Analysis of APN functions and functions of small differential uniformity from the Maiorana-McFarland class

Nurdagül Anbar
(joint work with Tekgül Kalaycı and Wilfried Meidl)

Sabancı University, İstanbul

15 - 17 September 2020, BFA

$\mathbb{V}_n$: An n-dimensional vector space over $\mathbb{F}_2$
$\langle , \rangle$: A non-degenerate inner product on $\mathbb{V}_n$

In general, $\mathbb{V}_n = \mathbb{F}_2^n$, $\mathbb{F}_{2^n}$ or $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$, $n = 2m$,
and $\langle x, y\rangle = x \cdot y$, $\langle x, y\rangle = \mathrm{Tr}_n(xy)$ or $\langle (x, y), (z, w)\rangle = \mathrm{Tr}_m(xz + yw)$,
respectively, where Tr_n is the absolute trace on $\mathbb{F}_{2^n}$.

Main Interest: Functions $F : \mathbb{V}_n \to \mathbb{V}_n$, their non-linearity and differential uniformity

Recall:
$F_\lambda(X) := \langle F(X), \lambda\rangle : \mathbb{V}_n \mapsto \mathbb{F}_2$: The component function corresponding to $\lambda \in \mathbb{V}_n \setminus \{0\}$
$\mathcal{W}_{F_\lambda}(a) = \sum_{x\in\mathbb{V}_n} (-1)^{F_\lambda(x)+\langle a,x\rangle}$: The Walsh coefficient of F_λ at a

Definition: Non-linearity $\mathcal{NL}(F)$ of F

$$\mathcal{NL}(F) = 2^{n-1} - \frac{1}{2} \max_{a,\lambda\in\mathbb{V}_n,\lambda\neq 0} |\mathcal{W}_{F_\lambda}(a)|$$

$\mathbb{V}_n$: An n-dimensional vector space over $\mathbb{F}_2$
$\langle , \rangle$: A non-degenerate inner product on $\mathbb{V}_n$

In general, $\mathbb{V}_n = \mathbb{F}_2^n$, $\mathbb{F}_{2^n}$ or $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$, $n = 2m$, and $\langle x, y \rangle = x \cdot y$, $\langle x, y \rangle = \mathrm{Tr}_n(xy)$ or $\langle (x,y),(z,w) \rangle = \mathrm{Tr}_m(xz + yw)$, respectively, where Tr_n is the absolute trace on $\mathbb{F}_{2^n}$.

Main Interest: Functions $F : \mathbb{V}_n \to \mathbb{V}_n$, their non-linearity and differential uniformity

Recall:
$F_\lambda(X) := \langle F(X), \lambda \rangle : \mathbb{V}_n \mapsto \mathbb{F}_2$: The component function corresponding to $\lambda \in \mathbb{V}_n \setminus \{0\}$
$\mathcal{W}_{F_\lambda}(a) = \sum_{x \in \mathbb{V}_n} (-1)^{F_\lambda(x) + \langle a, x \rangle}$: The Walsh coefficient of F_λ at a

Definition: Non-linearity $\mathcal{NL}(F)$ of F

$$\mathcal{NL}(F) = 2^{n-1} - \frac{1}{2} \max_{a, \lambda \in \mathbb{V}_n, \lambda \neq 0} |\mathcal{W}_{F_\lambda}(a)|$$

Definition: Derivative of F in the direction $u \in \mathbb{V}_n$ is $D_uF(X) = F(X+u) + F(X)$. F is differentially k-uniform if $D_uF(X) = v$ has at most k solutions for all non-zero $u \in \mathbb{V}_n$.

F is APN if F is differentially 2-uniform.

Objective: The construction of functions $F : \mathbb{V}_n \to \mathbb{V}_n$ with high non-linearity and small differential uniformity

Main Tool: Quadratic Functions

(I) $D_uF(X) + F(u)$ is a linear function ($F(0) = 0$).

(II) $|\mathcal{W}_{F_\lambda}(a)| \in \{0, 2^{(n+s)/2}\}$, where $s = \dim(\Lambda_{F_\lambda})$.

Recall:
$\Lambda_{F_\lambda} = \{u \in \mathbb{V}_n \mid D_uF_\lambda(X) = F_\lambda(X+u) + F_\lambda(X) \text{ is constant}\}$

Definition: Derivative of F in the direction $u \in \mathbb{V}_n$ is $D_uF(X) = F(X+u) + F(X)$. F is differentially k-uniform if $D_uF(X) = v$ has at most k solutions for all non-zero $u \in \mathbb{V}_n$.

F is APN if F is differentially 2-uniform.

Objective: The construction of functions $F : \mathbb{V}_n \to \mathbb{V}_n$ with high non-linearity and small differential uniformity

Main Tool: Quadratic Functions

(I) $D_uF(X) + F(u)$ is a linear function ($F(0) = 0$).

(II) $|\mathcal{W}_{F_\lambda}(a)| \in \{0, 2^{(n+s)/2}\}$, where $s = \dim(\Lambda_{F_\lambda})$.

Recall:
$\Lambda_{F_\lambda} = \{u \in \mathbb{V}_n \mid D_uF_\lambda(X) = F_\lambda(X+u) + F_\lambda(X) \text{ is constant}\}$

Bezout's Theorem:

Let $f(X,Y) \in \bar{\mathbb{F}}[X,Y]$, where $\bar{\mathbb{F}}$ is the algebraic closure $\mathbb{F}_2$. An (affine) curve $\mathcal{X}$ is a zero set of $f(X,Y)$, i.e.,

$$\mathcal{X} = \{P = (x,y) \in \bar{\mathbb{F}} \times \bar{\mathbb{F}} \mid f(x,y) = 0\}.$$

$\deg(\mathcal{X}) = \deg(f(X,Y))$

Let $P = (u,v) \in \mathcal{X}$, i.e., $f(u,v) = 0$.

$$f(X+u, Y+v) = f_m(X,Y) + f_{m+1}(X,Y) + \cdots + f_d(X,Y),$$

where f_i is a form of degree i and $f_m \neq 0$.

