Results on characterizations of plateaued functions in arbitrary characteristic

Sihem Mesnager[1] Ferruh Özbudak[2] Ahmet Sınak[3]

[1]Department of Mathematics, University of Paris VIII, LAGA, University of Paris XIII and Telecom ParisTech, France
[2]Department of Mathematics and Institute of Applied Mathematics, Middle East Technical University, Turkey
[3]Institute of Applied Mathematics, Middle East Technical University, Turkey

BalkanCryptSec 2015
Koper, Slovenia

September 3, 2015

Outline

- Basic tools
- **Part 1:**
  - Characterizations of bent functions
  - Characterizations of plateaued functions
- **Part 2:**
  - Characterizations of vectorial bent functions
  - Characterizations of vectorial s-plateaued functions
- Conclusion

Setting

- p is any odd prime number and m, n are positive integers

Setting

- p is any odd prime number and m, n are positive integers
- $\mathbb{F}_{p^n}$ is the finite field of order p^n

Setting

- p is any odd prime number and m, n are positive integers
- $\mathbb{F}_{p^n}$ is the finite field of order p^n
- ϵ_p is a primitive p-th root of unity in $\mathbb{C}$

Setting

- p is any odd prime number and m, n are positive integers
- $\mathbb{F}_{p^n}$ is the finite field of order p^n
- ϵ_p is a primitive p-th root of unity in $\mathbb{C}$
- $\mathrm{Tr}(\alpha) = \alpha + \alpha^p + \cdots + \alpha^{p^{n-1}}$ is the *trace* of $\alpha \in \mathbb{F}_{p^n}$ over $\mathbb{F}_p$

Setting

- p is any odd prime number and m, n are positive integers
- $\mathbb{F}_{p^n}$ is the finite field of order p^n
- ϵ_p is a primitive p-th root of unity in $\mathbb{C}$
- $\mathrm{Tr}(\alpha) = \alpha + \alpha^p + \cdots + \alpha^{p^{n-1}}$ is the *trace* of $\alpha \in \mathbb{F}_{p^n}$ over $\mathbb{F}_p$
- $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ is a p-ary $(n, 1)$ function

Setting

- p is any odd prime number and m, n are positive integers
- $\mathbb{F}_{p^n}$ is the finite field of order p^n
- ϵ_p is a primitive p-th root of unity in $\mathbb{C}$
- $\mathrm{Tr}(\alpha) = \alpha + \alpha^p + \cdots + \alpha^{p^{n-1}}$ is the *trace* of $\alpha \in \mathbb{F}_{p^n}$ over $\mathbb{F}_p$
- $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ is a p-ary $(n, 1)$ function
- $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$ is a p-ary (n, m) function

Setting

For a p-ary $(n, 1)$ function f, the derivative of f at $a \in \mathbb{F}_{p^n}$ is a map defined as

$$\begin{aligned} \mathcal{D}_a f : &\mathbb{F}_{p^n} \to \mathbb{F}_p \\ &x \longmapsto \mathcal{D}_a f(x) = f(x+a) - f(x), \ \forall x \in \mathbb{F}_{p^n} \end{aligned}$$

Setting

For a p-ary $(n, 1)$ function f, the derivative of f at $a \in \mathbb{F}_{p^n}$ is a map defined as

$$\begin{aligned} \mathcal{D}_a f : &\mathbb{F}_{p^n} \to \mathbb{F}_p \\ &x \longmapsto \mathcal{D}_a f(x) = f(x+a) - f(x), \ \forall x \in \mathbb{F}_{p^n} \end{aligned}$$

For a p-ary (n, m) function F, the derivative of F at $a \in \mathbb{F}_{p^n}$ is a map defined as

$$\begin{aligned} \mathcal{D}_a F : &\mathbb{F}_{p^n} \to \mathbb{F}_{p^m} \\ &x \longmapsto \mathcal{D}_a F(x) = F(x+a) - F(x), \ \forall x \in \mathbb{F}_{p^n} \end{aligned}$$

Setting

For a p-ary $(n, 1)$ function f, the *Walsh transform* of f at $\omega \in \mathbb{F}_{p^n}$ is a map defined as

$$\widehat{\chi_f} : \mathbb{F}_{p^n} \to \mathbb{C}$$
$$\omega \longmapsto \widehat{\chi_f}(\omega) = \sum_{x \in \mathbb{F}_{p^n}} \epsilon_p^{f(x) - Tr(\omega x)}.$$

Setting

For a p-ary $(n, 1)$ function f, the *Walsh transform* of f at $\omega \in \mathbb{F}_{p^n}$ is a map defined as

$$\widehat{\chi_f} : \mathbb{F}_{p^n} \to \mathbb{C}$$
$$\omega \longmapsto \widehat{\chi_f}(\omega) = \sum_{x \in \mathbb{F}_{p^n}} \epsilon_p^{f(x) - Tr(\omega x)}.$$

- f is called a *bent* function if $|\widehat{\chi_f}(\omega)| = p^{\frac{n}{2}}$ for all $\omega \in \mathbb{F}_{p^n}$

Setting

For a p-ary $(n, 1)$ function f, the *Walsh transform* of f at $\omega \in \mathbb{F}_{p^n}$ is a map defined as

$$\widehat{\chi_f} : \mathbb{F}_{p^n} \to \mathbb{C}$$
$$\omega \longmapsto \widehat{\chi_f}(\omega) = \sum_{x \in \mathbb{F}_{p^n}} \epsilon_p^{f(x) - Tr(\omega x)}.$$

- f is called a *bent* function if $|\widehat{\chi_f}(\omega)| = p^{\frac{n}{2}}$ for all $\omega \in \mathbb{F}_{p^n}$
- f is called an *s-plateaued* function if $|\widehat{\chi_f}(\omega)| \in \left\{0, p^{\frac{n+s}{2}}\right\}$ for all $\omega \in \mathbb{F}_{p^n}$ where $0 \leq s \leq n$

