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
Definition

Let $p$ be a prime, $f : \mathbb{F}_p^n \rightarrow \mathbb{F}_p$ 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

$$\hat{f}(b) = \sum_{x \in \mathbb{F}_p^n} \epsilon_p^{f(x) - \langle b, x \rangle}.$$

Definition

A function $f : \mathbb{F}_p^n \rightarrow \mathbb{F}_p$ is called a **bent function** if for all $b \in \mathbb{F}_p^n$, $|\hat{f}(b)| = p^{n/2}$.
Walsh Spectrum of Bent Functions

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

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

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

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

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

$$\zeta_b = \begin{cases} 
\pm 1 & n \text{ is even or } n \text{ is odd and } p \equiv 1 \mod 4, \\
\pm i & n \text{ is odd and } p \equiv 3 \mod 4.
\end{cases}$$
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**.
- $f_1 : \mathbb{F}_{3^2} \rightarrow \mathbb{F}_3$ defined as $f_1(x) = \text{Tr}_2(x^2)$
  Walsh spectrum: $\{3, 3\epsilon_3, 3\epsilon_3^2\} \Rightarrow \text{regular bent}$. 

A. Çeşmelioğlu (OvGU)

On the normality of $p$-ary bent functions
Weakly regular bent functions

**Definition**

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

**Example**

- \( f_2 : \mathbb{F}_{3^4} \to \mathbb{F}_3 \) defined as \( f_2(x) = \text{Tr}_4(2x^{14}) \)
  
  Walsh spectrum: \( \{-9, -9\epsilon_3, -9\epsilon_3^2\} \Rightarrow \text{weakly regular bent} \),

- \( f_3 : \mathbb{F}_{3^3} \to \mathbb{F}_3 \) defined as \( f_3(x) = \text{Tr}_3(2x^2) \)
  
  Walsh spectrum: \( \{i3\sqrt{3}, i3\sqrt{3}\epsilon_3, i3\sqrt{3}\epsilon_3^2\} \Rightarrow \text{weakly regular bent} \).

**Remark:**

regular bent \( \Rightarrow \) weakly regular bent.
For odd $p$ [Kumar, Scholz, Welch ’85]

$$\zeta_b = \begin{cases} 
\pm 1 & n \text{ is even or } n \text{ is odd and } p \equiv 1 \text{ mod } 4, \\ 
\pm i & n \text{ is odd and } p \equiv 3 \text{ mod } 4.
\end{cases}$$
Not weakly regular bent functions

**Definition**

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

**Example**

\( f_4 : \mathbb{F}_3 \rightarrow \mathbb{F}_3 \) defined as \( f_4(x) = \text{Tr}_3(x^8 + x^{22}) \)

Walsh spectrum: \( \{i3\sqrt{3}, -i3\sqrt{3}, -i3\sqrt{3} \epsilon_3, -i3\sqrt{3} \epsilon_3, i3\sqrt{3} \epsilon_3^2, -i3\sqrt{3} \epsilon_3^2 \} \Rightarrow **not weakly regular bent**.
Introduced by Dobbertin(’94)

**Definition**

\[ f : \mathbb{F}_p^n \rightarrow \mathbb{F}_p, \, n = 2m \]

- \( f \) 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 \( \mathbb{F}_p^n \).

\[ \text{normal} \Rightarrow \text{weakly normal} \]

In general, it is not easy to check the normality of functions.
Normal-Weakly normal

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

Weakly Normal Functions
Affine on an $m$-dim. aff. subspace
Functions from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$, $n = 2m$

Weakly Normal Functions
Affine on an $m$-dim. aff. subspace

Normal Functions
Constant on an $m$-dim. aff. subspace
Normality is defined for arbitrary functions but we consider bent functions only.

- **Maiorana-McFarland bent functions:**
  \[ f : \mathbb{F}_p^m \times \mathbb{F}_p^m \rightarrow \mathbb{F}_p \text{ defined as} \]
  \[ f(x, y) = \langle x, \pi(y) \rangle + h(y), \]

  \[ \pi : \mathbb{F}_p^m \rightarrow \mathbb{F}_p^m : \text{a permutation of } \mathbb{F}_p^m \]

  \[ h : \mathbb{F}_p^m \rightarrow \mathbb{F}_p : \text{an arbitrary function} \]
Normality is defined for arbitrary functions but we consider bent functions only.

