New Classes of Ternary Bent Functions from the Coulter-Matthews Bent Functions

Honggang Hu

University of Science and Technology of China

Shanghai University, Shanghai, P. R. China

Outline

Walsh Transform

- $f(x)$ is a function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$.
- Its Walsh transform $\widehat{f}(\lambda)$ is defined by

$$\widehat{f}(\lambda) = \sum_{x \in \mathbb{F}_{p^n}} \omega_p^{f(x) - Tr_1^n(\lambda x)}.$$

- $Tr_1^n(\cdot)$ is the trace function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$.
- $\omega_p = e^{2\pi i/p}$ is the complex primitive p-th root of unity.

Bent Functions

- If
$$|\widehat{f}(\lambda)|^2 = p^n$$
for all $\lambda \in \mathbb{F}_{p^n}$, then $f(x)$ is called a **p-ary bent** function.
- Boolean bent functions: $p = 2$, then n even.

(Weakly) Regular Bent Functions

- A p-ary bent function $f(x)$ is called **regular** if there exists a p-ary function $g(x)$ from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$ such that

$$\widehat{f}(\lambda) = p^{\frac{n}{2}} \omega_p^{g(\lambda)}.$$

- $g(x)$: the dual function of $f(x)$
- $p = 2$: regular

(Weakly) Regular Bent Functions (Cont.)

- A p-ary bent function $f(x)$ is called **weakly regular** if there exists a complex number u with $|u| = 1$ such that

$$\widehat{f}(\lambda) = up^{\frac{n}{2}}\omega_p^{g(\lambda)}.$$

- $g(x)$: the dual function of $f(x)$
- $u = \pm 1, \pm i$

All Known p-Ary Dual Functions

p	n	Forms	Year
odd	arbitrary	$Tr_1^n(ax^2), a \in \mathbb{F}_{p^n}^*$	2006
odd	$2m$	$Tr_1^n(ax^{p^m+1}), a + a^{p^m} \neq 0$	1992, 2006
odd	arbitrary	$Tr_1^n(ax^{p^j+1}), a \in \mathbb{F}_{p^n}^*$ $p^{\gcd(2j,n)} - 1 \not\mid \frac{p^n-1}{2} - \mathrm{ind}(a)(p^j - 1)$	2006, 2007
odd	arbitrary	$Tr_1^n(ax^{p^j+1}), a \in \mathbb{F}_{p^n}^*, \frac{n}{\gcd(j,n)}$ odd	2007
3	$2m$	$Tr_1^n(ax^{t(3^m-1)})$ $a \in \mathbb{F}_{3^n}^*, m > 1, \gcd(t, 3^m + 1) = 1$ $\sum_{x \in \mathbb{F}_{3^m}} \omega_3^{Tr_1^m(x + a^{3^m+1}x^{3^m-1})} = 0$	2006, 2010
odd	$4m$	$Tr_1^n(x^{p^{3m}+p^{2m}-p^m+1} + x^2)$	2010
$p \equiv 3 \bmod 4$	$2m$, m odd	$Tr_1^n(ax^{p^m-1}) + Tr_1^2(bx^{(p^n-1)/4})$ $a \in \mathbb{F}_{p^n}^*, b \in \mathbb{F}_{p^2}^*, V = \{1, \xi, \xi^2, \cdots, \xi^{p^m}\}$ $\sum_{x \in V} \omega_p^{Tr_1^n(ax^{p^m-1}) + Tr_1^2(bx^{(p^n-1)/4})} = 1$	2011
odd	$2m$	$Tr_1^n(ax^{t(p^m-1)}) + bx^{(p^n-1)/2}$ $a \in \mathbb{F}_{p^n}^*, b \in \mathbb{F}_p^*, \gcd(t, p^m + 1) = 1$ $\sum_{x \in \mathbb{F}_{p^m}} \omega_p^{Tr_1^m(x + a^{p^m+1}x^{p^m-1})} = 2/(\omega_p^b + \omega_p^{-b})$	2012
3	$2m$, m odd	$Tr_1^n(ax^{\frac{3^n-1}{4}+3^m+1}), a = \xi^{(3^m+1)/4}$	2006, 2009, 2012
odd	$2m$	$\sum_{i=0}^{p^m-1} Tr_1^n(a_i x^{i(p^m-1)}) + Tr_1^l(bx^{(p^n-1)/e})$ $e \mid (q+1), a_i \in \mathbb{F}_{p^n}, b \in \mathbb{F}_{p^l}, U = \{x \in \mathbb{F}_{p^n} : x^{p^m+1} = 1\}$ $l = \min\{k > 0 : k \mid n, e \mid (p^k - 1)\}$ $\sum_{x \in U} \omega_p^{Tr_1^n(\sum_{i=0}^{p^m-1} a_i x^{i(p^m-1)}) + Tr_1^l(bx^{(p^n-1)/e})} = \omega_p^{Tr(a_0)}$	2013
3	arbitrary	$Tr_1^n(ax^{(3^k+1)/2}), \gcd(k, 2n) = 1$	2008, 2015, 2018