$m_P(\mathcal{X}) := m$ multiplicity of P on $\mathcal{X}$

Bezout's Theorem:

Let $f(X,Y) \in \bar{\mathbb{F}}[X,Y]$, where $\bar{\mathbb{F}}$ is the algebraic closure $\mathbb{F}_2$. An (affine) curve $\mathcal{X}$ is a zero set of $f(X,Y)$, i.e.,

$$\mathcal{X} = \{P = (x,y) \in \bar{\mathbb{F}} \times \bar{\mathbb{F}} \mid f(x,y) = 0\}.$$

$\deg(\mathcal{X}) = \deg(f(X,Y))$

Let $P = (u,v) \in \mathcal{X}$, i.e., $f(u,v) = 0$.

$$f(X+u, Y+v) = f_m(X,Y) + f_{m+1}(X,Y) + \cdots + f_d(X,Y),$$

where f_i is a form of degree i and $f_m \neq 0$.

$m_P(\mathcal{X}) := m$ multiplicity of P on $\mathcal{X}$

Bezout's Theorem: Let $\mathcal{X}$ and $\mathcal{Y}$ be two (projective) curves. If $\mathcal{X}$ and $\mathcal{Y}$ do not have a common component, then

$$\sum_{P \in \mathcal{X} \cap \mathcal{Y}} m_P(\mathcal{X}) m_P(\mathcal{Y}) \leq \deg(\mathcal{X})\deg(\mathcal{Y}).$$

Aim: Use Bezout's Theorem to calculate the Walsh spectrum of known infinite classes of quadratic APN functions.

Example: $F(X,Y) = (XY, G(X,Y)) : \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \mapsto \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$

(I) $G(X,Y) = \alpha X^{2^i+2^j} + \beta X^{2^i} Y^{2^j} + \gamma X^{2^j} Y^{2^i} + \zeta X^{2^i+1}$ (Carlet, 2011)

(II) $G(X,Y) = X^{2^i+1} + \alpha Y^{(2^i+1)2^j}$ (Pott-Zhou, 2013)

(III) $G(X,Y) = X^{2^{3i}+2^{2i}} + \alpha X^{2^{2i}} Y^{2^i} + \beta Y^{2^i+1}$ (Taniguchi, 2019)

Bezout's Theorem: Let $\mathcal{X}$ and $\mathcal{Y}$ be two (projective) curves. If $\mathcal{X}$ and $\mathcal{Y}$ do not have a common component, then

$$\sum_{P \in \mathcal{X} \cap \mathcal{Y}} m_P(\mathcal{X}) m_P(\mathcal{Y}) \leq \deg(\mathcal{X}) \deg(\mathcal{Y}).$$

Aim: Use Bezout's Theorem to calculate the Walsh spectrum of known infinite classes of quadratic APN functions.

Example: $F(X,Y) = (XY, G(X,Y)) : \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \mapsto \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$

(I) $G(X,Y) = \alpha X^{2^i+2^j} + \beta X^{2^i} Y^{2^j} + \gamma X^{2^j} Y^{2^i} + \zeta X^{2^i+1}$ (Carlet, 2011)

(II) $G(X,Y) = X^{2^i+1} + \alpha Y^{(2^i+1)2^j}$ (Pott-Zhou, 2013)

(III) $G(X,Y) = X^{2^{3i}+2^{2i}} + \alpha X^{2^{2i}} Y^{2^i} + \beta Y^{2^i+1}$ (Taniguchi, 2019)

Theorem (Anbar, Kalayci, Meidl, 2019):

Taniguchi's APN functions F have the classical spectrum, i.e., a component of F is either bent or semibent.

Idea of the proof:

For $\lambda, \mu \in \mathbb{F}_{2^m}$, let $F_{\lambda,\mu} = \mathrm{Tr}_m(\lambda XY + \mu G(X,Y))$.

Aim: To determine the dimension over $\mathbb{F}_2$ of the linear space of $F_{\lambda,\mu}$, i.e.,

$$\Lambda = \{(u,v) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} | D_{(u,v)} F_{\lambda,\mu}(X,Y) \text{ is constant on } \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}\}.$$

Set

$$\tilde{\Lambda} = \{(u,v) \in \mathbb{F}_{2^{mi}} \times \mathbb{F}_{2^{mi}} | D_{(u,v)} F_{\lambda,\mu}(X,Y) \text{ is constant on } \mathbb{F}_{2^{mi}} \times \mathbb{F}_{2^{mi}}\}.$$

Observation: $\gcd(i,m) = 1 \Longrightarrow \dim_{\mathbb{F}_2}(\Lambda) = \dim_{\mathbb{F}_{2^i}}(\tilde{\Lambda})$

Theorem (Anbar, Kalayci, Meidl, 2019):

Taniguchi's APN functions F have the classical spectrum, i.e., a component of F is either bent or semibent.

Idea of the proof:

For $\lambda, \mu \in \mathbb{F}_{2^m}$, let $F_{\lambda,\mu} = \mathrm{Tr}_m(\lambda XY + \mu G(X,Y))$.