Setting

The sequence of the even power moments of the Walsh transform of f

For any non negative integer i,

$$S_i(f) = \sum_{\omega \in \mathbb{F}_{p^n}} |\widehat{\chi_f}(\omega)|^{2i}$$

Setting

The sequence of the even power moments of the Walsh transform of f

For any non negative integer i,

$$S_i(f) = \sum_{\omega \in \mathbb{F}_{p^n}} |\widehat{\chi_f}(\omega)|^{2i}$$

In [Mesnager, 2014],
for every integer A and every non-negative integer i, the following equation holds

$$\sum_{\omega \in \mathbb{F}_{p^n}} \left(|\widehat{\chi_f}(\omega)|^2 - A\right)^2 |\widehat{\chi_f}(\omega)|^{2i} = S_{i+2}(f) - 2AS_{i+1}(f) + A^2 S_i(f). \quad (1)$$

Part 1: Characterizations of s-plateaued $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$

By $S_i(f) = \sum_{\omega \in \mathbb{F}_{p^n}} |\widehat{\chi_f}(\omega)|^{2i}$

Theorem (Mesnager, 2014)

f is s-plateaued $\iff S_i(f) \cdot S_i(f) = S_{i+1}(f) \cdot S_{i-1}(f)$ *for* $i \geq 2$.

Part 1: Characterizations of s-plateaued $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$

By $S_i(f) = \sum_{\omega \in \mathbb{F}_{p^n}} |\widehat{\chi_f}(\omega)|^{2i}$

Theorem (Mesnager, 2014)

f is s-plateaued $\iff S_i(f) \cdot S_i(f) = S_{i+1}(f) \cdot S_{i-1}(f)$ *for* $i \geq 2$.

Theorem

f is s-plateaued $\iff S_i(f) \cdot S_j(f) = S_{i+1}(f) \cdot S_{j-1}(f)$ $\forall i \geq 1, j \geq 2$.

Part 1: Characterizations of s-plateaued $f : \mathbb{F}_{p^n} \longrightarrow \mathbb{F}_p$

By $S_i(f) = \sum_{\omega \in \mathbb{F}_{p^n}} |\widehat{\chi_f}(\omega)|^{2i}$

Theorem (Mesnager, 2014)

f is s-plateaued $\iff S_i(f) \cdot S_i(f) = S_{i+1}(f) \cdot S_{i-1}(f)$ *for* $i \geq 2$.

Theorem

f is s-plateaued $\iff S_i(f) \cdot S_j(f) = S_{i+1}(f) \cdot S_{j-1}(f)$ $\forall i \geq 1, j \geq 2$.

Actually, they are equivalent.

▸ Proof?

New characterizations of s-plateaued $f : \mathbb{F}_{p^n} \longrightarrow \mathbb{F}_p$

Theorem

$$f \text{ is } s\text{-plateaued} \iff S_2(f) = p^{3n+s} \text{ and } S_3(f) = p^{4n+2s}$$

New characterizations of s-plateaued $f : \mathbb{F}_{p^n} \longrightarrow \mathbb{F}_p$

Theorem

$$f \text{ is } s\text{-plateaued} \iff S_2(f) = p^{3n+s} \text{ and } S_3(f) = p^{4n+2s}$$

Proof.

- By (1) with $A = p^{n+s}$ and $i = 0$,

$$\begin{aligned} \sum_{\omega \in \mathbb{F}_{p^n}} \left(|\widehat{\chi_f}(\omega)|^2 - p^{n+s} \right)^2 &= S_2(f) - 2p^{n+s} S_1(f) + p^{2n+2s} \cdot S_0(f) \\ &= (p^n - p^{n-s})(-p^{n+s})^2 \end{aligned}$$

  By (1) with $A = p^{n+s}$ and $i = 1$, $S_3(f) = p^{4n+2s}$.
- Conversely, by (1) with $A = p^{n+s}$ and $i = 1$,

$$\sum_{\omega \in \mathbb{F}_{p^n}} (|\widehat{\chi_f}(\omega)|^2 - p^{n+s})^2 |\widehat{\chi_f}(\omega)|^2 = S_3(f) - 2p^{n+s} S_2(f) + p^{2n+2s} S_1(f) = 0.$$

New characterizations of s-plateaued $f : \mathbb{F}_{p^n} \longrightarrow \mathbb{F}_p$

Theorem

f is s-plateaued $\iff$ $S_2(f) = p^{3n+s}$ *and* $S_3(f) = p^{4n+2s}$

Proof.

- By (1) with $A = p^{n+s}$ and $i = 0$,

$$\begin{aligned}\sum_{\omega \in \mathbb{F}_{p^n}} \left(|\widehat{\chi_f}(\omega)|^2 - p^{n+s}\right)^2 &= S_2(f) - 2p^{n+s}S_1(f) + p^{2n+2s} \cdot S_0(f) \\ &= (p^n - p^{n-s})(-p^{n+s})^2\end{aligned}$$

  By (1) with $A = p^{n+s}$ and $i = 1$, $S_3(f) = p^{4n+2s}$.
- Conversely, by (1) with $A = p^{n+s}$ and $i = 1$,

$$\sum_{\omega \in \mathbb{F}_{p^n}} (|\widehat{\chi_f}(\omega)|^2 - p^{n+s})^2 |\widehat{\chi_f}(\omega)|^2 = S_3(f) - 2p^{n+s}S_2(f) + p^{2n+2s}S_1(f) = 0.$$

Corollary

If f is s-plateaued, then $S_i(f) = p^{(i+1)n+(i-1)s}$ for $i \geq 1$.

New characterizations of s-plateaued $f : \mathbb{F}_{p^n} \longrightarrow \mathbb{F}_p$

Theorem

f *is* s*-plateaued* $\iff$ $S_2(f) = p^{3n+s}$ *and* $S_3(f) = p^{4n+2s}$

Proof.

