $i = 1, 2, \cdots, t$

Main idea: Vandermonde matrix!

Remark: it has arbitrary number of Niho type nonzeros!

Weight distribution of $\mathcal{C}_{(i_1,i_2,\cdots,i_k)}$ with Niho Exponents

Recent Result (Xiong, L., Zhou and Ding, 2016)

Let $n = 2m$ and $d_i = s_i(2^m - 1) + \Delta$. Then the weight distribution of the dual of $\mathcal{C}_{(\cdots,d_i,\cdots)}$ is determined for the following cases:

- $s_i = ih + \frac{\Delta}{2}$, $i = 0, 1, 2, \cdots, t$
- $s_i = ih + \frac{\Delta - h}{2}$, $i = 1, 2, \cdots, t$

where $\gcd(\Delta, 2^m - 1) = 1$ and $h \not\equiv 0 \pmod{2^m + 1}$.

Main idea: Vandermonde matrix!

Remark: it has arbitrary number of Niho type nonzeros!

Problem of Weight distribution of $\mathcal{C}$ with Niho Exponents

Key Step: Let $n = 2m$, $d_i = s_i(2^m - 1) + 1$, $z_i \in \{z \in \mathbb{F}_{2^n} : z^{2^m+1} = 1\}$ and $y_i \in \mathbb{F}_{2^m}$. Then, how to determine the number of solutions to

$$\begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ z_1^{1-2s_1} & z_2^{1-2s_1} & z_3^{1-2s_1} & \cdots & z_k^{1-2s_1} \\ z_1^{1-2s_2} & z_2^{1-2s_2} & z_3^{1-2s_2} & \cdots & z_k^{1-2s_2} \\ z_1^{1-2s_3} & z_2^{1-2s_3} & z_3^{1-2s_3} & \cdots & z_k^{1-2s_3} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ z_1^{1-2s_t} & z_2^{1-2s_t} & z_3^{1-2s_t} & \cdots & z_k^{1-2s_t} \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \\ \vdots \\ y_k \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}?$$

Future Problems

1. Weight distribution for some other special coefficient matrices?
2. ......

Permutation Polynomials From Niho Exponents

Permutation Polynomial

A polynomial $f(x) \in \mathbb{F}_{q^2}[x]$ is called a permutation polynomial (PP) if the associated polynomial function $f : c \mapsto f(c)$ from $\mathbb{F}_{q^2}$ to $\mathbb{F}_{q^2}$ is a permutation of $\mathbb{F}_{q^2}$.

Application

- Coding Theory (Turbo codes; balanced component functions).
- Sequence Design (Welch's 3-valued conjecture; Helleseth's -1 conjecture).
- Cryptography (S-box; highly nonlinear function).
- Combinatorial Design (difference sets).

Permutation Polynomials over Finite Fields

Known Permutation Binomials over $\mathbb{F}_{q^2}$

1. $f(x) = x^r(x^{(q^2-1)/d} + a)$, Zieve 2009.
2. $f(x) = x^{r+s(q-1)} + ax^r$, Zieve 2013.
3. $f(x) = x^{s(q-1)+e} + ax^{(s-l)(q-1)+e}$, Tu, Zeng, Hu, Li 2013.
4. $f(x) = x^{2q+3} + ax$, $p = 2$, Tu, Zeng, Hu 2014.
5. $f(x) = x^{\frac{q}{4}(q+3)} + ax$, $p = 2$, Tu, Zeng, Hu 2014.
6. $f(x) = ax + x^{3q-2}$, Hou, Lappano 2015.
7. $f(x) = ax + x^{5q-4}$, Lappano 2015.
8. $f(x) = x(x^{q+1} + a)$, Li, Qu, Chen 2015.
9. $f(x) = x^r(x^{q-1} + a)$, Li, Qu, Chen 2015.

Permutation Polynomials over Finite Fields

Known Permutation Trinomials over $\mathbb{F}_{q^2}$ (q even)

1. Linearized PPs, Lidl, Niederreiter 1997.
2. $f(x) = x + x^5 + x^7$, Dickson polynomial, $n \equiv 1, 2 \pmod 3$.
3. $f(x) = x^{k(2^m+1)+3} + x^{k(2^m+1)+2^m+2} + x^{k(2^m+1)+3\cdot 2^m}$, Zieve 2013.
4. $f(x) = x + x^{kq-k+1} + x^{k+1-kq}$, Ding, Qu, Wang, Yuan, Yuan 2014.
5. $f(x) = x + ax^{2q-1} + a^{\frac{q}{2}}x^{q(q-1)+1}$, Ding et al. $(a = 1)$; Li et al. 2015.
6. $f(x) = ax + bx^q + x^{2q-1}$, Hou 2015.
7. $f(x) = x + x^q + x^{\frac{q}{2}(q-1)+1}$, $p = 2$, Li, Qu, Chen 2015.
8. $f(x) = x + x^{q+2} + x^{\frac{q}{2}(q+1)+1}$, Li, Qu, Chen 2015.
9. Two $n = 3m$ cases: Blokhuis et al. 2001 and Tu et al. 2014.

