On derivatives of Balanced Boolean functions and quadratic APN functions

A. Musukwa, M. Sala and M. Zaninelli

Department of Mathematics, University of Trento

BFA 2019 Florence, Italy
1 Preliminaries

2 Linear space of Balanced Boolean functions

3 Linear space of components for APN functions

4 Quadratic APN functions

5 Quadratic power functions
Outline

1 Preliminaries

2 Linear space of Balanced Boolean functions

3 Linear space of components for APN functions

4 Quadratic APN functions

5 Quadratic power functions
Outline

1 Preliminaries

2 Linear space of Balanced Boolean functions

3 Linear space of components for APN functions

4 Quadratic APN functions

5 Quadratic power functions
1 Preliminaries

2 Linear space of Balanced Boolean functions

3 Linear space of components for APN functions

4 Quadratic APN functions

5 Quadratic power functions
## Preliminaries

### Definitions and notations

- A function from $\mathbb{F}^n$ to $\mathbb{F}$ ($= \mathbb{F}_2 = \{0, 1\}$) is a **Boolean function (Bf)**. A set of all functions is denoted by $B_n$.

- ANF for Bf: $f(x_1, \ldots, x_n) = \sum_{u \in \mathbb{F}^n} a_u \prod_{i=1}^{n} x_i^{u_i}$ where $a_u \in \mathbb{F}$

- A function from $\mathbb{F}^n$ to $\mathbb{F}^n$ is a **vectorial Boolean function (vBf)**.

- vBf: $F := (f_1, \ldots, f_n)$ where $f_i$ (in $B_n$) are called **coordinate functions**.

- A **component** of vBf $F$ is $F_\lambda = \lambda \cdot F$, with $\lambda \neq 0 \in \mathbb{F}^n$. 

---

**A. Musukwa et. al.**

On derivatives of Balanced functions and APN functions
Definitions and notations

- A function from $\mathbb{F}^n$ to $\mathbb{F}$ ($= \mathbb{F}_2 = \{0, 1\}$) is a **Boolean function** ($Bf$). A set of all functions is denoted by $B_n$.

- ANF for $Bf$: $f(x_1, \ldots, x_n) = \sum_{u \in \mathbb{F}^n} a_u \prod_{i=1}^n x_i^{u_i}$ where $a_u \in \mathbb{F}$

- A function from $\mathbb{F}^n$ to $\mathbb{F}^n$ is a **vectorial Boolean function** ($vBf$).

- $vBf$: $F := (f_1, \ldots, f_n)$ where $f_i$ (in $B_n$) are called **coordinate functions**.

- A component of $vBf$ $F$ is $F_\lambda = \lambda \cdot F$, with $\lambda \neq 0 \in \mathbb{F}^n$. 

A. Musukwa et. al. 
On derivatives of Balanced functions and APN functions

A. Musukwa et. al. 
On derivatives of Balanced functions and APN functions
Definitions and notations

- A function from $\mathbb{F}^n$ to $\mathbb{F}$ ($= \mathbb{F}_2 = \{0, 1\}$) is a **Boolean function (Bf)**. A set of all functions is denoted by $B_n$

- ANF for Bf: $f(x_1, ..., x_n) = \sum_{u \in \mathbb{F}^n} a_u \prod_{i=1}^{n} x_i^{u_i}$ where $a_u \in \mathbb{F}$

- A function from $\mathbb{F}^n$ to $\mathbb{F}^n$ is a **vectorial Boolean function (vBf)**

- vBf: $F := (f_1, ..., f_n)$ where $f_i$ (in $B_n$) are called **coordinate functions**

- A component of vBf $F$ is $F_\lambda = \lambda \cdot F$, with $\lambda \neq 0 \in \mathbb{F}^n$
Definitions and notations

- A function from $\mathbb{F}^n$ to $\mathbb{F}$ ($= \mathbb{F}_2 = \{0, 1\}$) is a **Boolean function (Bf)**. A set of all functions is denoted by $B_n$

- ANF for Bf: $f(x_1, \ldots, x_n) = \sum_{u \in \mathbb{F}^n} a_u \prod_{i=1}^n x_i^{u_i}$ where $a_u \in \mathbb{F}$

- A function from $\mathbb{F}^n$ to $\mathbb{F}^n$ is a **vectorial Boolean function (vBf)**

- vBf: $F := (f_1, \ldots, f_n)$ where $f_i$ (in $B_n$) are called **coordinate functions**

- A component of vBf $F$ is $F_\lambda = \lambda \cdot F$, with $\lambda \neq 0 \in \mathbb{F}^n$
Preliminaries

Definitions and notations

- A function from $\mathbb{F}^n$ to $\mathbb{F}$ ($= \mathbb{F}_2 = \{0, 1\}$) is a **Boolean function (Bf)**. A set of all functions is denoted by $B_n$.

- ANF for Bf: $f(x_1, \ldots, x_n) = \sum_{u \in \mathbb{F}^n} a_u \prod_{i=1}^n x_i^{u_i}$ where $a_u \in \mathbb{F}$

- A function from $\mathbb{F}^n$ to $\mathbb{F}^n$ is a **vectorial Boolean function (vBf)**

- vBf: $F := (f_1, \ldots, f_n)$ where $f_i$ (in $B_n$) are called **coordinate functions**

- A **component** of vBf $F$ is $F_\lambda = \lambda \cdot F$, with $\lambda \neq 0 \in \mathbb{F}^n$
Definitions and notations

- $\deg(f) = \max_{a_u \neq 0} w(u)$ and $\deg(F) = \max_{\lambda \in \mathbb{F}^n} \deg(F_\lambda)$
- Weight of $f$: $w(f) = |\{x \in \mathbb{F}^n | f(x) = 1\}|$
- Balanced: $w(f) = 2^{n-1}$
- Affine functions: $A_n = \{g \in B_n | \deg(g) \leq 1\}$. 