The Coulter-Matthews Bent Function

- 1997, Coulter and Matthews
- $\mathbb{F}_{3^n}$
- $\gcd(2n, k) = 1$, $d = \frac{3^k+1}{2}$
- $f(x) = Tr_1^n(ax^d)$ is bent for any $a \in \mathbb{F}_{3^n}^*$

The Coulter-Matthews Bent Function (Cont.)

Weakly regular

- In 2006, Helleseth and Kholosha **conjectured** that the Coulter-Matthews bent functions are **weakly regular** bent.
- In 2008, this conjecture was proved in two special cases by Hou. ($k = n + 1$ or $k = n - 1$)
- Completely settled in 2009 by Helleseth, Hollmann, Kholosha, Wang, and Xiang.

The Coulter-Matthews Bent Function (Cont.)

Dual function, $k = n + 1$ or $k = n - 1$, Hou, 2008

Corollary 3.3. *Let $n > 0$ be even and $a \in \mathbb{F}_{3^n}^*$. Then $\mathrm{Tr}(ax^{\frac{1}{2}(3^{n+1}+1)})$ is a weakly regular bent function on $\mathbb{F}_{3^n}$ whose dual is given by*

$$g(b) = \begin{cases} \mathrm{Tr}(\frac{b^2}{a}) & \text{if } x - \frac{b^3}{a}x^3 + a^2x^9 \text{ has 1 or 9 roots in } \mathbb{F}_{3^n}, \\ -\mathrm{Tr}(\frac{b^2}{a}) & \text{if } x - \frac{b^3}{a}x^3 + a^2x^9 \text{ has 3 roots in } \mathbb{F}_{3^n}. \end{cases} \tag{3.13}$$

A Universal Formula

2015

Theorem 1

For any $a \in \mathbb{F}_{3^n}^*$ and $\lambda \in \mathbb{F}_{3^n}$, we have

$$\sum_{x \in \mathbb{F}_{3^n}} \omega_3^{Tr_1^n(ax^d+\lambda x)} = (-1)^{n+1}\eta(a)i^n\omega_3^{g(\lambda)}3^{n/2},$$

where η is the quadratic character of $\mathbb{F}_{3^n}$, and

$$g(\lambda) = \eta(a) \sum_{j:\mathrm{wt}(j)+\mathrm{wt}(-jd)=n+1} \sigma(j)\sigma(-jd)\left(\frac{a}{\lambda^d}\right)^j,$$

where $a/\lambda^d = 0$ if $\lambda = 0$.

A Universal Formula (Cont.)

- $q = p^n$
- For any $0 \leqslant k < q-1$, let $k = k_0 + k_1 p + \cdots + k_{n-1} p^{n-1}$ be the p-adic representation of k, where $0 \leqslant k_i < p$ for $i = 0, 1, \ldots, n-1$.
- $\mathrm{wt}(k) = k_0 + k_1 + \cdots + k_{n-1}$
- $\sigma(k) = k_0! k_1! \cdots k_{n-1}!$
- For any j, $\mathrm{wt}(j) = \mathrm{wt}(\bar{j})$, and $\sigma(j) = \sigma(\bar{j})$, where $0 \leqslant \bar{j} < q-1$ and $j \equiv \bar{j} \pmod{q-1}$.

