On the normality of p-ary bent functions

A. Çeşmelioğlu[1] W. Meidl [2] A. Pott [1]

[1]Otto-von-Guericke University, Magdeburg, Germany

[2]Sabancı University, Istanbul, Turkey

Bent Functions

Definition

Let p be a prime, $f : \mathbb{F}_p^n \to \mathbb{F}_p$ and $\epsilon_p = e^{\frac{2\pi i}{p}}$. For each $b \in \mathbb{F}_p^n$, the **Walsh (Fourier) transform** of f is defined as

$$\widehat{f}(b) = \sum_{x \in \mathbb{F}_p^n} \epsilon_p^{f(x) - <b,x>}.$$

Definition

A function $f : \mathbb{F}_p^n \to \mathbb{F}_p$ is called a bent function if for all $b \in \mathbb{F}_p^n$, $\left|\widehat{f}(b)\right| = p^{n/2}$.

Walsh Spectrum of Bent Functions

For a bent function $f : \mathbb{F}_p^n \to \mathbb{F}_p$,

$$\widehat{f}(b) = \zeta_b \, p^{n/2} \epsilon_p^{f^*(b)}.$$

For $p = 2$, for all $b \in \mathbb{F}_2^n$,

$$\widehat{f}(b) = 2^{n/2}(-1)^{f^*(b)} \Rightarrow \zeta_b = 1.$$

For odd p [Kumar, Scholz, Welch '85]

$$\zeta_b = \begin{cases} \pm 1 & n \text{ is even or } n \text{ is odd and } p \equiv 1 \bmod 4, \\ \pm i & n \text{ is odd and } p \equiv 3 \bmod 4. \end{cases}$$

Regular bent functions

Definition

f is called **regular bent** if $\zeta_b = 1$ for all $b \in \mathbb{F}_p^n$.

Example

- A Boolean bent function is always **regular bent**.
- $f_1 : \mathbb{F}_{3^2} \to \mathbb{F}_3$ defined as $f_1(x) = \mathrm{Tr}_2(x^2)$
  Walsh spectrum: $\{3, 3\epsilon_3, 3\epsilon_3^2\} \Rightarrow$ **regular bent**.

Weakly regular bent functions

Definition

f is called **weakly regular bent** if ζ_b is the same for all $b \in \mathbb{F}_p^n$.

Example

- $f_2 : \mathbb{F}_{3^4} \longrightarrow \mathbb{F}_3$ defined as $f_2(x) = \mathrm{Tr}_4(2x^{14})$
  Walsh spectrum: $\{-9, -9\epsilon_3, -9\epsilon_3^2\} \Rightarrow$ **weakly regular bent**,
- $f_3 : \mathbb{F}_{3^3} \longrightarrow \mathbb{F}_3$ defined as $f_3(x) = \mathrm{Tr}_3(2x^2)$
  Walsh spectrum: $\{\mathbf{i}3\sqrt{3}, \mathbf{i}3\sqrt{3}\epsilon_3, \mathbf{i}3\sqrt{3}\epsilon_3^2\} \Rightarrow$ **weakly regular bent**.

Remark:

regular bent $\Rightarrow$ **weakly regular bent**.

Kumar, Scholz, Welch result

For odd p [Kumar, Scholz, Welch '85]

$$\zeta_b = \begin{cases} \pm 1 & n \text{ is even or } n \text{ is odd and } p \equiv 1 \bmod 4, \\ \pm i & n \text{ is odd and } p \equiv 3 \bmod 4. \end{cases}$$

Not weakly regular bent functions

Definition

If ζ_b changes sign with $b \in \mathbb{F}_p^n$ then f is called **not weakly regular bent**.

Example

$f_4 : \mathbb{F}_{3^3} \rightarrow \mathbb{F}_3$ defined as $f_4(x) = \mathrm{Tr}_3(x^8 + x^{22})$
Walsh spectrum: $\{\mathbf{i}3\sqrt{3}, -\mathbf{i}3\sqrt{3}, -\mathbf{i}3\sqrt{3}\epsilon_3, -\mathbf{i}3\sqrt{3}\epsilon_3, \mathbf{i}3\sqrt{3}\epsilon_3^2, -\mathbf{i}3\sqrt{3}\epsilon_3^2\} \Rightarrow$
not weakly regular bent.