A. Musukwa et. al. 
On derivatives of Balanced functions and APN functions
Definitions and notations

- \( \deg(f) = \max_{a_u \neq 0} w(u) \) and \( \deg(F) = \max_{\lambda \in \mathbb{F}^n} \deg(F_{\lambda}) \)

- **Weight of** \( f \): \( w(f) = |\{x \in \mathbb{F}^n | f(x) = 1\}| \)

- **Balanced**: \( w(f) = 2^{n-1} \)

- **Affine functions**: \( A_n = \{g \in B_n | \deg(g) \leq 1\} \).
Preliminaries

Definitions and notations

- \( \deg(f) = \max_{a_u \neq 0} w(u) \) and \( \deg(F) = \max_{\lambda \in \mathbb{F}^n} \deg(F_\lambda) \)

- **Weight of** \( f \): \( w(f) = |\{x \in \mathbb{F}^n | f(x) = 1\}| \)

- **Balanced**: \( w(f) = 2^{n-1} \)

- **Affine functions**: \( A_n = \{g \in B_n | \deg(g) \leq 1\} \).
Definitions and notations

- \( \deg(f) = \max_{a_u \neq 0} w(u) \) and \( \deg(F) = \max_{\lambda \in \mathbb{F}^n} \deg(F_\lambda) \)

- **Weight of** \( f \): \( w(f) = |\{x \in \mathbb{F}^n | f(x) = 1\}| \)

- **Balanced**: \( w(f) = 2^{n-1} \)

- **Affine functions**: \( A_n = \{g \in B_n | \deg(g) \leq 1\} \)
Definitions and notations

- **Walsh Transform** of $f$: \( \mathcal{W}_f(a) = \sum_{x \in \mathbb{F}^n} (-1)^{f(x) + a \cdot x}, \) with $a \in \mathbb{F}^n$

- **Walsh Spectrum** of $f$: \{ $\mathcal{W}_f(a)$ | $a \in \mathbb{F}^n$ \}

- **Walsh Spectrum** of $vBf$ $F$: \{ $\mathcal{W}_{F,\lambda}(a)$ | $a, \lambda \in \mathbb{F}^n$ \}

- **Bent**: \( \mathcal{W}_f(a) = \pm 2^{n/2}, \) for all $a \in \mathbb{F}^n$ and $n$ even

- **Semi-bent** $f$: $\mathcal{W}_f(a) \in \{0, \pm 2^{(n+1)/2}\}$, for all $a \in \mathbb{F}^n$ and $n$ odd, $\mathcal{W}_f(a) \in \{0, \pm 2^{(n+2)/2}\}$, for all $a \in \mathbb{F}^n$ and $n$ even

- **Plateaued**: $\mathcal{W}_f(a) \in \{0, \pm \mu\}$, for some integer $\mu$. 
Preliminaries

Definitions and notations

- **Walsh Transform** of $f$: $W_f(a) = \sum_{x \in \mathbb{F}_n} (-1)^{f(x) + a \cdot x}$, with $a \in \mathbb{F}_n$

- **Walsh Spectrum** of $Bf$ $f$: $\{W_f(a) \mid a \in \mathbb{F}_n\}$

- **Walsh Spectrum** of $vBf$ $F$: $\{W_{F,\lambda}(a) \mid a, \lambda \in \mathbb{F}_n\}$

- **Bent**: $W_f(a) = \pm 2^{n/2}$, for all $a \in \mathbb{F}_n$ and $n$ even

- **Semi-bent** $f$: $W_f(a) \in \{0, \pm 2^{(n+1)/2}\}$, for all $a \in \mathbb{F}_n$ and $n$ odd, $W_f(a) \in \{0, \pm 2^{(n+2)/2}\}$, for all $a \in \mathbb{F}_n$ and $n$ even

- **Plateaued**: $W_f(a) \in \{0, \pm \mu\}$, for some integer $\mu$. 
Preliminaries

Definitions and notations

- **Walsh Transform** of \( f \): \( \mathcal{W}_f(a) = \sum_{x \in \mathbb{F}^n} (-1)^{f(x) + a \cdot x} \), with \( a \in \mathbb{F}^n \)

- **Walsh Spectrum** of \( Bf \): \( \{ \mathcal{W}_f(a) \mid a \in \mathbb{F}^n \} \)

- **Walsh Spectrum** of \( vBf \): \( \{ \mathcal{W}_{F,\lambda}(a) \mid a, \lambda \in \mathbb{F}^n \} \)

- **Bent**: \( \mathcal{W}_f(a) = \pm 2^{n/2} \), for all \( a \in \mathbb{F}^n \) and \( n \) even

- **Semi-bent** \( f \): \( \mathcal{W}_f(a) \in \{0, \pm 2^{(n+1)/2}\} \), for all \( a \in \mathbb{F}^n \) and \( n \) odd, \( \mathcal{W}_f(a) \in \{0, \pm 2^{(n+2)/2}\} \), for all \( a \in \mathbb{F}^n \) and \( n \) even

- **Plateaued**: \( \mathcal{W}_f(a) \in \{0, \pm \mu\} \), for some integer \( \mu \).
Definitions and notations

- **Walsh Transform** of $f$: $W_f(a) = \sum_{x \in \mathbb{F}^n} (-1)^{f(x)+a \cdot x}$, with $a \in \mathbb{F}^n$

- **Walsh Spectrum** of $Bf$ $f$: \{ $W_f(a) \mid a \in \mathbb{F}^n$ \}

- **Walsh Spectrum** of $vBf$ $F$: \{ $W_{F,\lambda}(a) \mid a, \lambda \in \mathbb{F}^n$ \}

- **Bent**: $W_f(a) = \pm 2^{n/2}$, for all $a \in \mathbb{F}^n$ and $n$ even

- **Semi-bent** $f$: $W_f(a) \in \{0, \pm 2^{(n+1)/2}\}$, for all $a \in \mathbb{F}^n$ and $n$ odd, $W_f(a) \in \{0, \pm 2^{(n+2)/2}\}$, for all $a \in \mathbb{F}^n$ and $n$ even

- **Plateaued**: $W_f(a) \in \{0, \pm \mu\}$, for some integer $\mu$. 
### Preliminaries

#### Definitions and notations

- **Walsh Transform** of $f$: $W_f(a) = \sum_{x \in \mathbb{F}^n} (-1)^{f(x) + a \cdot x}$, with $a \in \mathbb{F}^n$

- **Walsh Spectrum** of $Bf$ $f$: $\{ W_f(a) | a \in \mathbb{F}^n \}$

- **Walsh Spectrum** of $vBf$ $F$: $\{ W_{F,\lambda}(a) | a, \lambda \in \mathbb{F}^n \}$

- **Bent:** $W_f(a) = \pm 2^{n/2}$, for all $a \in \mathbb{F}^n$ and $n$ even

- **Semi-bent $f$:** $W_f(a) \in \{0, \pm 2^{(n+1)/2}\}$, for all $a \in \mathbb{F}^n$ and $n$ odd, $W_f(a) \in \{0, \pm 2^{(n+2)/2}\}$, for all $a \in \mathbb{F}^n$ and $n$ even

- **Plateaued:** $W_f(a) \in \{0, \pm \mu\}$, for some integer $\mu$. 