Regular Bent

2015

Theorem 2

If n is even and $\eta(a) = -(-1)^{n/2}$, then $Tr_1^n(ax^d)$ is a **regular** *bent function.*

Two Constructions of Simple Form

- 2015
- $\mathbb{F}_{3^n}$
- $n = 3t + 1, k = 2t + 1$ with $t \geqslant 1$, $a \in \mathbb{F}_{3^n}^*$, the new bent function is

$$f(x) = Tr_1^n \left(-\frac{x^{3^{2t+1}+3^{t+1}+2}}{a^{3^{2t+1}+3^{t+1}+1}} - \frac{x^{3^{2t}+1}}{a^{-3^{2t}+3^t+1}} + \frac{x^2}{a^{-3^{2t+1}+3^{t+1}+1}} \right)$$

- Degree: 4

Two Constructions of Simple Form (Cont.)

- 2015
- $\mathbb{F}_{3^n}$
- $n = 3t + 2, k = 2t + 1$ with $t \geqslant 1$, $a \in \mathbb{F}_{3^n}^*$, the new bent function is

$$f(x) = Tr_1^n \left(-\frac{x^{3^{2t+2}+1}}{a^{3^{2t+2}-3^{t+1}+3}} - \frac{x^{2\cdot 3^{2t+1}+3^{t+1}+1}}{a^{3^{2t+2}+3^{t+1}+1}} + \frac{x^2}{a^{-3^{2t+2}+3^{t+1}+3}} \right)$$

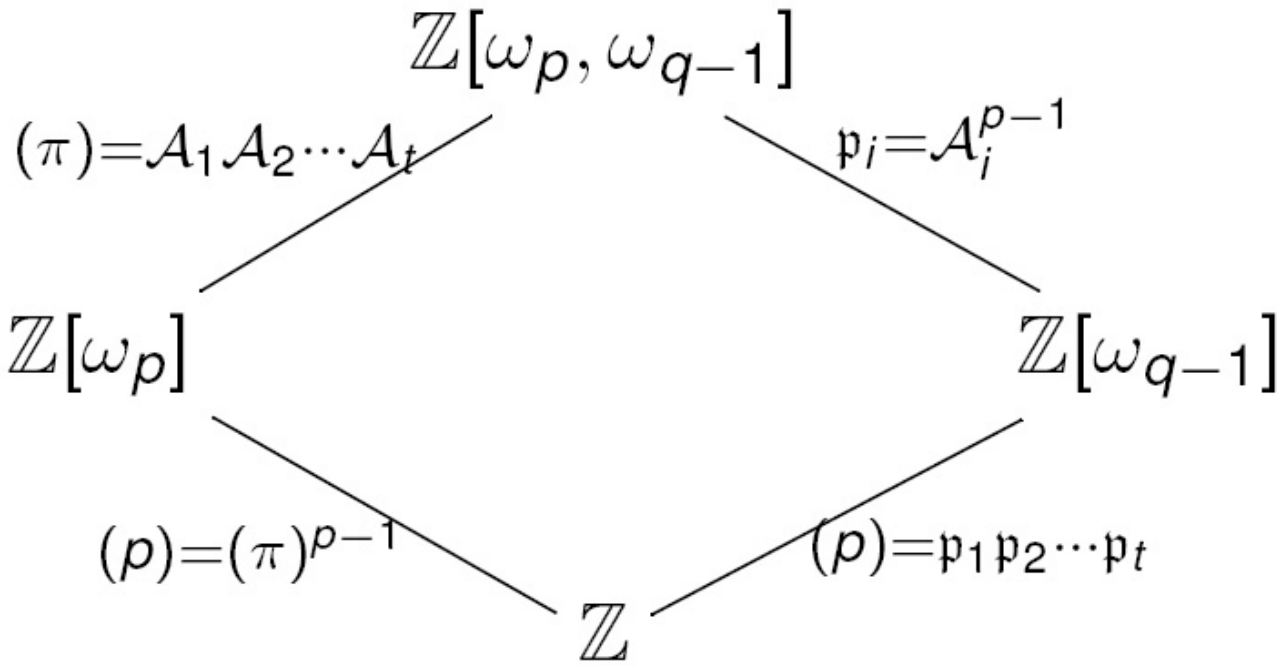
- Degree: 4

Gauss Sums over Finite Fields

- ψ: $\psi(x) = \omega_p^{\mathrm{Tr}_1^n(x)}$, additive character
- χ: multiplicative character of $\mathbb{F}_q$
- For any multiplicative character χ over $\mathbb{F}_q$, the Gauss sum $G(\chi)$ over $\mathbb{F}_q$ is defined by