Aim: To determine the dimension over $\mathbb{F}_2$ of the linear space of $F_{\lambda,\mu}$, i.e.,

$$\Lambda = \{(u,v) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} | D_{(u,v)} F_{\lambda,\mu}(X,Y) \text{ is constant on } \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}\}.$$

Set

$$\tilde{\Lambda} = \{(u,v) \in \mathbb{F}_{2^{mi}} \times \mathbb{F}_{2^{mi}} | D_{(u,v)} F_{\lambda,\mu}(X,Y) \text{ is constant on } \mathbb{F}_{2^{mi}} \times \mathbb{F}_{2^{mi}}\}.$$

Observation: $\gcd(i,m) = 1 \Longrightarrow \dim_{\mathbb{F}_2}(\Lambda) = \dim_{\mathbb{F}_{2^i}}(\tilde{\Lambda})$

Theorem (Anbar, Kalayci, Meidl, 2019):

Taniguchi's APN functions F have the classical spectrum, i.e., a component of F is either bent or semibent.

Idea of the proof:

For $\lambda, \mu \in \mathbb{F}_{2^m}$, let $F_{\lambda,\mu} = \mathrm{Tr}_m(\lambda XY + \mu G(X,Y))$.

Aim: To determine the dimension over $\mathbb{F}_2$ of the linear space of $F_{\lambda,\mu}$, i.e.,

$$\Lambda = \{(u,v) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} | D_{(u,v)} F_{\lambda,\mu}(X,Y) \text{ is constant on } \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}\}.$$

Set

$$\tilde{\Lambda} = \{(u,v) \in \mathbb{F}_{2^{mi}} \times \mathbb{F}_{2^{mi}} | D_{(u,v)} F_{\lambda,\mu}(X,Y) \text{ is constant on } \mathbb{F}_{2^{mi}} \times \mathbb{F}_{2^{mi}}\}.$$

Observation: $\gcd(i,m) = 1 \Longrightarrow \dim_{\mathbb{F}_2}(\Lambda) = \dim_{\mathbb{F}_{2^i}}(\tilde{\Lambda})$

$(u,v) \in \tilde{\Lambda}$ if and only if

$$D_{(u,v)}F_{\lambda,\mu}(X,Y) + F_{\lambda,\mu}(u,v) = \mathrm{Tr}_m(f_1 X^{2^i}) + \mathrm{Tr}_m(f_2 Y^{2^i}) = 0$$

for all $X, Y \in \mathbb{F}_{2^m}$, where
$f_1 = f_1(u,v) = \mu^{2^{-2i}}u + \mu^{2^{-i}}\alpha^{2^{-i}}v + \lambda^{2^i}v^{2^i} + \mu^{2^{-2i}}u^{2^{2i}}$ and
$f_2 = f_2(u,v) = \mu\beta v + \lambda^{2^i}u^{2^i} + \mu\alpha u^{2^{2i}} + \mu^{2^i}\beta^{2^i}v^{2^{2i}}$.

That is, $(u,v) \in \tilde{\Lambda} \iff f_1(u,v) = f_2(u,v) = 0$.

For $\mu \neq 0$, let $\mathcal{X}_1$ and $\mathcal{X}_2$ be the curves defined by f_1 and f_2, respectively.

$P_1 = (0:1:0)$ and $P_2 = ((\mu\beta)^{2^{-i}} : (\mu\alpha)^{2^{-2i}} : 0)$ are the unique points of $\mathcal{X}_1$ and $\mathcal{X}_2$ at infinity, respectively.

$\beta \neq 0 \implies P_1 \neq P_2 \implies \mathcal{X}_1$ and $\mathcal{X}_2$ do not have a common component.

$\implies |\tilde{\Lambda}| = |\mathcal{X}_1 \cap \mathcal{X}_2| \leq \deg(\mathcal{X}_1)\deg(\mathcal{X}_2) = 2^{4i}$ by Bezout's Theorem

$\implies \dim_{\mathbb{F}_2}(\Lambda) = 0$, 2 or 4

$(u,v) \in \tilde{\Lambda}$ if and only if

$$D_{(u,v)}F_{\lambda,\mu}(X,Y) + F_{\lambda,\mu}(u,v) = \mathrm{Tr}_m(f_1X^{2^i}) + \mathrm{Tr}_m(f_2Y^{2^i}) = 0$$

for all $X, Y \in \mathbb{F}_{2^m}$, where
$f_1 = f_1(u,v) = \mu^{2^{-2i}}u + \mu^{2^{-i}}\alpha^{2^{-i}}v + \lambda^{2^i}v^{2^i} + \mu^{2^{-2i}}u^{2^{2i}}$ and
$f_2 = f_2(u,v) = \mu\beta v + \lambda^{2^i}u^{2^i} + \mu\alpha u^{2^{2i}} + \mu^{2^i}\beta^{2^i}v^{2^{2i}}$.

That is, $(u,v) \in \tilde{\Lambda} \iff f_1(u,v) = f_2(u,v) = 0$.

For $\mu \neq 0$, let $\mathcal{X}_1$ and $\mathcal{X}_2$ be the curves defined by f_1 and f_2, respectively.

$P_1 = (0:1:0)$ and $P_2 = ((\mu\beta)^{2^{-i}} : (\mu\alpha)^{2^{-2i}} : 0)$ are the unique points of $\mathcal{X}_1$ and $\mathcal{X}_2$ at infinity, respectively.

$\beta \neq 0 \Longrightarrow P_1 \neq P_2 \Longrightarrow \mathcal{X}_1$ and $\mathcal{X}_2$ do not have a common component.