---

*A. Musukwa et al.*

*On derivatives of Balanced functions and APN functions*
Preliminaries

Definitions and notations

- **Walsh Transform** of $f$: $\mathcal{W}_f(a) = \sum_{x \in \mathbb{F}^n} (-1)^{f(x)+a \cdot x}$, with $a \in \mathbb{F}^n$

- **Walsh Spectrum** of Bf $f$: $\{ \mathcal{W}_f(a) \mid a \in \mathbb{F}^n \}$

- **Walsh Spectrum** of vBf $F$: $\{ \mathcal{W}_{F,\lambda}(a) \mid a, \lambda \in \mathbb{F}^n \}$

- **Bent**: $\mathcal{W}_f(a) = \pm 2^{n/2}$, for all $a \in \mathbb{F}^n$ and $n$ even

- **Semi-bent $f$**: $\mathcal{W}_f(a) \in \{0, \pm 2^{(n+1)/2}\}$, for all $a \in \mathbb{F}^n$ and $n$ odd, $\mathcal{W}_f(a) \in \{0, \pm 2^{(n+2)/2}\}$, for all $a \in \mathbb{F}^n$ and $n$ even

- **Plateaued**: $\mathcal{W}_f(a) \in \{0, \pm \mu\}$, for some integer $\mu$. 
Preliminaries

Affine Equivalence

- \( f \) and \( g \) are **affine equivalent** if there is an affinity \( \varphi : \mathbb{F}^n \to \mathbb{F}^n \) such that \( f = g \circ \varphi \). Write \( f \sim_A g \).

Proposition

Let \( f, g \in B_n \) be such that \( f \sim_A g \). Then \( w(f) = w(g) \).
Preliminaries

Affine Equivalence

- $f$ and $g$ are **affine equivalent** if there is an affinity $\varphi : \mathbb{F}^n \to \mathbb{F}^n$ such that $f = g \circ \varphi$. Write $f \sim_A g$.

Proposition

Let $f, g \in B_n$ be such that $f \sim_A g$. Then $w(f) = w(g)$. 

Theorem

Let $f \in B_n$ be a quadratic Boolean function. Then

(i) $f \sim_A x_1x_2 + \cdots + x_{2i-1}x_{2i} + x_{2i+1}$ with $i \leq \lfloor \frac{n-1}{2} \rfloor$, if $f$ is balanced,

(ii) $f \sim_A x_1x_2 + \cdots + x_{2i-1}x_{2i} + c$, with $c \in \mathbb{F}$ and $i \leq \lfloor \frac{n}{2} \rfloor$, if $f$ is unbalanced.

Lemma

Two (unbalanced) quadratic Bf’s $g$ and $h$ on $\mathbb{F}^n$ are affine equivalent if and only if $w(g) = w(h)$. 
Theorem

Let $f \in B_n$ be a quadratic Boolean function. Then

(i) $f \sim_A x_1x_2 + \cdots + x_{2i-1}x_{2i} + x_{2i+1}$ with $i \leq \lfloor \frac{n-1}{2} \rfloor$, if $f$ is balanced,

(ii) $f \sim_A x_1x_2 + \cdots + x_{2i-1}x_{2i} + c$, with $c \in \mathbb{F}$ and $i \leq \lfloor \frac{n}{2} \rfloor$, if $f$ is unbalanced.

Lemma

Two (unbalanced) quadratic Bf’s $g$ and $h$ on $\mathbb{F}^n$ are affine equivalent if and only if $\mathbf{w}(g) = \mathbf{w}(h)$.
Theorem

Let $f \in B_n$ be a quadratic Boolean function. Then

(i) $f \sim_A x_1x_2 + \cdots + x_{2i-1}x_{2i} + x_{2i+1}$ with $i \leq \left\lfloor \frac{n-1}{2} \right\rfloor$, if $f$ is balanced,

(ii) $f \sim_A x_1x_2 + \cdots + x_{2i-1}x_{2i} + c$, with $c \in \mathbb{F}$ and $i \leq \left\lfloor \frac{n}{2} \right\rfloor$, if $f$ is unbalanced.

Lemma

Two (unbalanced) quadratic Bf's $g$ and $h$ on $\mathbb{F}^n$ are affine equivalent if and only if $w(g) = w(h)$.
**Theorem**

Let $f \in B_n$ be a quadratic Boolean function. Then

(i) $f \sim_A x_1x_2 + \cdots + x_{2i-1}x_{2i} + x_{2i+1}$ with $i \leq \lfloor \frac{n-1}{2} \rfloor$, if $f$ is balanced,

(ii) $f \sim_A x_1x_2 + \cdots + x_{2i-1}x_{2i} + c$, with $c \in \mathbb{F}$ and $i \leq \lfloor \frac{n}{2} \rfloor$, if $f$ is unbalanced.

**Lemma**

Two (unbalanced) quadratic Bf’s $g$ and $h$ on $\mathbb{F}^n$ are affine equivalent if and only if $w(g) = w(h)$. 
Proposition

If \( g(x_1, ..., x_{n-1}) \) is an arbitrary Bf then \( f = g(x_1, ..., x_{n-1}) + x_n \) is balanced.

(First order) derivative of \( f \) at \( a \) in \( \mathbb{F}^n \):
\[
D_a f = f(x + a) + f(x)
\]

Theorem

\( f \in B_n \) is bent if and only if \( D_a f \) is balanced for any nonzero \( a \in \mathbb{F}^n \).
Preliminaries

**Proposition**
If \( g(x_1, ..., x_{n-1}) \) is an arbitrary Bf then \( f = g(x_1, ..., x_{n-1}) + x_n \) is balanced.

**Theorem**
\( f \in B_n \) is bent if and only if \( D_a f \) is balanced for any nonzero \( a \in \mathbb{F}^n \).

(First order) derivative of \( f \) at \( a \) in \( \mathbb{F}^n \): \( D_a f = f(x + a) + f(x) \)
**Proposition**

If \( g(x_1, ..., x_{n-1}) \) is an arbitrary Bf then \( f = g(x_1, ..., x_{n-1}) + x_n \) is balanced.