- **Maiorana-McFarland bent functions:**
  \[ f : \mathbb{F}_p^m \times \mathbb{F}_p^m \to \mathbb{F}_p \text{ defined as} \]
  \[ f(x, y) = \langle x, \pi(y) \rangle + h(y), \]
  \[ \pi : \mathbb{F}_p^m \to \mathbb{F}_p^m : \text{a permutation of } \mathbb{F}_p^m \]
  \[ h : \mathbb{F}_p^m \to \mathbb{F}_p : \text{an arbitrary function} \]
  \[ f \text{ is normal since } f(x, y) = 0 \text{ on the } m\text{-dimensional subspace } \mathbb{F}_p^m \times \{ \pi^{-1}(0) \}. \]
Normality of Classical Examples

\[ PS^+ \text{ bent functions:} \]

\[ V_i : m\text{-dimensional subspace of } F_2^{2m}, \ 1 \leq i \leq 2^{m-1} + 1, \]

\[ f : F_2^{2m} \rightarrow F_2, \]

\[ f(x) = 1 \text{ on each } V_i. \]
\( P S^+ \) bent functions:

\( V_i : m \)-dimensional subspace of \( \mathbb{F}_{2^m} \), \( 1 \leq i \leq 2^{m-1} + 1 \),
\( f : \mathbb{F}_{2^m} \rightarrow \mathbb{F}_2 \),
\[
f(x) = 1 \text{ on each } V_i.
\]

\( f \) is normal.
\(\mathcal{P}S^+\) bent functions:

\(V_i: m\)-dimensional subspace of \(\mathbb{F}_{2^m}^2\), \(1 \leq i \leq 2^{m-1} + 1\),

\(f: \mathbb{F}_{2^m} \rightarrow \mathbb{F}_2\),

\[f(x) = 1\] on each \(V_i\).

\(f\) is \textit{normal}.

\(\mathcal{P}S_{\text{ap}}\) bent functions:

\(g: \mathbb{F}_{p^m} \rightarrow \mathbb{F}_p\): a balanced function with \(g(0) = 0\).

\(f: \mathbb{F}_{p^m} \times \mathbb{F}_{p^m} \rightarrow \mathbb{F}_p\) 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 $\mathbb{F}_2^{2m}$, $1 \leq i \leq 2^{m-1} + 1$,
  
  $f: \mathbb{F}_2^{2m} \rightarrow \mathbb{F}_2$,
  
  \[ f(x) = 1 \text{ on each } V_i. \]
  
  $f$ is **normal**.

- **$\mathcal{PS}_{ap}$ bent functions:**
  
  $g: \mathbb{F}_p^m \rightarrow \mathbb{F}_p$: a balanced function with $g(0) = 0$.
  
  $f: \mathbb{F}_p^m \times \mathbb{F}_p^m \rightarrow \mathbb{F}_p$ defined as $f(x, y) = g(xy^{p^m-2})$ is a bent function.
  
  \[ f(x, y) = 0 \text{ on } \{0\} \times \mathbb{F}_p^m \Rightarrow f \text{ is normal}. \]
Lemma (Ç., Meidl, Pott 2013)

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

Let $p$ be an odd prime, $n = 2m$, and $f : \mathbb{F}_p^n \to \mathbb{F}_p$ 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 $E^\perp$. 

A. Çeşmelioğlu (OvGU)
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 \textit{weakly regular bent} but not regular then \( f \) is not \textit{weakly normal}.

(ii) If \( f \) is \textit{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.
**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.

(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 $E^\perp$. 
Example 1:

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

$f(x) = \text{Tr}_4(\omega^{10}x^{22} + x^4)$ is normal since $f(x) = 0$ on $E = \text{span}\{\omega, \omega^3 + \omega^2\}$.
Example 1:

\[ f : \mathbb{F}_3^4 \to \mathbb{F}_3, \, \omega \text{ a primitive element of } \mathbb{F}_3^4. \]

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

Example 2:

\[ f : \mathbb{F}_3^6 \to \mathbb{F}_3, \omega \text{ a primitive element of } \mathbb{F}_3^6. \]

\[ f(x) = \text{Tr}_6(\omega^7x^{98}) \text{ is } \text{not normal}. \]
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

\( f_{\alpha} : \mathbb{F}_3^n \rightarrow \mathbb{F}_3 \) defined as

\[
  f_{\alpha}(x) = \text{Tr}_n(\alpha x^{\frac{3^k+1}{2}}), \quad k \text{ is odd, } \gcd(n, k) = 1.
\]

Lemma (Ç., Meidl, Pott 2013)

\( f_{\alpha} \) is regular bent if and only if

\[
\begin{align*}
  n &\equiv 0 \pmod{4} \text{ and } \alpha \text{ is a nonsquare, } \\
  \text{or} \\
  n &\equiv 2 \pmod{4} \text{ and } \alpha \text{ is a square.}
\end{align*}
\]
Theorem (Ç., Meidl, Pott 2013)

Regular bent Coulter-Matthews functions are normal.
### Summary/Open Problems-odd characteristic case

<table>
<thead>
<tr>
<th></th>
<th>N</th>
<th>WN but not N</th>
<th>NWN</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>R</strong></td>
<td>MMF ( \overline{MMF} )</td>
<td>quadratics in ( \overline{MMF} )</td>
<td>??</td>
</tr>
<tr>
<td><strong>WR but not R</strong></td>
<td>–</td>
<td>–</td>
<td>All</td>
</tr>
<tr>
<td><strong>NWR</strong></td>
<td>Ex. 1</td>
<td>Ex. 2??</td>
<td>Ex. 2??</td>
</tr>
</tbody>
</table>

**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