- By (1) with $A = p^{n+s}$ and $i = 0$,

$$\begin{aligned}\sum_{\omega\in\mathbb{F}_{p^n}} \left(|\widehat{\chi_f}(\omega)|^2 - p^{n+s}\right)^2 &= S_2(f) - 2p^{n+s}S_1(f) + p^{2n+2s}\cdot S_0(f)\\ &= (p^n - p^{n-s})(-p^{n+s})^2\end{aligned}$$

  By (1) with $A = p^{n+s}$ and $i = 1$, $S_3(f) = p^{4n+2s}$.
- Conversely, by (1) with $A = p^{n+s}$ and $i = 1$,

$$\sum_{\omega\in\mathbb{F}_{p^n}} (|\widehat{\chi_f}(\omega)|^2 - p^{n+s})^2|\widehat{\chi_f}(\omega)|^2 = S_3(f) - 2p^{n+s}S_2(f) + p^{2n+2s}S_1(f) = 0.$$

Corollary

If f *is* s*-plateaued, then* $S_i(f) = p^{(i+1)n+(i-1)s}$ *for* $i \geq 1$.

In particular, if f *is bent, then* $S_i(f) = p^{(i+1)n}$ *for* $i \geq 0$.

Characterizations of s-plateaued $f : \mathbb{F}_{p^n} \longrightarrow \mathbb{F}_p$

Theorem

f is s-plateaued if and only if

$$\sum_{a,b \in \mathbb{F}_{p^n}} \epsilon_p^{\mathcal{D}_b \mathcal{D}_a f(x)} = \theta \quad \forall x \in \mathbb{F}_{p^n} \tag{2}$$

with $\theta = p^{n+s}$. In particular, f is bent if and only if $\theta = p^n$ for $s = 0$.

Characterizations of s-plateaued $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$

Theorem

f is s-plateaued if and only if

$$\sum_{a,b \in \mathbb{F}_{p^n}} \epsilon_p^{\mathcal{D}_b \mathcal{D}_a f(x)} = \theta \quad \forall x \in \mathbb{F}_{p^n} \tag{2}$$

with $\theta = p^{n+s}$. In particular, f is bent if and only if $\theta = p^n$ for $s = 0$.

Sketch of the proof.

For all $x \in \mathbb{F}_{p^n}$,

1. $\sum_{a,b \in \mathbb{F}_{p^n}} \epsilon_p^{f(x+a+b)-f(x+a)-f(x+b)} = \theta \cdot \epsilon_p^{-f(x)}$

Characterizations of s-plateaued $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$

Theorem

f is s-plateaued if and only if

$$\sum_{a,b \in \mathbb{F}_{p^n}} \epsilon_p^{\mathcal{D}_b \mathcal{D}_a f(x)} = \theta \quad \forall x \in \mathbb{F}_{p^n} \tag{2}$$

with $\theta = p^{n+s}$. In particular, f is bent if and only if $\theta = p^n$ for $s = 0$.

Sketch of the proof.

For all $x \in \mathbb{F}_{p^n}$,

1. $\sum_{a,b \in \mathbb{F}_{p^n}} \epsilon_p^{f(x+a+b)-f(x+a)-f(x+b)} = \theta \cdot \epsilon_p^{-f(x)}$
2. $G_1(x) = \sum_{a_1,b_1 \in \mathbb{F}_{p^n}} \epsilon_p^{f(a_1+b_1-x)-f(a_1)-f(b_1)} = \theta \cdot \epsilon_p^{-f(x)} = G_2(x)$

Characterizations of s-plateaued $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$

Theorem

f is s-plateaued if and only if

$$\sum_{a,b \in \mathbb{F}_{p^n}} \epsilon_p^{\mathcal{D}_b \mathcal{D}_a f(x)} = \theta \quad \forall x \in \mathbb{F}_{p^n} \tag{2}$$

with $\theta = p^{n+s}$. In particular, f is bent if and only if $\theta = p^n$ for $s = 0$.

Sketch of the proof.

For all $x \in \mathbb{F}_{p^n}$,

1. $\sum_{a,b \in \mathbb{F}_{p^n}} \epsilon_p^{f(x+a+b)-f(x+a)-f(x+b)} = \theta \cdot \epsilon_p^{-f(x)}$
2. $G_1(x) = \sum_{a_1,b_1 \in \mathbb{F}_{p^n}} \epsilon_p^{f(a_1+b_1-x)-f(a_1)-f(b_1)} = \theta \cdot \epsilon_p^{-f(x)} = G_2(x)$

   For all $\omega \in \mathbb{F}_{p^n}$,
3. $\widehat{G_1}(\omega) = \widehat{G_2}(\omega)$
4. $\widehat{G_1}(\omega) = \widehat{\chi_f}(-\omega) \cdot (-\widehat{\chi_f})(\omega) \cdot (-\widehat{\chi_f})(\omega)$ and $\widehat{G_2}(\omega) = \theta \cdot (-\widehat{\chi_f})(\omega)$

Characterizations of s-plateaued $f : \mathbb{F}_{p^n} \longrightarrow \mathbb{F}_p$

Theorem

f is s-plateaued if and only if

$$\sum_{a,b \in \mathbb{F}_{p^n}} \epsilon_p^{\mathcal{D}_b \mathcal{D}_a f(x)} = \theta \quad \forall x \in \mathbb{F}_{p^n} \tag{2}$$

with $\theta = p^{n+s}$. In particular, f is bent if and only if $\theta = p^n$ for $s = 0$.

Sketch of the proof.