**Theorem**

\( f \in B_n \) is bent if and only if \( D_a f \) is balanced for any nonzero \( a \in F^n \).
Definitions

- \( a \in \mathbb{F}^n \) is a **linear structure** of \( f \) if \( D_a f \) is a constant.
- We call the set of all linear structures of \( f \) the **linear space** of \( f \) and its denoted by \( V(f) \).
- If the only linear structure of \( f \) is \( a = 0 \), we say the linear space is **trivial**.
- Let \( \Gamma(f) = \{ a \in \mathbb{F}^n \mid D_a f \text{ is balanced} \} \).
- **Almost Perfect Nonlinear (APN):** a \( \nu \)BF \( F \) with \( \delta(F) = 2 \) where

\[
\delta(F) = \max_{a \neq 0, b \in \mathbb{F}^n} |\{ x \in \mathbb{F}^n \mid D_a F(x) = b \}|.
\]
 Definitions

- \( a \in \mathbb{F}^n \) is a **linear structure** of \( f \) if \( D_a f \) is a constant.
- We call the set of all linear structures of \( f \) the **linear space** of \( f \) and its denoted by \( V(f) \).
- If the only linear structure of \( f \) is \( a = 0 \), we say the linear space is **trivial**.
- Let \( \Gamma(f) = \{ a \in \mathbb{F}^n \mid D_a f \text{ is balanced} \} \).
- **Almost Perfect Nonlinear (APN):** a vBf \( F \) with \( \delta(F) = 2 \) where

\[
\delta(F) = \max_{a \neq 0, b \in \mathbb{F}^n} |\{ x \in \mathbb{F}^n \mid D_a F(x) = b \}|.
\]
Preliminary

Definitions

- \( a \in \mathbb{F}^n \) is a **linear structure** of \( f \) if \( D_a f \) is a constant.
- We call the set of all linear structures of \( f \) the **linear space** of \( f \) and its denoted by \( V(f) \).
- If the only linear structure of \( f \) is \( a = 0 \), we say the linear space is **trivial**.
- Let \( \Gamma(f) = \{ a \in \mathbb{F}^n \mid D_a f \text{ is balanced} \} \).
- **Almost Perfect Nonlinear (APN)**: a \( \nu \mathcal{B} f \) \( F \) with \( \delta(F) = 2 \) where

\[
\delta(F) = \max_{a \neq 0, b \in \mathbb{F}^n} \left| \{ x \in \mathbb{F}^n \mid D_a F(x) = b \} \right|.
\]
Definitions

- $a \in \mathbb{F}^n$ is a **linear structure** of $f$ if $Da f$ is a constant.
- We call the set of all linear structures of $f$ the **linear space** of $f$ and its denoted by $V(f)$.
- If the only linear structure of $f$ is $a = 0$, we say the linear space is **trivial**.
- Let $\Gamma(f) = \{ a \in \mathbb{F}^n \mid Da f \text{ is balanced} \}$.
- **Almost Perfect Nonlinear (APN):** a vBf $F$ with $\delta(F) = 2$ where
  $$\delta(F) = \max_{a \neq 0, b \in \mathbb{F}^n} |\{ x \in \mathbb{F}^n \mid Da F(x) = b \}|.$$
Definitions

- $a \in \mathbb{F}^n$ is a **linear structure** of $f$ if $D_a f$ is a constant.
- We call the set of all linear structures of $f$ the **linear space** of $f$ and its denoted by $V(f)$.
- If the only linear structure of $f$ is $a = 0$, we say the linear space is **trivial**.
- Let $\Gamma(f) = \{ a \in \mathbb{F}^n \mid D_a f \text{ is balanced} \}$.
- **Almost Perfect Nonlinear (APN):** a vBf $F$ with $\delta(F) = 2$ where
  \[
  \delta(F) = \max_{a \neq 0, b \in \mathbb{F}^n} |\{ x \in \mathbb{F}^n \mid D_a F(x) = b \}|.
  \]
Another vBf representation

Univariate polynomial over $\mathbb{F}_{2^n}$:

$$F(x) = \sum_{i=0}^{2^n-1} \delta_i x^i,$$

where $\delta_i \in \mathbb{F}_{2^n}$ and the degree of $F$ is at most $2^n - 1$.

Power function: $F(x) = x^d$, for some positive integer $d$.

Quadratic power function: is a power function with $d = 2^i + 2^j$ with $i, j \geq 0$, $i \neq j$. 

Quadratic power functions
Quadratic power functions

Another vBf representation

Univariate polynomial over $\mathbb{F}_{2^n}$:

$$F(x) = \sum_{i=0}^{2^n-1} \delta_i x^i,$$

where $\delta_i \in \mathbb{F}_{2^n}$ and the degree of $F$ is at most $2^n - 1$.

Power function: $F(x) = x^d$, for some positive integer $d$.

Quadratic power function: is a power function with $d = 2^i + 2^j$ with $i, j \geq 0, i \neq j$. 

A. Musukwa et. al. On derivatives of Balanced functions and APN functions
Another vBf representation

Univariate polynomial over $\mathbb{F}_{2^n}$:

$$F(x) = \sum_{i=0}^{2^n-1} \delta_i x^i,$$

where $\delta_i \in \mathbb{F}_{2^n}$ and the degree of $F$ is at most $2^n - 1$.

Power function: $F(x) = x^d$, for some positive integer $d$.

Quadratic power function: is a power function with $d = 2^i + 2^j$ with $i, j \geq 0$, $i \neq j$. 
Observation

- Any Bf can be expressed as:
  \[ f = x_{n+1}g(x_1, ..., x_n) + h(x_1, ..., x_n). \]
- If \( f \) in \( B_n \) only depends on \( m \) variables \( (m < n) \), then \( f|_{\mathbb{F}^m} \) denotes its restriction to these \( m \) variables.

Theorem

If \( f = x_{n+1}g(x_1, ..., x_n) + h(x_1, ..., x_n) \), then

1. \( w(f) = w((g + h)|_{\mathbb{F}^n}) + w(g|_{\mathbb{F}^n}) \),
2. \( f \) is balanced if \( g + h \) and \( h \) are both balanced,
3. \( f \) is unbalanced if one in \( \{g + h, h\} \) is balanced and another one not.
Observation

- Any $Bf$ can be expressed as:
  \[ f = x_{n+1}g(x_1, ..., x_n) + h(x_1, ..., x_n). \]
- If $f$ in $B_n$ only depends on $m$ variables ($m < n$), then $f\mid_{F^m}$ denotes its restriction to these $m$ variables.