$\Longrightarrow |\tilde{\Lambda}| = |\mathcal{X}_1 \cap \mathcal{X}_2| \leq \deg(\mathcal{X}_1)\deg(\mathcal{X}_2) = 2^{4i}$ by Bezout's Theorem

$\Longrightarrow \dim_{\mathbb{F}_2}(\Lambda) = 0$, 2 or 4

$(u, v) \in \tilde{\Lambda}$ if and only if

$$D_{(u,v)}F_{\lambda,\mu}(X, Y) + F_{\lambda,\mu}(u, v) = \mathrm{Tr}_m(f_1 X^{2^i}) + \mathrm{Tr}_m(f_2 Y^{2^i}) = 0$$

for all $X, Y \in \mathbb{F}_{2^m}$, where
$f_1 = f_1(u, v) = \mu^{2^{-2i}} u + \mu^{2^{-i}} \alpha^{2^{-i}} v + \lambda^{2^i} v^{2^i} + \mu^{2^{-2i}} u^{2^{2i}}$ and
$f_2 = f_2(u, v) = \mu\beta v + \lambda^{2^i} u^{2^i} + \mu\alpha u^{2^{2i}} + \mu^{2^i} \beta^{2^i} v^{2^{2i}}$.

That is, $(u, v) \in \tilde{\Lambda} \Longleftrightarrow f_1(u, v) = f_2(u, v) = 0$.

For $\mu \neq 0$, let $\mathcal{X}_1$ and $\mathcal{X}_2$ be the curves defined by f_1 and f_2, respectively.

$P_1 = (0 : 1 : 0)$ and $P_2 = ((\mu\beta)^{2^{-i}} : (\mu\alpha)^{2^{-2i}} : 0)$ are the unique points of $\mathcal{X}_1$ and $\mathcal{X}_2$ at infinity, respectively.

$\beta \neq 0 \Longrightarrow P_1 \neq P_2 \Longrightarrow \mathcal{X}_1$ and $\mathcal{X}_2$ do not have a common component.

$\Longrightarrow |\tilde{\Lambda}| = |\mathcal{X}_1 \cap \mathcal{X}_2| \leq \deg(\mathcal{X}_1)\deg(\mathcal{X}_2) = 2^{4i}$ by Bezout's Theorem

$\Longrightarrow \dim_{\mathbb{F}_2}(\Lambda) = 0$, 2 or 4

Suppose that $\dim_{\mathbb{F}_2}(\Lambda) = 4$, i.e., $\mathcal{X}_1$ and $\mathcal{X}_2$ intersects at exactly 2^{4i} affine points.

Set $g_1(X,Y) = f_1 f_2$ and $g_2(X,Y) = X f_1 + f_2$. Let $\mathcal{Y}_1$ and $\mathcal{Y}_2$ be the curves defined by g_1 and g_2, respectively.

Then

(I) $\mathcal{Y}_1$ and $\mathcal{Y}_2$ are curves without a common component of degrees 2^{2i+1} and $2^{2i}+1$, respectively.

(II) $P \in \mathcal{X}_1 \cap \mathcal{X}_2 \Longrightarrow P \in \mathcal{Y}_1 \cap \mathcal{Y}_2$ and $m_P(\mathcal{Y}_1) \geq 2$.

(III) $P_1 = (0:1:0) \in \mathcal{Y}_1 \cap \mathcal{Y}_2$ with $m_P(\mathcal{Y}_1) = 2^{2i}$ and $m_P(\mathcal{Y}_2) = 2^{2i}+1$.

$\Longrightarrow \sum_{P \in \mathcal{Y}_1 \cap \mathcal{Y}_2} m_P(\mathcal{Y}_1) m_P(\mathcal{Y}_2) \geq 2^{4i+1} + 2^{2i}(2^{2i}+1) > \deg(\mathcal{Y}_1)\deg(\mathcal{Y}_2)$, which is a contradiction to Bezout's Theorem.

□

Remark: Similarly, one obtains simple proof for the Walsh spectrum of Carlet's and Pott-Zhou APN functions.

Suppose that $\dim_{\mathbb{F}_2}(\Lambda) = 4$, i.e., $\mathcal{X}_1$ and $\mathcal{X}_2$ intersects at exactly 2^{4i} affine points.

Set $g_1(X,Y) = f_1 f_2$ and $g_2(X,Y) = Xf_1 + f_2$. Let $\mathcal{Y}_1$ and $\mathcal{Y}_2$ be the curves defined by g_1 and g_2, respectively.

Then

(I) $\mathcal{Y}_1$ and $\mathcal{Y}_2$ are curves without a common component of degrees 2^{2i+1} and $2^{2i}+1$, respectively.

(II) $P \in \mathcal{X}_1 \cap \mathcal{X}_2 \implies P \in \mathcal{Y}_1 \cap \mathcal{Y}_2$ and $m_P(\mathcal{Y}_1) \geq 2$.

(III) $P_1 = (0:1:0) \in \mathcal{Y}_1 \cap \mathcal{Y}_2$ with $m_P(\mathcal{Y}_1) = 2^{2i}$ and $m_P(\mathcal{Y}_2) = 2^{2i}+1$.

$\implies \sum_{P \in \mathcal{Y}_1 \cap \mathcal{Y}_2} m_P(\mathcal{Y}_1) m_P(\mathcal{Y}_2) \geq 2^{4i+1} + 2^{2i}(2^{2i}+1) > \deg(\mathcal{Y}_1)\deg(\mathcal{Y}_2)$, which is a contradiction to Bezout's Theorem.

□

Remark: Similarly, one obtains simple proof for the Walsh spectrum of Carlet's and Pott-Zhou APN functions.