For all $x \in \mathbb{F}_{p^n}$,

1. $\sum_{a,b \in \mathbb{F}_{p^n}} \epsilon_p^{f(x+a+b)-f(x+a)-f(x+b)} = \theta \cdot \epsilon_p^{-f(x)}$
2. $G_1(x) = \sum_{a_1,b_1 \in \mathbb{F}_{p^n}} \epsilon_p^{f(a_1+b_1-x)-f(a_1)-f(b_1)} = \theta \cdot \epsilon_p^{-f(x)} = G_2(x)$

   For all $\omega \in \mathbb{F}_{p^n}$,
3. $\widehat{G_1}(\omega) = \widehat{G_2}(\omega)$
4. $\widehat{G_1}(\omega) = \widehat{\chi_f}(-\omega) \cdot (-\widehat{\chi_f})(\omega) \cdot (-\widehat{\chi_f})(\omega)$ and $\widehat{G_2}(\omega) = \theta \cdot (-\widehat{\chi_f})(\omega)$
5. Recall that $(-\widehat{\chi_f})(\omega) = \overline{\widehat{\chi_f}(-\omega)}$

Characterizations of s-plateaued $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$

Theorem

f is s-plateaued if and only if

$$\sum_{a,b \in \mathbb{F}_{p^n}} \epsilon_p^{\mathcal{D}_b \mathcal{D}_a f(x)} = \theta \quad \forall x \in \mathbb{F}_{p^n} \tag{2}$$

with $\theta = p^{n+s}$. In particular, f is bent if and only if $\theta = p^n$ for $s = 0$.

Sketch of the proof.

For all $x \in \mathbb{F}_{p^n}$,

1. $\sum_{a,b \in \mathbb{F}_{p^n}} \epsilon_p^{f(x+a+b)-f(x+a)-f(x+b)} = \theta \cdot \epsilon_p^{-f(x)}$
2. $G_1(x) = \sum_{a_1,b_1 \in \mathbb{F}_{p^n}} \epsilon_p^{f(a_1+b_1-x)-f(a_1)-f(b_1)} = \theta \cdot \epsilon_p^{-f(x)} = G_2(x)$

   For all $\omega \in \mathbb{F}_{p^n}$,
3. $\widehat{G_1}(\omega) = \widehat{G_2}(\omega)$
4. $\widehat{G_1}(\omega) = \widehat{\chi_f}(-\omega) \cdot (-\widehat{\chi_f})(\omega) \cdot (-\widehat{\chi_f})(\omega)$ and $\widehat{G_2}(\omega) = \theta \cdot (-\widehat{\chi_f})(\omega)$
5. Recall that $(-\widehat{\chi_f})(\omega) = \overline{\widehat{\chi_f}(-\omega)}$
6. $\widehat{\chi_f}(-\omega) \cdot \overline{\widehat{\chi_f}(-\omega)} \cdot \overline{\widehat{\chi_f}(-\omega)} = \theta \cdot \overline{\widehat{\chi_f}(-\omega)}$

Characterizations of s-plateaued $f : \mathbb{F}_{p^n} \longrightarrow \mathbb{F}_p$

Theorem

f is s-plateaued if and only if

$$\sum_{a,b \in \mathbb{F}_{p^n}} \epsilon_p^{\mathcal{D}_b \mathcal{D}_a f(x)} = \theta \quad \forall x \in \mathbb{F}_{p^n} \tag{2}$$

with $\theta = p^{n+s}$. In particular, f is bent if and only if $\theta = p^n$ for $s = 0$.

Sketch of the proof.

For all $x \in \mathbb{F}_{p^n}$,

1. $\sum_{a,b \in \mathbb{F}_{p^n}} \epsilon_p^{f(x+a+b)-f(x+a)-f(x+b)} = \theta \cdot \epsilon_p^{-f(x)}$
2. $G_1(x) = \sum_{a_1,b_1 \in \mathbb{F}_{p^n}} \epsilon_p^{f(a_1+b_1-x)-f(a_1)-f(b_1)} = \theta \cdot \epsilon_p^{-f(x)} = G_2(x)$

   For all $\omega \in \mathbb{F}_{p^n}$,
3. $\widehat{G_1}(\omega) = \widehat{G_2}(\omega)$
4. $\widehat{G_1}(\omega) = \widehat{\chi_f}(-\omega) \cdot (-\widehat{\chi_f})(\omega) \cdot (-\widehat{\chi_f})(\omega)$ and $\widehat{G_2}(\omega) = \theta \cdot (-\widehat{\chi_f})(\omega)$
5. Recall that $(-\widehat{\chi_f})(\omega) = \overline{\widehat{\chi_f}(-\omega)}$
6. $\widehat{\chi_f}(-\omega) \cdot \overline{\widehat{\chi_f}(-\omega)} \cdot \overline{\widehat{\chi_f}(-\omega)} = \theta \cdot \overline{\widehat{\chi_f}(-\omega)}$
7. $|\widehat{\chi_f}(\omega)|^2 \in \{0, \theta\}$

New characterizations of s-plateaued $f : \mathbb{F}_{p^n} \longrightarrow \mathbb{F}_p$

Corollary

f is s-plateaued if and only if

$$\sum_{a,b,x \in \mathbb{F}_{p^n}} \epsilon_p^{\mathcal{D}_b \mathcal{D}_a f(x)} = p^{2n+s}$$

New characterizations of s-plateaued $f : \mathbb{F}_{p^n} \longrightarrow \mathbb{F}_p$

Corollary

f is s-plateaued if and only if

$$\sum_{a,b,x \in \mathbb{F}_{p^n}} \epsilon_p^{\mathcal{D}_b \mathcal{D}_a f(x)} = p^{2n+s}$$

Theorem (Mesnager, 2014)

$$S_2(f) = \sum_{\omega \in \mathbb{F}_{p^n}} |\widehat{\chi_f}(\omega)|^4 = p^n \sum_{a,b,x \in \mathbb{F}_{p^n}} \epsilon_p^{\mathcal{D}_b \mathcal{D}_a f(x)}$$

New characterizations of s-plateaued $f : \mathbb{F}_{p^n} \longrightarrow \mathbb{F}_p$

Corollary

f is s-plateaued if and only if

$$\sum_{a,b,x \in \mathbb{F}_{p^n}} \epsilon_p^{\mathcal{D}_b \mathcal{D}_a f(x)} = p^{2n+s}$$

Theorem (Mesnager, 2014)

$$S_2(f) = \sum_{\omega \in \mathbb{F}_{p^n}} |\widehat{\chi_f}(\omega)|^4 = p^n \sum_{a,b,x \in \mathbb{F}_{p^n}} \epsilon_p^{\mathcal{D}_b \mathcal{D}_a f(x)}$$

Theorem

f is s-plateaued if and only if

$$S_2(f) = p^{3n+s}.$$

Examples of s-plateaued $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$

For $p, n \geq 2$ and s, there exist p-ary s-plateaued functions.