Theorem

If $f = x_{n+1}g(x_1, ..., x_n) + h(x_1, ..., x_n)$, then

1. $w(f) = w((g + h)\mid_{F^n}) + w(g\mid_{F^n})$,
2. $f$ is balanced if $g + h$ and $h$ are both balanced,
3. $f$ is unbalanced if one in $\{g + h, h\}$ is balanced and another one not.
**Linear space of Balanced functions**

**Observation**
- Any Bf can be expressed as:
  \[ f = x_{n+1}g(x_1, ..., x_n) + h(x_1, ..., x_n). \]
- If \( f \) in \( B_n \) only depends on \( m \) variables \( (m < n) \), then \( f|_{\mathbb{F}_m} \) denotes its restriction to these \( m \) variables.

**Theorem**
If \( f = x_{n+1}g(x_1, ..., x_n) + h(x_1, ..., x_n) \), then

1. \( w(f) = w((g + h)|_{\mathbb{F}_n}) + w(g|_{\mathbb{F}_n}) \),
2. \( f \) is balanced if \( g + h \) and \( h \) are both balanced,
3. \( f \) is unbalanced if one in \( \{g + h, h\} \) is balanced and another one not.
Observation

• Any Bf can be expressed as:
  \[ f = x_{n+1}g(x_1, \ldots, x_n) + h(x_1, \ldots, x_n). \]

• If \( f \) in \( B_n \) only depends on \( m \) variables (\( m < n \)), then \( f|_{\mathbb{F}^m} \) denotes its restriction to these \( m \) variables.

Theorem

If \( f = x_{n+1}g(x_1, \ldots, x_n) + h(x_1, \ldots, x_n) \), then

1. \( w(f) = w((g + h)|_{\mathbb{F}^n}) + w(g|_{\mathbb{F}^n}) \),
2. \( f \) is balanced if \( g + h \) and \( h \) are both balanced,
3. \( f \) is unbalanced if one in \( \{g + h, h\} \) is balanced and another one not.
Observation

- Any Bf can be expressed as:
  \[ f = x_{n+1}g(x_1, \ldots, x_n) + h(x_1, \ldots, x_n). \]
- If \( f \) in \( B_n \) only depends on \( m \) variables \( (m < n) \), then \( f|_{\mathbb{F}^m} \) denotes its restriction to these \( m \) variables.

Theorem

If \( f = x_{n+1}g(x_1, \ldots, x_n) + h(x_1, \ldots, x_n) \), then

1. \( w(f) = w((g + h)|_{\mathbb{F}^n}) + w(g|_{\mathbb{F}^n}) \),
2. \( f \) is balanced if \( g + h \) and \( h \) are both balanced,
3. \( f \) is unbalanced if one in \( \{g + h, h\} \) is balanced and another one not.
Observation

- Any Bf can be expressed as:
  \[ f = x_{n+1}g(x_1, \ldots, x_n) + h(x_1, \ldots, x_n). \]
- If \( f \) in \( B_n \) only depends on \( m \) variables \( (m < n) \), then \( f|_{\mathbb{F}^m} \) denotes its restriction to these \( m \) variables.

Theorem

If \( f = x_{n+1}g(x_1, \ldots, x_n) + h(x_1, \ldots, x_n) \), then

1. \( w(f) = w((g + h)|_{\mathbb{F}^n}) + w(g|_{\mathbb{F}^n}) \),
2. \( f \) is balanced if \( g + h \) and \( h \) are both balanced,
3. \( f \) is unbalanced if one in \( \{g + h, h\} \) is balanced and another one not.
Lemma

Let \( f = x_{n+1}g(x_1, ..., x_n) + h(x_1, ..., x_n) \), with \( g, h \in B_n \) and let \( \alpha \in (a_{n+1}, a) \in \mathbb{F} \times \mathbb{F}^n \). Then

1. \( D_\alpha f \sim_A x_{n+1} Da g + a_{n+1}g + Da h \),

2. \( D_\alpha f \) is constant if and only if \( Da g = 0 \) and \( Da h = a_{n+1}g + c \), for some \( c \in \mathbb{F} \).

Proposition

If \( f = x_{n+1}g(x_1, ..., x_n) + h(x_1, ..., x_n) \), with \( n \) even, \( f \in B_{n+1} \), \( g, h \in B_n \) and \( g \) bent, then the linear space of \( f \) is trivial.
Lemma

Let $f = x_{n+1}g(x_1, ..., x_n) + h(x_1, ..., x_n)$, with $g, h \in B_n$ and let $\alpha \in (a_{n+1}, a) \in \mathbb{F} \times \mathbb{F}^n$. Then

1. $D_{\alpha}f \sim_A x_{n+1}Da g + a_{n+1}g + Da h$,

2. $D_{\alpha}f$ is constant if and only if $Da g = 0$ and $Da h = a_{n+1}g + c$, for some $c \in \mathbb{F}$.

Proposition

If $f = x_{n+1}g(x_1, ..., x_n) + h(x_1, ..., x_n)$, with $n$ even, $f \in B_{n+1}$, $g, h \in B_n$ and $g$ bent, then the linear space of $f$ is trivial.
Lemma

Let \( f = x_{n+1}g(x_1, ..., x_n) + h(x_1, ..., x_n) \), with \( g, h \in B_n \) and let \( \alpha \in (a_{n+1}, a) \in \mathbb{F} \times \mathbb{F}^n \). Then

1. \( D_\alpha f \sim_A x_{n+1} Da g + a_{n+1}g + Da h \),
2. \( D_\alpha f \) is constant if and only if \( Da g = 0 \) and \( Da h = a_{n+1}g + c \), for some \( c \in \mathbb{F} \).

Proposition

If \( f = x_{n+1}g(x_1, ..., x_n) + h(x_1, ..., x_n) \), with \( n \) even, \( f \in B_{n+1} \), \( g, h \in B_n \) and \( g \) bent, then the linear space of \( f \) is trivial.
Linear space of Balanced functions

Lemma

Let $f = x_{n+1}g(x_1, \ldots, x_n) + h(x_1, \ldots, x_n)$, with $g, h \in B_n$ and let $\alpha \in (a_{n+1}, a) \in \mathbb{F} \times \mathbb{F}^n$. Then

1. $D_\alpha f \sim_A x_{n+1}D_ag + a_{n+1}g + D_ah$,
2. $D_\alpha f$ is constant if and only if $D_ag = 0$ and $D_ah = a_{n+1}g + c$, for some $c \in \mathbb{F}$.