$$G(\chi) = \sum_{x \in \mathbb{F}_q} \psi(x)\chi(x).$$

Prime Ideal Factorization



Algebraic Integer Rings

- In $\mathbb{Z}$: p is a prime number (can not be factored).
- In $\mathbb{Z}$: (p) is a prime ideal.

- In $\mathbb{Z}[\omega_p]$: let $\pi = \omega_p - 1$, (π) is a prime ideal.
- In $\mathbb{Z}[\omega_p]$: $(p) = (\pi)^{p-1}$ in $\mathbb{Z}[\omega_p]$.

- In $\mathbb{Z}[\omega_p, \omega_{q-1}]$: $(\pi) = \mathcal{A}_1\mathcal{A}_2\cdots\mathcal{A}_t$ in $\mathbb{Z}[\omega_p, \omega_{q-1}]$, where $\mathcal{A}_i$ are prime ideals in $\mathbb{Z}[\omega_p, \omega_{q-1}]$, and $t = \phi(q-1)/n$.

Algebraic Integer Rings and Finite Fields

- For each $\mathcal{A}_i$, $\mathbb{Z}[\omega_p, \omega_{q-1}]/\mathcal{A}_i \cong \mathbb{F}_q$
- There exists one multiplicative character χ on $\mathbb{F}_q$ satisfying

$$\chi(x) \pmod{\mathcal{A}} = x$$

  where $x \in \mathbb{Z}[\omega_p, \omega_{q-1}]/\mathcal{A} \cong \mathbb{F}_q$.
- This character is called the Teichmüller character, and we denote it by $\chi_{\mathfrak{p}}$.

Gauss Sums Again

- For any $x \in \mathbb{F}_q$, $\psi(x) \in \mathbb{Z}[\omega_p]$.
- For any $x \in \mathbb{F}_q$, $\chi(x) \in \mathbb{Z}[\omega_{q-1}]$.
- $G(\chi) = \sum_{x \in \mathbb{F}_q} \psi(x)\chi(x) \in \mathbb{Z}[\omega_p, \omega_{q-1}]$.

Stickelberger's Theorem

- For any $0 \leqslant k < q-1$, we have

$$G(\chi_{\mathfrak{p}}^{-k}) \equiv -\frac{\pi^{\mathrm{wt}(k)}}{\sigma(k)} \pmod{\pi^{\mathrm{wt}(k)+p-1}}.$$

- Let $e = \lfloor \mathrm{wt}(k)/(p-1) \rfloor$.
- Then $p^e \| G(\chi_{\mathfrak{p}}^{-k})$ for any $0 < k < q-1$ by Stickelberger's theorem.
- Because $(\pi) = \mathcal{A}_1 \mathcal{A}_2 \cdots \mathcal{A}_t$, we have

$$G(\chi_{\mathfrak{p}}^{-k}) \equiv -\frac{\pi^{\mathrm{wt}(k)}}{\sigma(k)} \pmod{\mathcal{A}^{\mathrm{wt}(k)+p-1}}$$

for any $0 \leqslant k < q-1$.

One Lemma

2015

Lemma 3

1) $\mathrm{wt}(j)+\mathrm{wt}(-jd) \geqslant n$ *for any* $0<j<3^n-1$, *and* $j=(3^n-1)/2$ *is the only value such that* $\mathrm{wt}(j)+\mathrm{wt}(-jd)=n$.