Suppose that $\dim_{\mathbb{F}_2}(\Lambda) = 4$, i.e., $\mathcal{X}_1$ and $\mathcal{X}_2$ intersects at exactly 2^{4i} affine points.

Set $g_1(X,Y) = f_1 f_2$ and $g_2(X,Y) = X f_1 + f_2$. Let $\mathcal{Y}_1$ and $\mathcal{Y}_2$ be the curves defined by g_1 and g_2, respectively.

Then

(I) $\mathcal{Y}_1$ and $\mathcal{Y}_2$ are curves without a common component of degrees 2^{2i+1} and $2^{2i}+1$, respectively.

(II) $P \in \mathcal{X}_1 \cap \mathcal{X}_2 \Longrightarrow P \in \mathcal{Y}_1 \cap \mathcal{Y}_2$ and $m_P(\mathcal{Y}_1) \geq 2$.

(III) $P_1 = (0:1:0) \in \mathcal{Y}_1 \cap \mathcal{Y}_2$ with $m_P(\mathcal{Y}_1) = 2^{2i}$ and $m_P(\mathcal{Y}_2) = 2^{2i}+1$.

$\Longrightarrow \sum_{P \in \mathcal{Y}_1 \cap \mathcal{Y}_2} m_P(\mathcal{Y}_1) m_P(\mathcal{Y}_2) \geq 2^{4i+1} + 2^{2i}(2^{2i}+1) > \deg(\mathcal{Y}_1)\deg(\mathcal{Y}_2)$, which is a contradiction to Bezout's Theorem.

□

Remark: Similarly, one obtains simple proof for the Walsh spectrum of Carlet's and Pott-Zhou APN functions.

Suppose that $\dim_{\mathbb{F}_2}(\Lambda) = 4$, i.e., $\mathcal{X}_1$ and $\mathcal{X}_2$ intersects at exactly 2^{4i} affine points.

Set $g_1(X,Y) = f_1 f_2$ and $g_2(X,Y) = Xf_1 + f_2$. Let $\mathcal{Y}_1$ and $\mathcal{Y}_2$ be the curves defined by g_1 and g_2, respectively.

Then

(I) $\mathcal{Y}_1$ and $\mathcal{Y}_2$ are curves without a common component of degrees 2^{2i+1} and $2^{2i}+1$, respectively.

(II) $P \in \mathcal{X}_1 \cap \mathcal{X}_2 \Longrightarrow P \in \mathcal{Y}_1 \cap \mathcal{Y}_2$ and $m_P(\mathcal{Y}_1) \geq 2$.

(III) $P_1 = (0:1:0) \in \mathcal{Y}_1 \cap \mathcal{Y}_2$ with $m_P(\mathcal{Y}_1) = 2^{2i}$ and $m_P(\mathcal{Y}_2) = 2^{2i}+1$.

$\Longrightarrow \sum_{P \in \mathcal{Y}_1 \cap \mathcal{Y}_2} m_P(\mathcal{Y}_1) m_P(\mathcal{Y}_2) \geq 2^{4i+1} + 2^{2i}(2^{2i}+1) > \deg(\mathcal{Y}_1)\deg(\mathcal{Y}_2)$, which is a contradiction to Bezout's Theorem.

□

Remark: Similarly, one obtains simple proof for the Walsh spectrum of Carlet's and Pott-Zhou APN functions.

Suppose that $\dim_{\mathbb{F}_2}(\Lambda) = 4$, i.e., $\mathcal{X}_1$ and $\mathcal{X}_2$ intersects at exactly 2^{4i} affine points.

Set $g_1(X,Y) = f_1 f_2$ and $g_2(X,Y) = Xf_1 + f_2$. Let $\mathcal{Y}_1$ and $\mathcal{Y}_2$ be the curves defined by g_1 and g_2, respectively.

Then

(I) $\mathcal{Y}_1$ and $\mathcal{Y}_2$ are curves without a common component of degrees 2^{2i+1} and $2^{2i}+1$, respectively.

(II) $P \in \mathcal{X}_1 \cap \mathcal{X}_2 \Longrightarrow P \in \mathcal{Y}_1 \cap \mathcal{Y}_2$ and $m_P(\mathcal{Y}_1) \geq 2$.

(III) $P_1 = (0:1:0) \in \mathcal{Y}_1 \cap \mathcal{Y}_2$ with $m_P(\mathcal{Y}_1) = 2^{2i}$ and $m_P(\mathcal{Y}_2) = 2^{2i}+1$.

$\Longrightarrow \sum_{P \in \mathcal{Y}_1 \cap \mathcal{Y}_2} m_P(\mathcal{Y}_1) m_P(\mathcal{Y}_2) \geq 2^{4i+1} + 2^{2i}(2^{2i}+1) > \deg(\mathcal{Y}_1)\deg(\mathcal{Y}_2)$, which is a contradiction to Bezout's Theorem.

□

Remark: Similarly, one obtains simple proof for the Walsh spectrum of Carlet's and Pott-Zhou APN functions.

Common Phenomena: Many quadratic APN and differentially 4-uniform functions have a large amount of bent components.

Recall: Carlet, Pott-Zhou and Taniguchi use Maiorana-McFarland bent function $F(X, Y) = XY$.

Idea: To use functions having many bent components to construct functions having small differential uniformity.

Theorem:(Pott et al., 2018) A function $\mathcal{F} : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, $n = 2m$, can have at most $2^n - 2^m$ bent components. Moreover, $\mathcal{F}(X) = X^{2^r}\mathrm{Tr}_m^n(X) = X^{2^r}(X + X^{2^m})$ has $2^n - 2^m$ bent components. $\mathcal{F}_\gamma$ is bent for $\gamma \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^m}$, i.e., $F(X) = \mathrm{Tr}_m^n(\gamma\mathcal{F}(X))$ is a vectorial bent function.