Example

For $p = 3$, $n = 5$ and $0 \leq s \leq 4$,

- $f_1(x) = \mathrm{Tr}(x^2 + x^4 + 2x^{10})$ is 0-plateaued and $S_2(f_1) = 3^{15}$

Examples of s-plateaued $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$

For $p, n \geq 2$ and s, there exist p-ary s-plateaued functions.

Example

For $p = 3$, $n = 5$ and $0 \leq s \leq 4$,

- $f_1(x) = \mathrm{Tr}(x^2 + x^4 + 2x^{10})$ is 0-plateaued and $S_2(f_1) = 3^{15}$
- $f_2(x) = \mathrm{Tr}(x^2 + x^4 + x^{10})$ is 1-plateaued and $S_2(f_2) = 3^{16}$

Examples of s-plateaued $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$

For $p, n \geq 2$ and s, there exist p-ary s-plateaued functions.

Example

For $p = 3$, $n = 5$ and $0 \leq s \leq 4$,

- $f_1(x) = \mathrm{Tr}(x^2 + x^4 + 2x^{10})$ is 0-plateaued and $S_2(f_1) = 3^{15}$
- $f_2(x) = \mathrm{Tr}(x^2 + x^4 + x^{10})$ is 1-plateaued and $S_2(f_2) = 3^{16}$
- $f_3(x) = \mathrm{Tr}(\xi x^2 + x^4 + 2x^{10})$ is 2-plateaued and $S_2(f_3) = 3^{17}$
- $f_4(x) = \mathrm{Tr}(\xi^2 x^2 + 2x^4 + \xi^{28} x^{10})$ is 3-plateaued, $S_2(f_4) = 3^{18}$ where ξ is a primitive element of $\mathbb{F}_{3^5}$ with $\xi^5 + 2\xi + 1 = 0$

Examples of s-plateaued $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$

For $p, n \geq 2$ and s, there exist p-ary s-plateaued functions.

Example

For $p = 3$, $n = 5$ and $0 \leq s \leq 4$,

- $f_1(x) = \mathrm{Tr}(x^2 + x^4 + 2x^{10})$ is 0-plateaued and $S_2(f_1) = 3^{15}$
- $f_2(x) = \mathrm{Tr}(x^2 + x^4 + x^{10})$ is 1-plateaued and $S_2(f_2) = 3^{16}$
- $f_3(x) = \mathrm{Tr}(\xi x^2 + x^4 + 2x^{10})$ is 2-plateaued and $S_2(f_3) = 3^{17}$
- $f_4(x) = \mathrm{Tr}(\xi^2 x^2 + 2x^4 + \xi^{28} x^{10})$ is 3-plateaued, $S_2(f_4) = 3^{18}$ where ξ is a primitive element of $\mathbb{F}_{3^5}$ with $\xi^5 + 2\xi + 1 = 0$
- $f_5(x) = \mathrm{Tr}(x^2 + 2x^4 + 2x^{10})$ is the 4-plateaued, $S_2(f_5) = 3^{19}$

Characterizations of vectorial bent $F : \mathbb{F}_{p^n} \longrightarrow \mathbb{F}_{p^m}$

Part 2: The vectorial function $F : \mathbb{F}_{p^n} \longrightarrow \mathbb{F}_{p^m}$

Recall that, for a vectorial function F, f_λ from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$ for every $\lambda \in \mathbb{F}_{p^m}^\star$ is defined as

$$f_\lambda(x) = \mathrm{Tr}_1^m(\lambda F(x))$$

for all $x \in \mathbb{F}_{p^n}$. Then F is called *vectorial bent* if f_λ is bent for all $\lambda \in \mathbb{F}_{p^m}^\star$.

Characterizations of vectorial bent $F : \mathbb{F}_{p^n} \longrightarrow \mathbb{F}_{p^m}$

- In [Nyberg, 1991], F is a vectorial bent function if and only if $\mathcal{D}_a F$ is balanced for all $a \in \mathbb{F}_{p^n}^{\star}$.

Characterizations of vectorial bent $F : \mathbb{F}_{p^n} \longrightarrow \mathbb{F}_{p^m}$

- In [Nyberg, 1991], F is a vectorial bent function if and only if $\mathcal{D}_a F$ is balanced for all $a \in \mathbb{F}_{p^n}^{\star}$.
- In [Mesnager, 2014], F is a vectorial bent function if and only if

$$\mathfrak{N}(F) = \#\left\{(a, b, x) \in \mathbb{F}_{p^n}^3 | \mathcal{D}_b \mathcal{D}_a F(x) = 0\right\} = p^{2n-m}(p^n - 1) + p^{2n}.$$

Characterizations of vectorial bent $F : \mathbb{F}_{p^n} \longrightarrow \mathbb{F}_{p^m}$

- In [Nyberg, 1991], F is a vectorial bent function if and only if $\mathcal{D}_a F$ is balanced for all $a \in \mathbb{F}_{p^n}^{\star}$.
- In [Mesnager, 2014], F is a vectorial bent function if and only if

$$\mathfrak{N}(F) = \#\left\{(a, b, x) \in \mathbb{F}_{p^n}^3 | \mathcal{D}_b \mathcal{D}_a F(x) = 0\right\} = p^{2n-m}(p^n - 1) + p^{2n}.$$