Proposition

If $f = x_{n+1}g(x_1, \ldots, x_n) + h(x_1, \ldots, x_n)$, with $n$ even, $f \in B_{n+1}$, $g, h \in B_n$ and $g$ bent, then the linear space of $f$ is trivial.
Proposition

Let $f = x_{n+1}g + h$ with $g = \tilde{g}(x_1, \ldots, x_{n-1}) + x_n$ and $h = \tilde{h}(x_1, \ldots, x_{n-2}) + x_{n-1}$. Then

- $f$ is balanced and its linear space is trivial if $n$ is odd and $\tilde{g}|_{\mathbb{F}^{n-1}}$ is bent.

Corollary

Let $f = x_1g_1 + \cdots + x_{i-1}g_{i-1} + g_i$, with $g_i = \tilde{g}_i(x_{i+1}, \ldots, x_{n-i}) + x_{n-i+1}$, $g_i \in B_{n-2i+1}$ and $i \leq \lfloor n/2 \rfloor$. Then

- $f$ is balanced and its linear space is trivial if $n$ is even and $\tilde{g}_1|_{\mathbb{F}^{n-2}}$ is bent.
Proposition

Let $f = x_{n+1}g + h$ with $g = \tilde{g}(x_1, ..., x_{n-1}) + x_n$ and $h = \tilde{h}(x_1, ..., x_{n-2}) + x_{n-1}$. Then

- $f$ is balanced and its linear space is trivial if $n$ is odd and $\tilde{g}|_{\mathbb{F}^{n-1}}$ is bent.

Corollary

Let $f = x_1g_1 + \cdots + x_{i-1}g_{i-1} + g_i$, with $g_i = \tilde{g}_i(x_{i+1}, ..., x_{n-i}) + x_{n-i+1}$, $g_i \in B_{n-2i+1}$ and $i \leq \lfloor n/2 \rfloor$. Then

- $f$ is balanced and its linear space is trivial if $n$ is even and $\tilde{g}_1|_{\mathbb{F}^{n-2}}$ is bent.
Linear space of Balanced functions

**Proposition**

Let \( f = x_{n+1}g + h \) with \( g = \tilde{g}(x_1, \ldots, x_{n-1}) + x_n \) and \( h = \tilde{h}(x_1, \ldots, x_{n-2}) + x_{n-1} \). Then

- \( f \) is balanced and its linear space is trivial if \( n \) is odd and \( \tilde{g}|_{\mathbb{F}^{n-1}} \) is bent.

**Corollary**

Let \( f = x_1g_1 + \cdots + x_{i-1}g_{i-1} + g_i \), with \( g_i = \tilde{g}_i(x_{i+1}, \ldots, x_{n-i}) + x_{n-i+1}, \) \( g_i \in B_{n-2i+1} \) and \( i \leq \lfloor n/2 \rfloor \). Then

- \( f \) is balanced and its linear space is trivial if \( n \) is even and \( \tilde{g}_1|_{\mathbb{F}^{n-2}} \) is bent.
Observation

Any Bf can be represented in the form:

\[ f = x_{n+1}g(x_1, \ldots, x_n) + (1 + x_{n+1})h(x_1, \ldots, x_{n+1}), \]

with \( g, h \in B_n \). We call this convolutional product of \( g \) and \( h \).

Proposition

Let \( f = x_{n+1}g(x_1, \ldots, x_n) + (1 + x_{n+1})h(x_1, \ldots, x_n) \), with \( g, h \in B_n \) and \( \deg(h), \deg(g) \leq 2 \), be cubic. Then

- \( f \) is balanced if and only if both \( g \) and \( h \) are balanced or \( g = h \circ \varphi + 1 \), for some affinity \( \varphi \).
Linear space of Balanced functions

Observation

Any Bf can be represented in the form:

\[ f = x_{n+1}g(x_1, \ldots, x_n) + (1 + x_{n+1})h(x_1, \ldots, x_{n+1}), \]

with \( g, h \in B_n \). We call this convolutional product of \( g \) and \( h \).

Proposition

Let \( f = x_{n+1}g(x_1, \ldots, x_n) + (1 + x_{n+1})h(x_1, \ldots, x_n) \), with \( g, h \in B_n \) and \( \deg(h), \deg(g) \leq 2 \), be cubic. Then

- \( f \) is balanced if and only if both \( g \) and \( h \) are balanced or \( g = h \circ \varphi + 1 \), for some affinity \( \varphi \).
Observation

Any Bf can be represented in the form:

\[ f = x_{n+1}g(x_1, \ldots, x_n) + (1 + x_{n+1})h(x_1, \ldots, x_{n+1}), \]

with \( g, h \in B_n \). We call this **convolutional product** of \( g \) and \( h \).

Proposition

Let \( f = x_{n+1}g(x_1, \ldots, x_n) + (1 + x_{n+1})h(x_1, \ldots, x_n) \), with \( g, h \in B_n \) and \( \deg(h), \deg(g) \leq 2 \), be cubic. Then

- \( f \) is balanced if and only if both \( g \) and \( h \) are balanced or \( g = h \circ \varphi + 1 \), for some affinity \( \varphi \).
Proposition

Let \( f = x_{n+1}g(x_1, \ldots, x_n) + (1 + x_{n+1})h(x_1, \ldots, x_n) \), with \( g, h \in B_n \).

Then

- \( f \) is balanced if \( g \) and \( h \) are both balanced or \( g = h \circ \varphi + 1 \), for some affinity \( \varphi \),
- \( f \) is balanced if \( n \) is even, \( g|_{F^n} \) and \( h|_{F^n} \) are both bent with \( w(g) \neq w(h) \),
- \( f \) is plateaued if \( n \) is even, \( g|_{F^n} \) and \( h|_{F^n} \) are both bent,
- the linear space of \( f \) is trivial if \( n \) is even, \( h|_{F^n} \) is bent and \( \deg(f) = \max\{\deg(g), \deg(h)\} + 1 \).
Proposition

Let $f = x_{n+1}g(x_1, \ldots, x_n) + (1 + x_{n+1})h(x_1, \ldots, x_n)$, with $g, h \in B_n$. Then

- $f$ is balanced if $g$ and $h$ are both balanced or $g = h \circ \varphi + 1$, for some affinity $\varphi$,
- $f$ is balanced if $n$ is even, $g|_{\mathbb{F}^n}$ and $h|_{\mathbb{F}^n}$ are both bent with $w(g) \neq w(h)$,
- $f$ is plateaued if $n$ is even, $g|_{\mathbb{F}^n}$ and $h|_{\mathbb{F}^n}$ are both bent,
- the linear space of $f$ is trivial if $n$ is even, $h|_{\mathbb{F}^n}$ is bent and $\deg(f) = \max\{\deg(g), \deg(h)\} + 1$. 