Remark: For $r = 0$, $\mathcal{F}$ is equivalent to X^{2^m+1}.

Common Phenomena: Many quadratic APN and differentially 4-uniform functions have a large amount of bent components.

Recall: Carlet, Pott-Zhou and Taniguchi use Maiorana-McFarland bent function $F(X, Y) = XY$.

Idea: To use functions having many bent components to construct functions having small differential uniformity.

Theorem:(Pott et al., 2018) A function $\mathcal{F} : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, $n = 2m$, can have at most $2^n - 2^m$ bent components. Moreover, $\mathcal{F}(X) = X^{2^r}\mathrm{Tr}^n_m(X) = X^{2^r}(X + X^{2^m})$ has $2^n - 2^m$ bent components. $\mathcal{F}_\gamma$ is bent for $\gamma \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^m}$, i.e., $F(X) = \mathrm{Tr}^n_m(\gamma\mathcal{F}(X))$ is a vectorial bent function.

Remark: For $r = 0$, $\mathcal{F}$ is equivalent to X^{2^m+1}.

Common Phenomena: Many quadratic APN and differentially 4-uniform functions have a large amount of bent components.

Recall: Carlet, Pott-Zhou and Taniguchi use Maiorana-McFarland bent function $F(X,Y) = XY$.

Idea: To use functions having many bent components to construct functions having small differential uniformity.

Theorem:(Pott et al., 2018) A function $\mathcal{F} : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, $n = 2m$, can have at most $2^n - 2^m$ bent components. Moreover, $\mathcal{F}(X) = X^{2^r} \mathrm{Tr}_m^n(X) = X^{2^r}(X + X^{2^m})$ has $2^n - 2^m$ bent components. $\mathcal{F}_\gamma$ is bent for $\gamma \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^m}$, i.e., $F(X) = \mathrm{Tr}_m^n(\gamma \mathcal{F}(X))$ is a vectorial bent function.

Remark: For $r = 0$, $\mathcal{F}$ is equivalent to X^{2^m+1}.

Theorem:(Mesnager et al., 2019)

(I) Having the maximum number of bent components invariant under the CCZ-equivalence.

(II) $\mathcal{F}(X) = X^{2^r}\mathrm{Tr}_m^n(X + \sum_{j=1}^{\sigma} \alpha_j X^{2^{t_j}})$, $\alpha_j \in \mathbb{F}_{2^m}$, has the maximum number of bent components if $\mathcal{A}_1 = 1 + \sum_{j=1}^{\sigma} \alpha_j^{2^{m-t_j}} X^{2^{m-t_j}-1}$ and $\mathcal{A}_2 = 1 + \sum_{j=1}^{\sigma} \alpha_j^{2^{m-r}} X^{2^{t_j}-1}$ has no zero in $\mathbb{F}_{2^m}$. $\mathcal{F}_\gamma$ is bent for $\gamma \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^m}$.

Theorem:(Anbar, Kalaycı, Meidl, 2020)

(I) Let $F : \mathbb{F}_{2^n} \mapsto \mathbb{F}_{2^n}$, $n = 2m$, be a plateaued vectorial function with the maximal number of bent components. Then the non-linearity of F is at most $2^{n-1} - 2^{\lfloor \frac{n+m}{2} \rfloor}$.

(II) $\mathcal{F}(X) = X^{2^r}\mathrm{Tr}_m^n(\Lambda(X))$ on $\mathbb{F}_{2^n}$, where $\Lambda \in \mathbb{F}_{2^m}[X]$ linearized, have maximal number of bent components if and only if Λ is a permutation of $\mathbb{F}_{2^m}$.

Aim: Investigate the differential uniformity and non-linearity of functions $H(X) = (F(X), G(X)) : \mathbb{F}_{2^n} \mapsto \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ for $F(X) = \mathrm{Tr}_m^n(\gamma\mathcal{F}(X))$, $\gamma \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^m}$.

Theorem:(Mesnager et al., 2019)

(I) Having the maximum number of bent components invariant under the CCZ-equivalence.

(II) $\mathcal{F}(X) = X^{2^r}\mathrm{Tr}_m^n(X + \sum_{j=1}^{\sigma} \alpha_j X^{2^{t_j}})$, $\alpha_j \in \mathbb{F}_{2^m}$, has the maximum number of bent components if $\mathcal{A}_1 = 1 + \sum_{j=1}^{\sigma} \alpha_j^{2^{m-t_j}} X^{2^{m-t_j}-1}$ and $\mathcal{A}_2 = 1 + \sum_{j=1}^{\sigma} \alpha_j^{2^{m-r}} X^{2^{t_j}-1}$ has no zero in $\mathbb{F}_{2^m}$. $\mathcal{F}_\gamma$ is bent for $\gamma \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^m}$.

Theorem:(Anbar, Kalaycı, Meidl, 2020)

(I) Let $F : \mathbb{F}_{2^n} \mapsto \mathbb{F}_{2^n}$, $n = 2m$, be a plateaued vectorial function with the maximal number of bent components. Then the non-linearity of F is at most $2^{n-1} - 2^{\lfloor \frac{n+m}{2} \rfloor}$.

(II) $\mathcal{F}(X) = X^{2^r}\mathrm{Tr}_m^n(\Lambda(X))$ on $\mathbb{F}_{2^n}$, where $\Lambda \in \mathbb{F}_{2^m}[X]$ linearized, have maximal number of bent components if and only if Λ is a permutation of $\mathbb{F}_{2^m}$.