2) Moreover, $\mathrm{wt}(j)+\mathrm{wt}(-jd)=n+1$ *if and only if one of the following two conditions holds:*

(i) $\mathrm{wt}(j)+\mathrm{wt}(3^k j)=\mathrm{wt}((3^k+1)j)$ *and* $2\mathrm{wt}(-jd)=\mathrm{wt}(-(3^k+1)j)+2$;
(ii) $\mathrm{wt}(j)+\mathrm{wt}(3^k j)=\mathrm{wt}((3^k+1)j)+2$ *and* $2\mathrm{wt}(-jd)=\mathrm{wt}(-(3^k+1)j)$.

Cyclotomic Cosets Modulo $3^n - 1$

- For any $0 \leqslant s < 3^n - 1$, let n_s be the smallest positive integer such that $s \equiv s3^{n_s} (\text{mod } 3^n - 1)$.
- The cyclotomic coset C_s modulo $3^n - 1$ is defined to be the set

$$C_s = \{s, 3s, ..., 3^{n_s - 1}s\}.$$

- Assume that s is the smallest integer in C_s. Then s is called the coset leader of C_s.
- $n = 2$, the cyclotomic cosets modulo 8 are:

$$C_0 = \{0\}, C_1 = \{1, 3\}, C_2 = \{2, 6\}, C_4 = \{4\}, C_5 = \{5, 7\}.$$

- $\{0, 1, 2, 4, 5\}$ are coset leaders modulo 8.

The Main Problem

$$\{j|0 \leqslant j < 3^n - 1, \mathrm{wt}(j) + \mathrm{wt}(-jd) = n + 1\}?$$

Complicated computation!

Two Nice Cases

2015

- $n = 3t + 1$, $k = 2t + 1$ with $t \geqslant 1$
- $d = (3^{2t+1} + 1)/2$
- $u = \frac{3^n-1}{2} - 3^{3t} - 3^{2t} - 3^t$
- $v = \frac{3^n-1}{2} - 3^{3t} - 3^{2t} + 3^{t-1}$
- $w = \frac{3^n-1}{2} - 3^{3t} - 3^{2t-1} + 3^{t-1}$

- $C_u \bigcup C_v \bigcup C_w = \{j | 0 \leqslant j < 3^n - 1, \mathrm{wt}(j) + \mathrm{wt}(-jd) = n + 1\}$

- $g(x) = Tr_1^n \left(-\frac{x^{3^{2t+1}+3^{t+1}+2}}{a^{3^{2t+1}+3^{t+1}+1}} - \frac{x^{3^{2t}+1}}{a^{-3^{2t}+3^t+1}} + \frac{x^2}{a^{-3^{2t+1}+3^{t+1}+1}} \right)$

Two Nice Cases (Cont.)

2015

- $n = 3t + 2$, $k = 2t + 1$ with $t \geqslant 1$
- $d = (3^{2t+1} + 1)/2$
- $u = \frac{3^n-1}{2} - 3^{3t+1} - 3^{2t+1} - 3^t$
- $v = \frac{3^n-1}{2} - 3^{3t+1} - 3^{2t+1} + 3^t$
- $w = \frac{3^n-1}{2} - 3^{3t+1} - 3^{2t} + 3^{t-1}$

- $C_u \bigcup C_v \bigcup C_w = \{j | 0 \leqslant j < 3^n - 1, \mathrm{wt}(j) + \mathrm{wt}(-jd) = n + 1\}$

- $g(x) = Tr_1^n \left(- \frac{x^{3^{2t+2}+1}}{a^{3^{2t+2}-3^{t+1}+3}} - \frac{x^{2\cdot 3^{2t+1}+3^{t+1}+1}}{a^{3^{2t+2}+3^{t+1}+1}} + \frac{x^2}{a^{-3^{2t+2}+3^{t+1}+3}} \right)$

The General Case

Case 1:

$$S_0 = \{ j \mid 0 < j < 3^n - 1, \mathrm{wt}(j) + \mathrm{wt}(3^k j) = \mathrm{wt}((3^k+1)j), 2\mathrm{wt}(-jd) = \mathrm{wt}(-(3^k+1)j) + 2 \}$$

Case 2:

$$S_1 = \{ j \mid 0 < j < 3^n - 1, \mathrm{wt}(j) + \mathrm{wt}(3^k j) = \mathrm{wt}((3^k+1)j) + 2, 2\mathrm{wt}(-jd) = \mathrm{wt}(-(3^k+1)j) \}$$