A. Musukwa et. al.  
On derivatives of Balanced functions and APN functions
Proposition

Let $f = x_{n+1}g(x_1, ..., x_n) + (1 + x_{n+1})h(x_1, ..., x_n)$, with $g, h \in B_n$. Then

- $f$ is balanced if $g$ and $h$ are both balanced or $g = h \circ \varphi + 1$, for some affinity $\varphi$,
- $f$ is balanced if $n$ is even, $g|_{F^n}$ and $h|_{F^n}$ are both bent with $w(g) \neq w(h)$,
- $f$ is plateaued if $n$ is even, $g|_{F^n}$ and $h|_{F^n}$ are both bent,
- the linear space of $f$ is trivial if $n$ is even, $h|_{F^n}$ is bent and $\deg(f) = \max\{\deg(g), \deg(h)\} + 1$. 

A. Musukwa et. al.

On derivatives of Balanced functions and APN functions
Let $f = x_{n+1}g(x_1, ..., x_n) + (1 + x_{n+1})h(x_1, ..., x_n)$, with $g, h \in B_n$. Then

- $f$ is balanced if $g$ and $h$ are both balanced or $g = h \circ \varphi + 1$, for some affinity $\varphi$,
- $f$ is balanced if $n$ is even, $g|_{\mathbb{F}^n}$ and $h|_{\mathbb{F}^n}$ are both bent with $w(g) \neq w(h)$,
- $f$ is plateaued if $n$ is even, $g|_{\mathbb{F}^n}$ and $h|_{\mathbb{F}^n}$ are both bent,
- the linear space of $f$ is trivial if $n$ is even, $h|_{\mathbb{F}^n}$ is bent and $\deg(f) = \max\{\deg(g), \deg(h)\} + 1$. 
Proposition

Let \( f = x_{n+1}g(x_1, ..., x_n) + (1 + x_{n+1})h(x_1, ..., x_n) \), with \( g, h \in B_n \).
Then

- \( f \) is balanced if \( g \) and \( h \) are both balanced or \( g = h \circ \varphi + 1 \), for some affinity \( \varphi \),
- \( f \) is balanced if \( n \) is even, \( g|_{\mathbb{F}^n} \) and \( h|_{\mathbb{F}^n} \) are both bent with \( w(g) \neq w(h) \),
- \( f \) is plateaued if \( n \) is even, \( g|_{\mathbb{F}^n} \) and \( h|_{\mathbb{F}^n} \) are both bent,
- the linear space of \( f \) is trivial if \( n \) is even, \( h|_{\mathbb{F}^n} \) is bent and \( \deg(f) = \max\{\deg(g), \deg(h)\} + 1 \).
Theorem [Well-known]

Let $F$ be vBf from $\mathbb{F}^n$ into $\mathbb{F}^n$. Then

$$\sum_{\lambda \in \mathbb{F}^n \backslash \{0\}} \sum_{a \in \mathbb{F}^n} \mathcal{F}^2(D_a F_{\lambda}) \geq 2^{2n+1}(2^n - 1).$$

Moreover, $F$ is APN if and only if equality holds.

Lemma

Let $f \in B_n$, with $n$ even, be such that $\dim V(f) \geq 1$. Then

$$|\Gamma(f)| \leq 2^n - 4.$$
Theorem [Well-known]
Let $F$ be a vectorial function from $\mathbb{F}^n$ into $\mathbb{F}^n$. Then
\[ \sum_{\lambda \in \mathbb{F}^n \setminus \{0\}} \sum_{a \in \mathbb{F}^n} \mathcal{F}^2(D_aF_\lambda) \geq 2^{2n+1}(2^n - 1). \]
Moreover, $F$ is APN if and only if equality holds.

Lemma
Let $f \in B_n$, with $n$ even, be such that $\dim V(f) \geq 1$. Then
\[ |\Gamma(f)| \leq 2^n - 4. \]
Lemma

Let $F$ be a vBf from $\mathbb{F}^n$ into $\mathbb{F}^n$, with $n$ even. If $\dim V(F_\lambda) \geq 1$, for all $\lambda \in \mathbb{F}^n$, then

$$\sum_{\lambda \in \mathbb{F}^n \setminus \{0\}} \sum_{a \in \mathbb{F}^n} F^2(D_a F_\lambda) > 2^{2n+1}(2^n - 1).$$

Theorem

Let $F$ from $\mathbb{F}^n$ to $\mathbb{F}^n$, with $n$ even, be an APN. Then there is a $\lambda \in \mathbb{F}^n \setminus \{0\}$ such that the linear space of $F_\lambda$ is trivial.
Lemma

Let $F$ be a vBf from $F^n$ into $F^n$, with $n$ even. If $\dim V(F_\lambda) \geq 1$, for all $\lambda \in F^n$, then

$$\sum_{\lambda \in F^n \setminus \{0\}} \sum_{a \in F^n} \mathcal{F}^2(D_aF_\lambda) > 2^{2n+1}(2^n - 1).$$

Theorem

Let $F$ from $F^n$ to $F^n$, with $n$ even, be an APN. Then there is a $\lambda \in F^n \setminus \{0\}$ such that the linear space of $F_\lambda$ is trivial.
Proposition

For any \( Q : \mathbb{F}^n \rightarrow \mathbb{F}^n \), we have

\[
\sum_{\lambda \in \mathbb{F}^n \setminus \{0\}} (2^{\dim V(F_\lambda)} - 1) \geq 2^n - 1.
\]

(2)

Moreover, equality holds if and only if \( Q \) is APN.

Proposition

Let \( Q : \mathbb{F}^n \rightarrow \mathbb{F}^n \), with \( n \) even, be such that \( Q_\lambda \), with \( \lambda \neq 0 \), is bent or semi-bent. Then \( Q \) is APN if and only if there are exactly \( \frac{2}{3}(2^n - 1) \) bent components.
Proposition

For any $Q : \mathbb{F}^n \rightarrow \mathbb{F}^n$, we have

$$\sum_{\lambda \in \mathbb{F}^n \setminus \{0\}} (2^{\dim V(F_\lambda)} - 1) \geq 2^n - 1.$$  (2)

Moreover, equality holds if and only if $Q$ is APN.

Proposition

Let $Q : \mathbb{F}^n \rightarrow \mathbb{F}^n$, with $n$ even, be such that $Q_\lambda$, with $\lambda \neq 0$, is bent or semi-bent. Then $Q$ is APN if and only if there are exactly $\frac{2}{3}(2^n - 1)$ bent components.
Remark

The maximum number of bent components of vBf $F : \mathbb{F}^n \rightarrow \mathbb{F}^n$ is $2^n - 2^{n/2}$ [Pott et al. 2018].