Niho Type Permutation Polynomials: Recent Results

New permutation trinomials over $\mathbb{F}_{2^n}$ with the form

$$f(x) = x + x^{s(2^m-1)+1} + x^{t(2^m-1)+1},$$

where $n = 2m$ and $1 \leq s, t \leq 2^m$.

Theorem (L. and Helleseth, 2016)

The polynomial $f(x)$ defined as above is a permutation polynomial if

1. $(s,t) = (-\frac{1}{3}, \frac{4}{3})$;
2. $(s,t) = (3, -1)$;
3. $(s,t) = (-\frac{2}{3}, \frac{5}{3})$;
4. $(s,t) = (\frac{1}{5}, \frac{4}{5})$.

Niho Type Permutation Polynomials: Recent Results

New permutation trinomials over $\mathbb{F}_{2^n}$ with the form

$$f(x) = x + x^{s(2^m-1)+1} + x^{t(2^m-1)+1},$$

where $n = 2m$ and $1 \leq s, t \leq 2^m$.

Theorem (L. and Helleseth, 2017)

The polynomial $f(x)$ defined as above is a permutation polynomial if

1. $(s,t) = (\frac{2^k}{2^k-1}, \frac{-1}{2^k-1})$, $\gcd(2^k-1, 2^m+1) = 1$; or
2. $(s,t) = (\frac{2^k}{2^k+1}, \frac{1}{2^k+1})$, $\gcd(2^k+1, 2^m+1) = 1$.

Main idea: Linear Fractional Polynomial!

Niho Type Permutation Polynomials: Recent Results

Table: Known pairs (s,t) such that $f(x)$ are permutation polynomials

No.	(s,t)	Equivalent Pairs	Proved by
1	$(k,-k)$	$(\frac{\pm k}{2k\mp1},\frac{\pm 2k}{2k\mp1})$	Ding et al.
2	$(2,-1)$	$(1,\frac{1}{3}),\ (1,\frac{2}{3})$	Ding et al.
3	$(1,-\frac{1}{2})$	$(1,\frac{3}{2}),\ (\frac{1}{4},\frac{3}{4})$	Li et al.; Gupta et al.
4	$(-\frac{1}{3},\frac{4}{3})$	$(1,\frac{1}{5}),\ (1,\frac{4}{5})$	L., Helleseth; Li et al.
5	$(3,-1)$	$(\frac{3}{5},\frac{4}{5}),\ (\frac{1}{3},\frac{4}{3})$	L., Helleseth; Li et al.
6	$(-\frac{2}{3},\frac{5}{3})$	$(1,\frac{2}{7}),\ (1,\frac{5}{7})$	L., Helleseth
7	$(\frac{1}{5},\frac{4}{5})$	$(1,-\frac{1}{3}),\ (1,\frac{4}{3})$	L., Helleseth; Li et al.
8	$(2,-\frac{1}{2})$	$(\frac{2}{3},\frac{5}{6}),(\frac{1}{4},\frac{5}{4})$	Li, Qu, Li, Fu
9	$(4,-2)$	$(\frac{2}{3},\frac{5}{6}),(\frac{1}{4},\frac{5}{4})$	Li, Qu, Li, Fu
10	$(\frac{2^k}{2^k-1},\frac{-1}{2^k-1})$	$(1,\frac{1}{2^k+1}),\ (1,\frac{2^k}{2^k+1})$	L., Helleseth
11	$(\frac{1}{2^k+1},\frac{2^k}{2^k+1})$	$(1,\frac{2^k}{2^k-1}),\ (1,\frac{-1}{2^k-1})$	L., Helleseth

Permutation Polynomials From Niho Exponents

Find permutation polynomials from Niho exponents with the form of

$$f(x) = x + ax^{s(p^m-1)+1} + bx^{t(p^m-1)+1} + \cdots \in \mathbb{F}_{p^n}[x],$$

where $n = 2m$ and $1 \leq s, t \leq p^m$.

Future Problems

1. More general results from Niho exponents?
2. Permutation polynomials from generalized Niho exponents?
3. Permutation polynomials for odd prime p.
4. Differential property of PPs (not from Niho exponents).

Niho Exponents: Another Application?

The Kim function is defined by

$$f(x) = x^{3} + x^{10} + ux^{24},$$

where u is a primitive element of $\mathbb{F}_{2^6}$.

An Interesting Fact

1. Using Kim function (which is APN)
2. Via simplex codes
3. Dillon et al. found the first APN permutation in even dimension!
4. The obtained APN permutation is CCZ-equivalent to Kim function!

Note that: $3 = 10 = 24 \pmod{2^3 - 1}$, i.e., they are generalized Niho exponents!!!

Thank You!

Questions? Comments? Suggestions?