Aim: Investigate the differential uniformity and non-linearity of functions $H(X) = (F(X), G(X)) : \mathbb{F}_{2^n} \mapsto \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ for $F(X) = \mathrm{Tr}_m^n(\gamma\mathcal{F}(X))$, $\gamma \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^m}$.

Theorem:(Mesnager et al., 2019)

(I) Having the maximum number of bent components invariant under the CCZ-equivalence.

(II) $\mathcal{F}(X) = X^{2^r}\mathrm{Tr}_m^n(X + \sum_{j=1}^{\sigma} \alpha_j X^{2^{t_j}})$, $\alpha_j \in \mathbb{F}_{2^m}$, has the maximum number of bent components if $\mathcal{A}_1 = 1 + \sum_{j=1}^{\sigma} \alpha_j^{2^{m-t_j}} X^{2^{m-t_j}-1}$ and $\mathcal{A}_2 = 1 + \sum_{j=1}^{\sigma} \alpha_j^{2^{m-r}} X^{2^{t_j}-1}$ has no zero in $\mathbb{F}_{2^m}$. $\mathcal{F}_\gamma$ is bent for $\gamma \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^m}$.

Theorem:(Anbar, Kalaycı, Meidl, 2020)

(I) Let $F : \mathbb{F}_{2^n} \mapsto \mathbb{F}_{2^n}$, $n = 2m$, be a plateaued vectorial function with the maximal number of bent components. Then the non-linearity of F is at most $2^{n-1} - 2^{\lfloor \frac{n+m}{2} \rfloor}$.

(II) $\mathcal{F}(X) = X^{2^r}\mathrm{Tr}_m^n(\Lambda(X))$ on $\mathbb{F}_{2^n}$, where $\Lambda \in \mathbb{F}_{2^m}[X]$ linearized, have maximal number of bent components if and only if Λ is a permutation of $\mathbb{F}_{2^m}$.

Aim: Investigate the differential uniformity and non-linearity of functions $H(X) = (F(X), G(X)) : \mathbb{F}_{2^n} \mapsto \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ for $F(X) = \mathrm{Tr}_m^n(\gamma \mathcal{F}(X))$, $\gamma \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^m}$.

The Solution Space of $D_uF(X) + F(u) = F(X+u) + F(X) + F(u) = 0$:

For $z \in \mathbb{F}_{2^m}$, set $U_z = \{x \in \mathbb{F}_{2^n} \mid \mathrm{Tr}_m^n(\gamma x) + z\mathrm{Tr}_m^n(\Lambda(x)) = 0\}$.

Lemma: Let $F(X) = \mathrm{Tr}_m^n(\gamma X^{2^r}\mathrm{Tr}_m^n(\Lambda(X)))$. The solution space of $D_uF(X) + F(u) = 0$ is

(I) $\mathbb{F}_{2^m}$ if and only if $u \in \mathbb{F}_{2^m}^*$, and

(II) U_z if and only if $u \in U_z$.

(III) $U_0 = \beta\mathbb{F}_{2^m}$, where $\beta = \gamma^{2^{-r}}$.

(IV) $\alpha \in U_z$, $z \neq 0$, if and only if $c\alpha \in U_{c^{2^r-1}z}$.

Corollary: $\mathbb{F}_{2^m}$ and the subspaces U_z, $z \in \mathbb{F}_{2^m}$, form a spread of $\mathbb{F}_{2^n}$.

Remark: Let $F(X) = \mathrm{Tr}_m^n(\gamma X^3)$, m odd and γ non-cube. Set $S_u = \{x \in \mathbb{F}_{2^n} \mid D_uF(x) + F(u) = 0\}$. By Bezout's Theorem, if $u \neq v$, then $|S_u \cap S_v| \leq 4$.

We investigate $H(X) = (F(X), G(X))$ for $G(X) = \mathrm{Tr}_m^n\left(\sigma X^{2^i+1}\right)$ and $G(X) = \mathrm{Tr}_m^n(\sigma X^{2^i+1} + \tau X^{2^{m+i}+1})$.

The Solution Space of $D_uF(X) + F(u) = F(X+u) + F(X) + F(u) = 0$:

For $z \in \mathbb{F}_{2^m}$, set $U_z = \{x \in \mathbb{F}_{2^n} \mid \mathrm{Tr}^n_m(\gamma x) + z\mathrm{Tr}^n_m(\Lambda(x)) = 0\}$.

Lemma: Let $F(X) = \mathrm{Tr}^n_m(\gamma X^{2^r}\mathrm{Tr}^n_m(\Lambda(X)))$. The solution space of $D_uF(X) + F(u) = 0$ is

(I) $\mathbb{F}_{2^m}$ if and only if $u \in \mathbb{F}^*_{2^m}$, and

(II) U_z if and only if $u \in U_z$.

(III) $U_0 = \beta\mathbb{F}_{2^m}$, where $\beta = \gamma^{2^{-r}}$.

(IV) $\alpha \in U_z$, $z \neq 0$, if and only if $c\alpha \in U_{c^{2^r-1}z}$.

Corollary: $\mathbb{F}_{2^m}$ and the subspaces U_z, $z \in \mathbb{F}_{2^m}$, form a spread of $\mathbb{F}_{2^n}$.

Remark: Let $F(X) = \mathrm{Tr}^n_m(\gamma X^3)$, m odd and γ non-cube. Set $S_u = \{x \in \mathbb{F}_{2^n} \mid D_uF(x) + F(u) = 0\}$. By Bezout's Theorem, if $u \neq v$, then $|S_u \cap S_v| \leq 4$.