Normal-Weakly normal

Introduced by Dobbertin('94)

Definition

$f : \mathbb{F}_p^n \longrightarrow \mathbb{F}_p, \mathbf{n} = \mathbf{2m}$

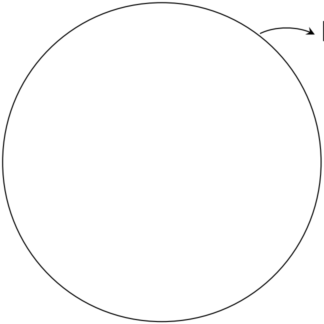
f is **normal** if it is *constant* on an **m**-dimensional affine subspace of $\mathbb{F}_p^n$.

f is **weakly normal** if it is *affine* on an **m**-dimensional affine subspace of $\mathbb{F}_p^n$.

normal $\Rightarrow$ **weakly normal**

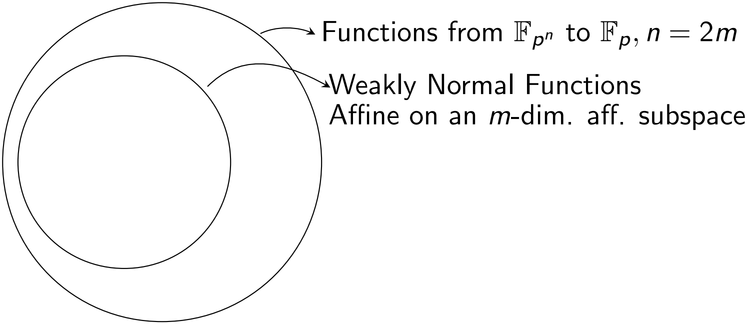
In general, it is not easy to check the normality of functions.

Normal-Weakly normal

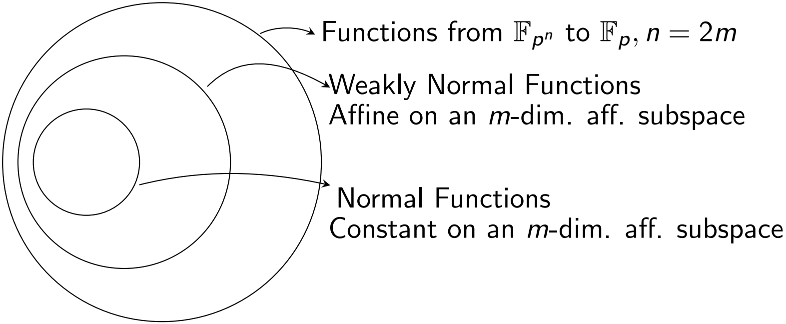


Functions from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p, n = 2m$

Normal-Weakly normal



Normal-Weakly normal



Normality of Classical Examples

Normality is defined for arbitrary functions but we consider bent functions only.

- **Maiorana-McFarland bent functions:**

  $f : \mathbb{F}_p^m \times \mathbb{F}_p^m \rightarrow \mathbb{F}_p$ defined as

$$f(x, y) = < x, \pi(y) > + h(y),$$

  $\pi : \mathbb{F}_p^m \rightarrow \mathbb{F}_p^m$: a permutation of $\mathbb{F}_p^m$
  $h : \mathbb{F}_p^m \rightarrow \mathbb{F}_p$: an arbitrary function

Normality of Classical Examples

Normality is defined for arbitrary functions but we consider bent functions only.

- **Maiorana-McFarland bent functions:**

  $f : \mathbb{F}_p^m \times \mathbb{F}_p^m \to \mathbb{F}_p$ defined as

  $$f(x, y) =< x, \pi(y) > +h(y),$$

  $\pi : \mathbb{F}_p^m \to \mathbb{F}_p^m$: a permutation of $\mathbb{F}_p^m$
  $h : \mathbb{F}_p^m \to \mathbb{F}_p$: an arbitrary function

  f is **normal** since $f(x, y) = 0$ on the m-dimensional subspace $\mathbb{F}_p^m \times \{\pi^{-1}(0)\}$.