No plateaued APN functions can achieve the maximum number [Mesnager et al., 2018].

Let $B$ denote the number of bent components.
Remark

The maximum number of bent components of \( vBF : \mathbb{F}^n \rightarrow \mathbb{F}^n \) is \( 2^n - 2^{n/2} \) [Pott et al. 2018].
No plateaued APN functions can achieve the maximum number [Mesnager et al., 2018].

Let \( B \) denote the number of bent components.
Theorem

Let \( Q : \mathbb{F}^n \rightarrow \mathbb{F}^n \), with \( n \) even, be APN. Then

\[
2(2^n - 1)/3 \leq B \leq 2^n - 2^{n/2} - 2
\]

where \( B = 2(2^n - 1)/3 + 4t \), for some integer \( t \geq 0 \).

Remark

If \( t > 0 \), then there is a component which is not bent or semi-bent.

One known such quadratic APN with \( t > 0 \) is [Dillon, 2006]
\[
F(x) = x^3 + z^{11}x^5 + z^{13}x^9 + x^{17} + z^{11}x^{33} + x^{48}
\]
defined over \( \mathbb{F}_{2^6} \) and \( z \) is primitive. It has 46 bent components.
Quadratic APN functions in even dimension

Theorem
Let \( Q : \mathbb{F}^n \rightarrow \mathbb{F}^n \), with \( n \) even, be APN. Then

\[
2(2^n - 1)/3 \leq B \leq 2^n - 2^{n/2} - 2
\]

where \( B = 2(2^n - 1)/3 + 4t \), for some integer \( t \geq 0 \).

Remark
If \( t > 0 \), then there is a component which is not bent or semi-bent.

One known such quadratic APN with \( t > 0 \) is [Dillon, 2006]
\[
F(x) = x^3 + z^{11}x^5 + z^{13}x^9 + x^{17} + z^{11}x^{33} + x^{48}
\]
defined over \( \mathbb{F}_{2^6} \) and \( z \) is primitive. It has 46 bent components.
Theorem

Let $F(x) = x^d$ be a function in $\mathbb{F}_{2^n}[x]$ where $n$ is even and $d = 2^j(2^k + 1)$ with integer $j \geq 0$, $k \geq 1$. Let $s = (n, 2k)$, $e = (2^n - 1, 2^k + 1)$. Then the

(i) number of bent components for $F(x)$ is $2^n - \frac{2^n-1}{e} - 1$,

(ii) Walsh spectrum of $F(x)$ is $\{0, \pm 2^{(n+s)/2}\}$ if $e = 1$ and $\{0, \pm 2^{(n+s)/2}, \pm 2^n/2\}$ if $e \geq 3$.

Remark

$F(x) = x^d$, with $d = 2^j(2^k + 1)$, has the maximum number of bent components if and only if $n = 2k$ (i.e. $e = 2^k + 1$). In this case $F$ has only bent and affine components.
Quadratic power functions

Theorem
Let $F(x) = x^d$ be a function in $\mathbb{F}_{2^n}[x]$ where $n$ is even and $d = 2^j(2^k + 1)$ with integer $j \geq 0$, $k \geq 1$. Let $s = (n, 2k)$, $e = (2^n - 1, 2^k + 1)$. Then the

(i) number of bent components for $F(x)$ is $2^n - \frac{2^n-1}{e} - 1$,

(ii) Walsh spectrum of $F(x)$ is $\{0, \pm 2^{(n+s)/2}\}$ if $e = 1$ and $\{0, \pm 2^{(n+s)/2}, \pm 2^n/2\}$ if $e \geq 3$.

Remark

$F(x) = x^d$, with $d = 2^j(2^k + 1)$, has the maximum number of bent components if and only if $n = 2k$ (i.e. $e = 2^k + 1$). In this case $F$ has only bent and affine components.
Theorem

Let $F(x) = x^d$ be a function in $\mathbb{F}_{2^n}[x]$ where $n$ is even and $d = 2^j(2^k + 1)$ with integer $j \geq 0$, $k \geq 1$. Let $s = (n, 2k)$, $e = (2^n - 1, 2^k + 1)$. Then the

(i) number of bent components for $F(x)$ is $2^n - \frac{2^n-1}{e} - 1$,

(ii) Walsh spectrum of $F(x)$ is $\{0, \pm 2^{(n+s)/2}\}$ if $e = 1$ and $\{0, \pm 2^{(n+s)/2}, \pm 2^{n/2}\}$ if $e \geq 3$.

Remark

$F(x) = x^d$, with $d = 2^j(2^k + 1)$, has the maximum number of bent components if and only if $n = 2k$ (i.e. $e = 2^k + 1$). In this case $F$ has only bent and affine components.
Theorem

Let $F(x) = x^d$ be a function in $\mathbb{F}_{2^n}[x]$ where $n$ is even and 
\[ d = 2^j(2^k + 1) \]
with integer $j \geq 0$, $k \geq 1$. Let $s = (n, 2k)$, $e = (2^n - 1, 2^k + 1)$. Then the

(i) number of bent components for $F(x)$ is $2^n - \frac{2^n-1}{e} - 1$,
(ii) Walsh spectrum of $F(x)$ is $\{0, \pm 2^{(n+s)/2}\}$ if $e = 1$ and 
$\{0, \pm 2^{(n+s)/2}, \pm 2^{n/2}\}$ if $e \geq 3$.

Remark

$F(x) = x^d$, with $d = 2^j(2^k + 1)$, has the maximum number of bent components if and only if $n = 2k$ (i.e. $e = 2^k + 1$). In this case $F$ has only bent and affine components.
Corollary

Let \( F(x) = x^d \) be a power polynomial in \( \mathbb{F}_{2^n}[x] \) where \( n \) is even and \( d = 2^j(2^k + 1) \) with integer \( j \geq 0, k \geq 1 \). Let \( s = (n, 2k) \), \( e = (2^n - 1, 2^k + 1) \). Then \( F(x) \) is APN if and only if \( e = 3 \) and \( s = 2 \). Equivalently, \( F(x) \) is APN if and only if there are exactly \( 2(2^n - 1)/3 \) bent components and the rest semi-bent.

Corollary

If a quadratic power function, in even dimension, has some bent components, then they are at least \( 2(2^n - 1)/3 \).
THANK YOU FOR YOUR ATTENTION!