Some Notation

- n, k odd, $\gcd(n, k) = 1$
- $0 < w < n$, $wk \equiv 1 (\mathrm{mod}\ n)$
- $\mathcal{A} = \{0, k, 2k, \cdots, (w-1)k\} (\mathrm{mod}\ n)$

Case 1

$$
\begin{aligned}
U_0 \;=\; \{\, j \mid & j_{ik} = 1 \text{ for } w \leqslant i \leqslant n-1,\ j_{ik} = 0 \text{ for } i \in \{0, w-1\}, \\
& j_{ik} \in \{0,2\} \text{ for } 1 \leqslant i \leqslant w-2, \\
& \text{and no consecutive 2's in } \{j_{ik}\}_{i=1}^{w-2} \,\}
\end{aligned}
$$

$$
\begin{aligned}
U_1 \;=\; \{\, j \mid & j_{ik} = 1 \text{ for } 0 \leqslant i \leqslant w-1,\ j_{ik} = 0 \text{ for } i \in \{w, n-1\}, \\
& j_{ik} \in \{0,2\} \text{ for } w+1 \leqslant i \leqslant n-2, \\
& \text{and no consecutive 2's in } \{j_{ik}\}_{i=w+1}^{n-2} \,\}
\end{aligned}
$$

Case 1 (Cont.)

If $|\mathcal{A} \cap \{n-k, n-k+1, \cdots, n-1\}|$ is even, then

- $S_0 = \bigcup_{j \in U_0} C_j$,
- $|S_0| = n\left(\left(\frac{1+\sqrt{5}}{2}\right)^w - \left(\frac{1-\sqrt{5}}{2}\right)^w\right)/\sqrt{5}$.

If $|\mathcal{A} \cap \{n-k, n-k+1, \cdots, n-1\}|$ is odd, then

- $S_0 = \bigcup_{j \in U_1} C_j$,
- $|S_0| = n\left(\left(\frac{1+\sqrt{5}}{2}\right)^{n-w} - \left(\frac{1-\sqrt{5}}{2}\right)^{n-w}\right)/\sqrt{5}$.

Case 2

$$
\begin{aligned}
V_0 \;=\; \{\, j \mid\; & j_{ik} = 1 \text{ for } w \leqslant i \leqslant n-1, \\
& j_{ik} = 2 \text{ for } i = 0, j_{ik} = 0 \text{ for } i \in \{1, w-1\}, \\
& j_{ik} \in \{0,2\} \text{ for } 2 \leqslant i \leqslant w-2, \\
& \text{and no consecutive 2's in } \{j_{ik}\}_{i=2}^{w-2} \,\}
\end{aligned}
$$

$$
\begin{aligned}
V_1 \;=\; \{\, j \mid\; & j_{ik} = 1 \text{ for } 0 \leqslant i \leqslant w-1,\ j_{ik} = 0 \text{ for } i \in \{w, n-2\}, \\
& j_{ik} \in \{0,2\} \text{ for } w+1 \leqslant i \leqslant n-3,\ j_{ik} = 2 \text{ for } i = n-1, \\
& \text{and no consecutive 2's in } \{j_{ik}\}_{i=w+1}^{n-3} \,\}
\end{aligned}
$$

Case 2 (Cont.)

If $|\mathcal{A} \cap \{n-k, n-k+1, \cdots, n-1\}|$ is even, then

- $S_1 = \bigcup_{j \in V_0} C_j$,
- $|S_1| = n\left(\left(\frac{1+\sqrt{5}}{2}\right)^{w-1} - \left(\frac{1-\sqrt{5}}{2}\right)^{w-1}\right)/\sqrt{5}$.

If $|\mathcal{A} \cap \{n-k, n-k+1, \cdots, n-1\}|$ is odd, then

- $S_1 = \bigcup_{j \in V_1} C_j$,
- $|S_1| = n\left(\left(\frac{1+\sqrt{5}}{2}\right)^{n-w-1} - \left(\frac{1-\sqrt{5}}{2}\right)^{n-w-1}\right)/\sqrt{5}$.