Without using bentness of F,

$$\mathcal{D}_a F \text{ is balanced for all } a \in \mathbb{F}_{p^n}^{\star} \Longleftrightarrow \mathfrak{N}(F) = p^{2n-m}(p^n - 1) + p^{2n}.$$

Characterizations of vectorial bent $F : \mathbb{F}_{p^n} \longrightarrow \mathbb{F}_{p^m}$

For $x_1, x_2, \ldots, x_m$ such that $x_1 + x_2 + \cdots + x_m = n$, then we have

$$x_1^2 + x_2^2 + \cdots + x_m^2 \geq \frac{n^2}{m}.$$

The " $\geq$ " becomes " $=$ " if and only if $x_1 = x_2 = \cdots = x_m$.

Characterizations of vectorial bent $F : \mathbb{F}_{p^n} \longrightarrow \mathbb{F}_{p^m}$

For $x_1, x_2, \ldots, x_m$ such that $x_1 + x_2 + \cdots + x_m = n$, then we have

$$x_1^2 + x_2^2 + \cdots + x_m^2 \geq \frac{n^2}{m}.$$

The " $\geq$ " becomes " $=$ " if and only if $x_1 = x_2 = \cdots = x_m$.

Lemma

Let G be a vectorial function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^m}$. Then

$$\#\left\{(x_1, x_2) \in \mathbb{F}_{p^n}^2 : G(x_1) = G(x_2)\right\} \geq p^{2n-m}.$$

The " $\geq$ " becomes " $=$ " if and only if G is balanced.

▸ Proof?

Characterizations of vectorial bent $F : \mathbb{F}_{p^n} \longrightarrow \mathbb{F}_{p^m}$

Proposition

$$\mathcal{D}_a F \text{ is balanced } \forall a \in \mathbb{F}_{p^n}^{\star} \Longleftrightarrow \mathfrak{N}(F) = p^{2n-m}(p^n - 1) + p^{2n}$$

where $\mathfrak{N}(F) = \#\left\{(a, b, x) \in \mathbb{F}_{p^n}^3 | \mathcal{D}_b \mathcal{D}_a F(x) = 0\right\}$.

Characterizations of vectorial bent $F : \mathbb{F}_{p^n} \longrightarrow \mathbb{F}_{p^m}$

Proposition

$$\mathcal{D}_a F \text{ is balanced } \forall a \in \mathbb{F}_{p^n}^{\star} \Longleftrightarrow \mathfrak{N}(F) = p^{2n-m}(p^n - 1) + p^{2n}$$

where $\mathfrak{N}(F) = \#\left\{(a, b, x) \in \mathbb{F}_{p^n}^3 | \mathcal{D}_b \mathcal{D}_a F(x) = 0\right\}$.

Proof.

- Notice that $\mathcal{D}_b \mathcal{D}_a F(x) = 0$ if and only if

$$\mathcal{D}_a F(x) = \mathcal{D}_a F(x + b). \tag{3}$$

Characterizations of vectorial bent $F : \mathbb{F}_{p^n} \longrightarrow \mathbb{F}_{p^m}$

Proposition

$$\mathcal{D}_a F \text{ is balanced } \forall a \in \mathbb{F}_{p^n}^{\star} \Longleftrightarrow \mathfrak{N}(F) = p^{2n-m}(p^n - 1) + p^{2n}$$

where $\mathfrak{N}(F) = \#\left\{(a, b, x) \in \mathbb{F}_{p^n}^3 | \mathcal{D}_b \mathcal{D}_a F(x) = 0\right\}$.

Proof.

- Notice that $\mathcal{D}_b \mathcal{D}_a F(x) = 0$ if and only if

$$\mathcal{D}_a F(x) = \mathcal{D}_a F(x + b). \tag{3}$$

- For $a = 0$, we have $\#\left\{(0, b, x) \in \mathbb{F}_{p^n}^3 | \mathcal{D}_b \mathcal{D}_a F(x) = 0\right\} = p^{2n}$.

Characterizations of vectorial bent $F : \mathbb{F}_{p^n} \longrightarrow \mathbb{F}_{p^m}$

Proposition

$$\mathcal{D}_a F \text{ is balanced } \forall a \in \mathbb{F}_{p^n}^{\star} \Longleftrightarrow \Re(F) = p^{2n-m}(p^n - 1) + p^{2n}$$

where $\Re(F) = \#\left\{(a, b, x) \in \mathbb{F}_{p^n}^3 | \mathcal{D}_b \mathcal{D}_a F(x) = 0\right\}$.

Proof.

- Notice that $\mathcal{D}_b \mathcal{D}_a F(x) = 0$ if and only if

$$\mathcal{D}_a F(x) = \mathcal{D}_a F(x + b). \tag{3}$$

- For $a = 0$, we have $\#\left\{(0, b, x) \in \mathbb{F}_{p^n}^3 | \mathcal{D}_b \mathcal{D}_a F(x) = 0\right\} = p^{2n}$.
- For $a \neq 0$, by previous lemma, the number of pairs $(b, x) \in \mathbb{F}_{p^n}^2$ satisfying (3) is equal to p^{2n-m} if and only if $\mathcal{D}_a F$ is balanced.

□

Characterizations of vectorial s-plateaued $F : \mathbb{F}_{p^n} \longrightarrow \mathbb{F}_{p^m}$

Definition

For a vectorial function F, f_λ from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$ for every $\lambda \in \mathbb{F}_{p^m}^\star$ is defined as

$$f_\lambda(x) = \mathrm{Tr}_1^m(\lambda F(x))$$

for all $x \in \mathbb{F}_{p^n}$. Then

- F is called *vectorial plateaued* if f_λ is plateaued for all $\lambda \in \mathbb{F}_{p^m}^\star$.