We investigate $H(X) = (F(X), G(X))$ for $G(X) = \mathrm{Tr}^n_m\left(\sigma X^{2^i+1}\right)$ and $G(X) = \mathrm{Tr}^n_m(\sigma X^{2^i+1} + \tau X^{2^{m+i}+1})$.

The Solution Space of $D_uF(X) + F(u) = F(X+u) + F(X) + F(u) = 0$:

For $z \in \mathbb{F}_{2^m}$, set $U_z = \{x \in \mathbb{F}_{2^n} \mid \mathrm{Tr}_m^n(\gamma x) + z\mathrm{Tr}_m^n(\Lambda(x)) = 0\}$.

Lemma: Let $F(X) = \mathrm{Tr}_m^n(\gamma X^{2^r}\mathrm{Tr}_m^n(\Lambda(X)))$. The solution space of $D_uF(X) + F(u) = 0$ is

(I) $\mathbb{F}_{2^m}$ if and only if $u \in \mathbb{F}_{2^m}^*$, and

(II) U_z if and only if $u \in U_z$.

(III) $U_0 = \beta\mathbb{F}_{2^m}$, where $\beta = \gamma^{2^{-r}}$.

(IV) $\alpha \in U_z$, $z \neq 0$, if and only if $c\alpha \in U_{c^{2^r-1}z}$.

Corollary: $\mathbb{F}_{2^m}$ and the subspaces U_z, $z \in \mathbb{F}_{2^m}$, form a spread of $\mathbb{F}_{2^n}$.

Remark: Let $F(X) = \mathrm{Tr}_m^n(\gamma X^3)$, m odd and γ non-cube. Set $S_u = \{x \in \mathbb{F}_{2^n} \mid D_uF(x) + F(u) = 0\}$. By Bezout's Theorem, if $u \neq v$, then $|S_u \cap S_v| \leq 4$.

We investigate $H(X) = (F(X), G(X))$ for $G(X) = \mathrm{Tr}_m^n\left(\sigma X^{2^i+1}\right)$ and $G(X) = \mathrm{Tr}_m^n(\sigma X^{2^i+1} + \tau X^{2^{m+i}+1})$.

The Solution Space of $D_uF(X) + F(u) = F(X+u) + F(X) + F(u) = 0$:

For $z \in \mathbb{F}_{2^m}$, set $U_z = \{x \in \mathbb{F}_{2^n} \mid \mathrm{Tr}_m^n(\gamma x) + z\mathrm{Tr}_m^n(\Lambda(x)) = 0\}$.

Lemma: Let $F(X) = \mathrm{Tr}_m^n(\gamma X^{2^r}\mathrm{Tr}_m^n(\Lambda(X)))$. The solution space of $D_uF(X) + F(u) = 0$ is

(I) $\mathbb{F}_{2^m}$ if and only if $u \in \mathbb{F}_{2^m}^*$, and

(II) U_z if and only if $u \in U_z$.

(III) $U_0 = \beta\mathbb{F}_{2^m}$, where $\beta = \gamma^{2^{-r}}$.

(IV) $\alpha \in U_z$, $z \neq 0$, if and only if $c\alpha \in U_{c^{2^r-1}z}$.

Corollary: $\mathbb{F}_{2^m}$ and the subspaces U_z, $z \in \mathbb{F}_{2^m}$, form a spread of $\mathbb{F}_{2^n}$.

Remark: Let $F(X) = \mathrm{Tr}_m^n(\gamma X^3)$, m odd and γ non-cube. Set $S_u = \{x \in \mathbb{F}_{2^n} \mid D_uF(x) + F(u) = 0\}$. By Bezout's Theorem, if $u \neq v$, then $|S_u \cap S_v| \leq 4$.

We investigate $H(X) = (F(X), G(X))$ for $G(X) = \mathrm{Tr}_m^n\left(\sigma X^{2^i+1}\right)$ and $G(X) = \mathrm{Tr}_m^n(\sigma X^{2^i+1} + \tau X^{2^{m+i}+1})$.

Theorem (Anbar, Kalayci, Meidl, 2020):

Let $\gamma, \sigma \in \mathbb{F}_{2^n}$, where $n = 2m$ for an odd integer m, and r be a positive integer relatively prime to m. If
$\gamma, \sigma, \sigma\gamma^{-(2^r+1)2^r}, \sigma\gamma^{-1}, \gamma^{2^r}\sigma^{-(2^r-1)} \notin \mathbb{F}_{2^m}$ and $\gamma^{-1} \notin U_1^{2^r-1}$, then

$$H(X) = \left(\mathrm{Tr}_m^n\left(\gamma X^{2^r}(X + X^{2^m})\right), \mathrm{Tr}_m^n\left(\sigma X^{2^r+1}\right)\right)$$

is differentially 4-uniform and has the classical spectrum.

Theorem (Anbar, Kalayci, Meidl, 2020):

Let $\gcd(r, m) = 1$, $\gamma \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^m}$, $\tau \in \mathbb{F}_{2^m}^*$ such that $\tau^{-1} \neq \mathrm{Tr}_m^n(\gamma^{-1})$, and $\sigma = \gamma + \tau$. Then

$$H(X) = (\mathrm{Tr}_m^n(\gamma X^{2^r}\mathrm{Tr}_m^n(X)), \mathrm{Tr}_m^n(\sigma X^{2^r+1} + \tau X^{2^{m+r}+1}))$$

is differentially $2^{2\gcd(m,2)}$-uniform, and any component function of H is at most $2\gcd(2, m)$-plateaued. In particular, if m is odd, then $H(X)$ is differentially 4-uniform and has the classical spectrum.

We wish you healthy days!