The Coefficients

- If $j \in S_0$, then $\sigma(j)\sigma(-jd) = 2^{N_2(j)+1}$.
- If $j \in S_1$, then $\sigma(j)\sigma(-jd) = 2^{N_2(j)}$.

Main Results

If $|\mathcal{A} \cap \{n-k, n-k+1, \cdots, n-1\}|$ is even, then

- $$\begin{aligned} g(x) &= \sum_{j \in U_0} Tr_1^n \left((-1)^{N_2(j)+1} \eta(a) a^j x^{-jd} \right) \\ &\quad + \sum_{j \in V_0} Tr_1^n \left((-1)^{N_2(j)} \eta(a) a^j x^{-jd} \right), \end{aligned}$$
- $\left(\left(\frac{1+\sqrt{5}}{2} \right)^{w+1} - \left(\frac{1-\sqrt{5}}{2} \right)^{w+1} \right) / \sqrt{5}$ trace terms.

Main Results (Cont.)

If $|\mathcal{A} \cap \{n-k, n-k+1, \cdots, n-1\}|$ is odd, then

- $$\begin{aligned} g(x) &= \sum_{j \in U_1} Tr_1^n \left((-1)^{N_2(j)+1} \eta(a) a^j x^{-jd} \right) \\ &\quad + \sum_{j \in V_1} Tr_1^n \left((-1)^{N_2(j)} \eta(a) a^j x^{-jd} \right), \end{aligned}$$
- $\left(\left(\frac{1+\sqrt{5}}{2} \right)^{n-w+1} - \left(\frac{1-\sqrt{5}}{2} \right)^{n-w+1} \right) / \sqrt{5}$ trace terms.

Example 1

- $n = 8,\ k = 7$
- $d = 1094,\ w = 7$
- $|\mathcal{A} \cap \{n-k, n-k+1, \cdots, n-1\}| = 6$
- $U_0 = \{00000010, 00002010, 00020010, 00200010, 00202010, 02000010, 02002010, 02020010, 20000010, 20002010, 20020010, 20200010, 20202010\}$
- $V_0 = \{00000012, 00002012, 00020012, 00200012, 00202012, 02000012, 02002012, 02020012\}$
- The Coulter-Matthews bent function over $\mathbb{F}_{3^8}$ is $Tr(ax^{1094})$.
-

$$\begin{aligned} g(x) &= \sum_{j \in U_0} Tr_1^n((-1)^{N_2(j)+1}\eta(a)a^j x^{-1094j}) \\ &\quad + \sum_{j \in V_0} Tr_1^n((-1)^{N_2(j)}\eta(a)a^j x^{-1094j}). \end{aligned}$$

- 21 trace terms

Example 2

- $n = 9,\ k = 7$
- $d = 1094,\ w = 4$
- $|\mathcal{A} \cap \{n-k, n-k+1, \cdots, n-1\}| = 3$
- $U_1 = \{010101001, 010121001,\ 012101001, 210101001, 210121001\}$
- $V_1 = \{010101201,\ 012101201, 210101201\}$
- the dual function $g(x)$ of the Coulter-Matthews bent function $Tr(ax^{1094})$ over $\mathbb{F}_{3^9}$
-

$$\begin{aligned} g(x) &= \sum_{j \in U_1} Tr_1^n((-1)^{N_2(j)+1}\eta(a)a^j x^{-1094j}) \\ &\quad + \sum_{j \in V_1} Tr_1^n((-1)^{N_2(j)}\eta(a)a^j x^{-1094j}). \end{aligned}$$

- 8 trace terms

Four Special Cases

- $k|n+1$ and $k>1$
- $k|n-1$ and $k>1$
- $(n-k)|n+1$ and $1<k<n-1$
- $(n-k)|n-1$ and $1<k<n-1$

The Fibonacci Sequence

The number of trace terms:

1, 1, 2, **3**, 5, **8**, 13, **21**, 34, **55**, ...

An Open Problem

- $|\mathcal{A} \cap \{n-k, n-k+1, \cdots, n-1\}|$: even or odd?
- $\mathcal{A} = \{0, k, 2k, \cdots, (w-1)k\} (\text{mod } n)$

Thanks for your attention!