Normality of Classical Examples

- $\mathcal{PS}^+$ **bent functions:**
  V_i : m-dimensional subspace of $\mathbb{F}_2^{2m}$, $1 \leq i \leq 2^{m-1}+1$,
  $f : \mathbb{F}_2^{2m} \rightarrow \mathbb{F}_2$,
  $$f(x) = 1 \text{ on each } V_i.$$

Normality of Classical Examples

- $\mathcal{PS}^+$ **bent functions:**

  V_i : m-dimensional subspace of $\mathbb{F}_2^{2m}$, $1 \leq i \leq 2^{m-1} + 1$,

  $f : \mathbb{F}_2^{2m} \longrightarrow \mathbb{F}_2$,

  $$f(x) = 1 \text{ on each } V_i.$$

  f is **normal**.

Normality of Classical Examples

- $\mathcal{PS}^+$ **bent functions:**

  V_i : m-dimensional subspace of $\mathbb{F}_2^{2m}$, $1 \leq i \leq 2^{m-1}+1$,

  $f : \mathbb{F}_2^{2m} \to \mathbb{F}_2$,

  $$f(x) = 1 \text{ on each } V_i.$$

  f is **normal**.

- $\mathcal{PS}_{\mathbf{ap}}$ **bent functions:**

  $g : \mathbb{F}_p^m \to \mathbb{F}_p$: a balanced function with $g(0) = 0$.

  $f : \mathbb{F}_p^m \times \mathbb{F}_p^m \to \mathbb{F}_p$ defined as $f(x, y) = g(xy^{p^m-2})$ is a bent function.

Normality of Classical Examples

- $\mathcal{PS}^+$ **bent functions:**

  V_i : m-dimensional subspace of $\mathbb{F}_2^{2m}$, $1 \leq i \leq 2^{m-1}+1$,

  $f : \mathbb{F}_2^{2m} \longrightarrow \mathbb{F}_2$,

  $$f(x) = 1 \text{ on each } V_i.$$

  f is **normal**.

- $\mathcal{PS}_{\mathbf{ap}}$ **bent functions:**

  $g : \mathbb{F}_p^m \longrightarrow \mathbb{F}_p$: a balanced function with $g(0) = 0$.

  $f : \mathbb{F}_p^m \times \mathbb{F}_p^m \longrightarrow \mathbb{F}_p$ defined as $f(x,y) = g(xy^{p^m-2})$ is a bent function.

  $$f(x,y) = 0 \text{ on } \{0\} \times \mathbb{F}_p^m \Rightarrow f \text{ is } \textbf{normal}.$$

Lemma (Ç., Meidl, Pott 2013)

A function $f : \mathbb{F}_p^n \longrightarrow \mathbb{F}_p$ is **weakly normal** *if and only if there exists $a \in \mathbb{F}_p^n$ such that $f(x) - a \cdot x$ is* **normal**.

- **$\mathbf{p = 2}$ case:**

  For $n = 2, 4, 6$ all bent functions are **normal**.

  $n = 10$ is the smallest dimension where a **weakly normal** but **not normal** bent function exists, [Canteaut, Daum, Dobbertin, Leander 2006]

  $n = 10$ is the smallest dimension where a **not weakly normal** bent function exists, [Leander, McGuire 2009].

- **$p = 2$ case:**
  For $n = 2, 4, 6$ all bent functions are **normal**.

  $n = 10$ is the smallest dimension where a **weakly normal** but **not normal** bent function exists, [Canteaut, Daum, Dobbertin, Leander 2006]

  $n = 10$ is the smallest dimension where a **not weakly normal** bent function exists, [Leander, McGuire 2009].

- **odd p case:**
  One can easily find examples of **not weakly normal** bent functions even for $n = 2$.

Normality for odd characteristic case

Theorem (Ç., Meidl, Pott 2013)

p odd prime, $n = 2m$, $f : \mathbb{F}_p^n \rightarrow \mathbb{F}_p$ a bent function

(i) *If f is* **weakly regular bent** *but* **not regular** *then f is* **not weakly normal**.