Characterizations of vectorial s-plateaued $F : \mathbb{F}_{p^n} \longrightarrow \mathbb{F}_{p^m}$

Definition

For a vectorial function F, f_λ from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$ for every $\lambda \in \mathbb{F}_{p^m}^\star$ is defined as

$$f_\lambda(x) = \mathrm{Tr}_1^m(\lambda F(x))$$

for all $x \in \mathbb{F}_{p^n}$. Then

- F is called *vectorial plateaued* if f_λ is plateaued for all $\lambda \in \mathbb{F}_{p^m}^\star$.
- F is called *vectorial s-plateaued* if f_λ is s-plateaued with the same amplitude s for all $\lambda \in \mathbb{F}_{p^m}^\star$.

Characterizations of vectorial s-plateaued $F : \mathbb{F}_{p^n} \longrightarrow \mathbb{F}_{p^m}$

Definition

For a vectorial function F, f_λ from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$ for every $\lambda \in \mathbb{F}_{p^m}^\star$ is defined as

$$f_\lambda(x) = \mathrm{Tr}_1^m(\lambda F(x))$$

for all $x \in \mathbb{F}_{p^n}$. Then

- F is called *vectorial plateaued* if f_λ is plateaued for all $\lambda \in \mathbb{F}_{p^m}^\star$.
- F is called *vectorial s-plateaued* if f_λ is s-plateaued with the same amplitude s for all $\lambda \in \mathbb{F}_{p^m}^\star$.

The vectorial plateaued functions are strictly more general than the vectorial s-plateaued function for any s. ▸ Example

Characterizations of vectorial s-plateaued $F : \mathbb{F}_{p^n} \longrightarrow \mathbb{F}_{p^m}$

Theorem

F is a vectorial s-plateaued function if and only if

$$\sum_{\lambda \in \mathbb{F}_{p^m}^{\star}} S_2(f_\lambda) = p^{3n+s}(p^m - 1) \text{ and } \sum_{\lambda \in \mathbb{F}_{p^m}^{\star}} S_3(f_\lambda) = p^{4n+2s}(p^m - 1). \quad (4)$$

Characterizations of vectorial s-plateaued $F : \mathbb{F}_{p^n} \longrightarrow \mathbb{F}_{p^m}$

Theorem

F is a vectorial s-plateaued function if and only if

$$\sum_{\lambda \in \mathbb{F}_{p^m}^{\star}} S_2(f_\lambda) = p^{3n+s}(p^m - 1) \text{ and } \sum_{\lambda \in \mathbb{F}_{p^m}^{\star}} S_3(f_\lambda) = p^{4n+2s}(p^m - 1). \quad (4)$$

Proof.

- It is obvious that (4) holds.

Characterizations of vectorial s-plateaued $F : \mathbb{F}_{p^n} \longrightarrow \mathbb{F}_{p^m}$

Theorem

F is a vectorial s-plateaued function if and only if

$$\sum_{\lambda \in \mathbb{F}_{p^m}^\star} S_2(f_\lambda) = p^{3n+s}(p^m - 1) \text{ and } \sum_{\lambda \in \mathbb{F}_{p^m}^\star} S_3(f_\lambda) = p^{4n+2s}(p^m - 1). \quad (4)$$

Proof.

- It is obvious that (4) holds.
- Conversely, by (1) with $A = p^{n+s}$ and $i = 1$, for all $\lambda \in \mathbb{F}_{p^m}^\star$

$$D_\lambda = \sum_{\omega \in \mathbb{F}_{p^n}} (|\widehat{\chi}_{f_\lambda}(\omega)|^2 - p^{n+s})^2 |\widehat{\chi}_{f_\lambda}(\omega)|^2 = S_3(f_\lambda) - 2p^{n+s} S_2(f_\lambda) + p^{2(n+s)} S_1(f_\lambda).$$

Then by (4), $\sum_{\lambda \in \mathbb{F}_{p^m}^\star} D_\lambda = (p^m - 1) \cdot (p^{4n+2s} - 2p^{4n+2s} + p^{4n+2s}) = 0$.
Finally, since $D_\lambda \geq 0$, we have $D_\lambda = 0$ for every $\lambda \in \mathbb{F}_{p^m}^\star$.

Characterizations of vectorial s-plateaued $F : \mathbb{F}_{p^n} \longrightarrow \mathbb{F}_{p^m}$

Theorem (Mesnager, 2014)

$$\sum_{\lambda \in \mathbb{F}_{p^m}^{\star}} S_2(f_\lambda) = p^{n+m}\mathfrak{N}(F) - p^{4n}$$

where $\mathfrak{N}(F) = \#\Big\{(a, b, x) \in \mathbb{F}_{p^n}^3 | \mathcal{D}_b\mathcal{D}_a F(x) = 0\Big\}$.

Characterizations of vectorial s-plateaued $F : \mathbb{F}_{p^n} \longrightarrow \mathbb{F}_{p^m}$

Theorem (Mesnager, 2014)

$$\sum_{\lambda \in \mathbb{F}_{p^m}^{\star}} S_2(f_\lambda) = p^{n+m}\mathfrak{N}(F) - p^{4n}$$

where $\mathfrak{N}(F) = \#\left\{(a,b,x) \in \mathbb{F}_{p^n}^3 | \mathcal{D}_b\mathcal{D}_a F(x) = 0\right\}$.

Theorem

F is vectorial s-plateaued if and only if

$$\mathfrak{N}(F) = p^{3n-m} + p^{2n+s} - p^{2n+s-m}$$

where $\mathfrak{N}(F) = \#\left\{(a,b,x) \in \mathbb{F}_{p^n}^3 | \mathcal{D}_b\mathcal{D}_a F(x) = 0\right\}$ *and* $S_3(f_\lambda) = p^{4n+2s}$ *for all* $\lambda \in \mathbb{F}_{p^m}^{\star}$.