Normality for odd characteristic case

Theorem (Ç., Meidl, Pott 2013)

p odd prime, $n = 2m$, $f : \mathbb{F}_p^n \to \mathbb{F}_p$ a bent function

(i) *If f is* **weakly regular bent** *but* **not regular** *then f is* **not weakly normal**.

(ii) *If f is* **normal**, *constant on the affine subspace $E + b$ for an $m-$dimensional subspace E and $b \in \mathbb{F}_p^n$, then f is balanced on the remaining cosets.*

Normality for odd characteristic case

Theorem (Ç., Meidl, Pott 2013)

p odd prime, $n = 2m$, $f : \mathbb{F}_p^n \to \mathbb{F}_p$ a bent function

(i) *If f is* **weakly regular bent** *but* **not regular** *then f is* **not weakly normal**.

(ii) *If f is* **normal***, constant on the affine subspace $E + b$ for an $m-$dimensional subspace E and $b \in \mathbb{F}_p^n$, then f is balanced on the remaining cosets. The dual of f is* **weakly normal** *on $E^{\perp}$.*

Not weakly regular functions?

Example 1:

$f : \mathbb{F}_{3^4} \to \mathbb{F}_3$, ω a primitive element of $\mathbb{F}_{3^4}$.

$f(x) = \mathrm{Tr}_4(\omega^{10}x^{22} + x^4)$ is **normal** since $f(x) = 0$ on $E = span\{\omega, \omega^3 + \omega^2\}$.

Not weakly regular functions?

Example 1:

$f : \mathbb{F}_{3^4} \to \mathbb{F}_3$, ω a primitive element of $\mathbb{F}_{3^4}$.
$f(x) = \mathrm{Tr}_4(\omega^{10}x^{22} + x^4)$ is **normal** since $f(x) = 0$ on $E = span\{\omega, \omega^3 + \omega^2\}$.

Example 2:

$f : \mathbb{F}_{3^6} \to \mathbb{F}_3, \omega$ a primitive element of $\mathbb{F}_{3^6}$.
$f(x) = \mathrm{Tr}_6(\omega^7 x^{98})$ is **not normal**.

Quadratics?

Theorem (Ç., Meidl, Pott 2013)

p odd prime, $n = 2m$, $f : \mathbb{F}_p^n \rightarrow \mathbb{F}_p$ a quadratic bent function

f *is* **regular bent** $\Rightarrow$ *f is in the completed Maiorana-McFarland class*

$\Rightarrow$ *f is* **weakly normal**.

f *is* **weakly regular (not regular) bent** $\Rightarrow$ *f is* **not weakly normal**

Coulter-Matthews bent functions?

Definition

$f_\alpha : \mathbb{F}_{3^n} \longrightarrow \mathbb{F}_3$ defined as $f_\alpha(x) = \mathrm{Tr_n}(\alpha x^{\frac{3^k+1}{2}})$, k is odd, $\gcd(n,k) = 1$.

Lemma (Ç., Meidl, Pott 2013)

f_α *is* **regular bent** *if and only if*
$$\begin{cases} n \equiv 0 \mod 4 \text{ and } \alpha \text{ is a nonsquare,} \\ \text{or} \\ n \equiv 2 \mod 4 \text{ and } \alpha \text{ is a square.} \end{cases}$$

Normality of Coulter-Matthews functions

Theorem (Ç., Meidl, Pott 2013)

Regular bent *Coulter-Matthews functions are* ***normal****.*

Summary/Open Problems-odd characteristic case

	N	**WN** but not **N**	**NWN**
R	MMF PSap	quadratics in $\overline{MMF}$	??
WR but not **R**	–	–	All
NWR	Ex. 1	Ex. 2??	Ex. 2??

MMF: Mairoana-McFarland class, $\overline{MMF}$: completed Maiorana-McFarland class

N: Normal, **WN**: Weakly normal, **NWN**: Not weakly normal

R:Regular bent, **WR**:Weakly regular bent, **NWR**:Not weakly regular bent