Examples of vectorial s-plateaued $F : \mathbb{F}_{p^n} \longrightarrow \mathbb{F}_{p^m}$

For each odd prime p, integers m and n, there exist vectorial p-ary s-plateaued functions.

Example

For $p = 3$, $m = 2$ and $n = 6$

- $f_1(x) = \mathrm{Tr}_2^6(x^2 + x^{10})$ is the 0-plateaued function and
- $f_2(x) = \mathrm{Tr}_2^6(x^2 + 2x^{10})$ is the 1-plateaued function.

Conclusion

- Further results on characterizations of bent and s-plateaued functions

Conclusion

- Further results on characterizations of bent and s-plateaued functions
- Provided new characterizations of s-plateaued functions

Conclusion

- Further results on characterizations of bent and s-plateaued functions
- Provided new characterizations of s-plateaued functions
- Presented a direct proof of the balancedness of $\mathcal{D}_a F(x)$ and the number of zeros of $\mathcal{D}_b \mathcal{D}_a F(x)$

Conclusion

- Further results on characterizations of bent and s-plateaued functions
- Provided new characterizations of s-plateaued functions
- Presented a direct proof of the balancedness of $\mathcal{D}_a F(x)$ and the number of zeros of $\mathcal{D}_b \mathcal{D}_a F(x)$
- Introduced the vectorial s-plateaued functions and their characterizations

Main References

- C. Carlet. On the Properties of Vectorial Functions with Plateaued Components and Their Consequences on APN Functions. In *Proceedings C2SI 2015, S. El Hajji et al. (Eds.)*, LNCS 9084, pp:63-73, 2015.
- C. Carlet and E. Prouff. On plateaued functions and their constructions. In *Proceedings of Fast Software Encryption*, LNCS, 2887, pp:54-73, 2003.
- S. Mesnager. Characterizations of plateaued and bent functions in characteristic p. *Springer International Publishing Switzerland 2014, K. U. Schmidt and A. Winterhof (Eds.)*, SETA 2014, LNCS 8865, pp.72-82, 2014.
- K. Nyberg. Perfect nonlinear S-boxes. *Advances in cryptology EUROCRYPT'91 (Brighton, 1991) 378386, LNCS, 547, Srpinger*, Berlin, 1991.
- Y. Zheng, and X. Zhang. Plateaued functions. *Information and Communication Security*, Springer Berlin Heidelberg, pp:284-300, 1999.

Thanks for your attention !

Proof of result

Proof.

- Assume $i < j$ and fix $i \geq 2$, and proceed by induction on j.
- Let $j = i + 3$. We have

$$\begin{aligned} S_{i+1}(f) \cdot S_{i+1}(f) &= S_{i+2}(f) \cdot S_i(f), \\ S_{i+2}(f) \cdot S_{i+2}(f) &= S_{i+3}(f) \cdot S_{i+1}(f). \end{aligned}$$

  It follows that $S_i(f) \cdot S_{i+3}(f) = S_{i+1}(f) \cdot S_{i+2}(f)$.
- For $j = i + k$, assume that it holds.
- For $j = i + k + 1$, $S_i(f) \cdot S_{i+k+1}(f) = S_{i+1}(f) \cdot S_{i+k}(f)$.

Proof of result

Proof.

- Assume $i < j$ and fix $i \geq 2$, and proceed by induction on j.
- Let $j = i + 3$. We have

$$\begin{aligned} S_{i+1}(f) \cdot S_{i+1}(f) &= S_{i+2}(f) \cdot S_i(f), \\ S_{i+2}(f) \cdot S_{i+2}(f) &= S_{i+3}(f) \cdot S_{i+1}(f). \end{aligned}$$

  It follows that $S_i(f) \cdot S_{i+3}(f) = S_{i+1}(f) \cdot S_{i+2}(f)$.
- For $j = i + k$, assume that it holds.
- For $j = i + k + 1$, $S_i(f) \cdot S_{i+k+1}(f) = S_{i+1}(f) \cdot S_{i+k}(f)$.
- The converse is obvious for $j = i$.

□

Return

Proof of Lemma

Proof.

- Let $A_j = \{x \in \mathbb{F}_{p^n} : G(x) = y_j \in \mathbb{F}_{p^m}\}$ and $z_j = |A_j|$ for all j.
- Then

$$\begin{aligned} \left|\left\{(x_1, x_2) \in \mathbb{F}_{p^n}^2 : G(x_1) = G(x_2)\right\}\right| &= \left|\cup_{j=1}^{p^m} \left\{(x_1, x_2) \in \mathbb{F}_{p^n}^2 : x_1, x_2 \in A_j\right\}\right| \\ &= \sum_{j=1}^{p^m} |A_j|^2 = \sum_{j=1}^{p^m} z_j^2. \end{aligned}$$

- By previous fact, for $\sum_{j=1}^{p^m} z_j = p^n$ and $z_j \geq 0$, we have $\sum_{j=1}^{p^m} z_j^2 \geq p^{2n-m}$.
- G is balanced if and only if $z_1 = z_2 = \cdots = z_{p^m}$.

□

Return

Example of vectorial plateaued function

Example

For any prime p,

- f_1 is the quadratic p-ary s_1-plateaued function from $\mathbb{F}_{p^4}$ to $\mathbb{F}_p$
- f_2 is the quadratic p-ary s_2-plateaued function from $\mathbb{F}_{p^4}$ to $\mathbb{F}_p$

with $s_1 \neq s_2$. For any $\theta \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$, a function F given as

$$F(x) = f_1(x) + \theta f_2(x)$$

is the vectorial plateaued function from $\mathbb{F}_{p^4}$ to $\mathbb{F}_{p^2}$ but it is not the vectorial s-plateaued function for any integer s with $0 \leq s \leq r - 1$.

Return