Generalized plateaued functions and admissible (plateaued) functions

Sihem Mesnager
(work in common with Chunming Tang and Yanfeng Qi)

University of Paris VIII (department of Mathematics),
University of Paris XIII (LAGA), CNRS and Telecom ParisTech

The 2nd International Workshop on Boolean Functions and Their Applications
5 July 2017, Solstrand, Norway

Outline

Walsh transform

p a prime , $\zeta_p = \exp\left(\frac{2i\pi}{p}\right)$

V_n : an n-dimensional vector space over $\mathbb{Z}_p$

$a \cdot x$: any inner product on V_n

Definition

The Walsh transform of $f : V_n \to \mathbb{Z}_p$ *at* $a \in V_n$ *is*

$$\widehat{\chi_f}(a) = \sum_{x \in V_n} \zeta_p^{f(x) - a \cdot x}$$

Remark

When $p = 2$, $\zeta_2 = -1$

Plateaued functions

Definition

*A function $f : V_n \to \mathbb{Z}_p$ is called a **plateaued function** if the Walsh transform $\widehat{\chi_f}$ takes at most three values.*

Facts :

- Because of Parseval identify, $|\widehat{\chi_f}(a)| \in \{0, p^{\frac{n+r}{2}}\}$ for some nonnegative integer r.
- $r = 0 \to |\widehat{\chi_f}(a)| = p^{\frac{n}{2}}$: bent functions
- $p = 2$, $r = 1$, n odd $\to |\widehat{\chi_f}(a)| \in \{0, 2^{\frac{n+1}{2}}\}$: semi-bent functions

The power $p^{\frac{n+r}{2}}$ is called the amplitude of f.

Plateaued functions

Definition

*A function $f : V_n \to \mathbb{Z}_p$ is called a **plateaued function** if the Walsh transform $\widehat{\chi_f}$ takes at most three values.*

Facts :

- Because of Parseval identify, $|\widehat{\chi_f}(a)| \in \{0, p^{\frac{n+r}{2}}\}$ for some nonnegative integer r.
- $r = 0 \to |\widehat{\chi_f}(a)| = p^{\frac{n}{2}}$: bent functions
- $p = 2$, $r = 1$, n odd $\to |\widehat{\chi_f}(a)| \in \{0, 2^{\frac{n+1}{2}}\}$: semi-bent functions

The power $p^{\frac{n+r}{2}}$ is called the amplitude of f.

☞ Characterizations of plateaued functions : Carlet-Prouff 2003, Cesmelioglu-Meidl 2013, SM 2014, Carlet 2015, Hyun- Lee-Lee 2016, Carlet-SM-Ozbudak-Sinak 2017, etc.

Generalized plateaued functions

$\zeta_{p^k} = \exp\left(\frac{2i\pi}{p^k}\right)$, k a positive integer

Definition

*Let r be an nonnegative integer. A function $f : V_n \to \mathbb{Z}_{p^k}$ is called a **generalized plateaued function** with amplitude $p^{\frac{n+r}{2}}$ if the generalized Walsh transform*

$$\mathcal{H}_f(a) = \sum_{x \in V_n} \zeta_{p^k}^{f(x)} \zeta_p^{-a \cdot x}$$

has modulus 0 or $p^{\frac{n+r}{2}}$ for all $a \in V_n$.

Remark

$r = 0$: generalized bent functions introduced by Kumar, Scholtz and Welch

Example

Let f be a function from $\mathbb{Z}_2^{2k+1} = \mathbb{Z}_2^k \times \mathbb{Z}_2^{k+1}$ to $\mathbb{Z}_{2^{k+1}}$, defined as

$$f(\mathbf{x}, \mathbf{y}) = (\sum_{i=1}^{k} x_i y_i + y_{k+1}) \cdot 2^k + \sum_{i=1}^{k} y_i 2^{i-1},$$

where $\mathbf{x} = (x_1, \cdots, x_k) \in \mathbb{Z}_2^k$ and $\mathbf{y} = (y_1, \cdots, y_{k+1}) \in \mathbb{Z}_2^{k+1}$. Then for any $\mathbf{u} = (u_1, \cdots, u_k) \in \mathbb{Z}_2^k$ and $\mathbf{v} = (v_1, \cdots, v_{k+1}) \in \mathbb{Z}_2^{k+1}$, one has

$$|\mathcal{H}_f(\mathbf{u}, \mathbf{v})| = \begin{cases} 2^{\frac{(2k+1)+1}{2}} & \text{if } v_{k+1} = 1, \\ 0 & \text{if } v_{k+1} = 0. \end{cases}$$

f is generalized plateaued with amplitude $2^{\frac{(2k+1)+1}{2}}$

Notation

There is an one-to-one correspondence between $\mathbb{Z}_{p^k}$ and $\mathbb{Z}_p^k$:

Every $u \in \mathbb{Z}_{p^k}$ can be uniquely expressed in the form

$$u = \sum_{i=1}^{k} u_i p^{i-1}, \quad u_i \in \mathbb{Z}_p$$

u_i shall be called the ith-digit of u in the p-base representation of u.

In the sequel, we shall often use the same notation to denote an element u of $\mathbb{Z}_{p^k}$ and the sequence $u = (u_1, \ldots, u_k)$ of its digits.

Component functions

Given a $\mathbb{Z}_{p^k}$-valued function f, define

$$f_c = f_k + \sum_{i=1}^{k-1} c_i f_i, \quad c = (c_1, \ldots, c_{k-1}) \in \mathbb{Z}_p^{k-1}.$$

f_c : a component function of f ;

f_i : ith-digit of f.

Component functions

Given a $\mathbb{Z}_{p^k}$-valued function f, define

$$f_c = f_k + \sum_{i=1}^{k-1} c_i f_i, \quad c = (c_1, \ldots, c_{k-1}) \in \mathbb{Z}_p^{k-1}.$$

f_c : a component function of f ;

f_i : ith-digit of f.

When $p = 2$, if f is a generalized bent function from V_n to $\mathbb{Z}_{p^k}$:

THEOREM (MARTINSEN, MEIDL, STANICA)

If n is even then f_c is bent for all $c \in \mathbb{Z}_p^k$.

THEOREM (MARTINSEN, MEIDL, SM, STANICA)

If n is odd then f_c is semi-bent for all $c \in \mathbb{Z}_p^k$.

Component functions of a generalized plateaued function

Theorem

If $f : V_n \to \mathbb{Z}_{p^k}$ is a generalized plateaued function with amplitude $p^{\frac{n+r}{2}}$ then :

1. *if p is odd or if $p = 2$ and $n + r$ is even, f_c is plateaued with amplitude $p^{\frac{n+r}{2}}$*
2. *if $p = 2$, $n + r$ is odd and $k \geq 3$, f_c is plateaued with amplitude $2^{\frac{n+r+1}{2}}$*

Remark

For $r = 0$ and p odd (generalized bent functions), it has been also established independently by Wang, Wu and Liu.

Sketch of proof

k a positive integer

A basis of the vectorspace $\mathbb{Q}(\zeta_{p^k})$ over $K := \mathbb{Q}(\zeta_p)$ is $\{\zeta_{p^k}^u, \ 0 \le u \le p^{k-1} - 1\}$.

The (unique) decomposition of a Walsh coefficient over this basis is :

$$\mathcal{H}_f(a) \quad = \quad \sum_{x \in V_n} \zeta_{p^k}^{f(x)} \zeta_p^{-a \cdot x} = \sum_{u \in \mathbb{Z}_p^{k-1}} \zeta_{p^k}^u \sum_{x \in W_u} \zeta_p^{f_k(x) - a \cdot x} \in \mathbb{Q}(\zeta_{p^k})$$

where $W_u = \{x \in V_n \mid f_1(x) = u_1, \ldots, f_{k-1}(x) = u_{k-1}\}$.

Sketch of proof

k a positive integer

A basis of the vectorspace $\mathbb{Q}(\zeta_{p^k})$ over $K := \mathbb{Q}(\zeta_p)$ is $\{\zeta_{p^k}^u,\ 0 \leq u \leq p^{k-1} - 1\}$.

The (unique) decomposition of a Walsh coefficient over this basis is :

$$\mathcal{H}_f(a) \;=\; \sum_{x\in V_n} \zeta_{p^k}^{f(x)} \zeta_p^{-a\cdot x} = \sum_{u\in \mathbb{Z}_p^{k-1}} \zeta_{p^k}^{u} \sum_{x\in W_u} \zeta_p^{f_k(x)-a\cdot x} \in \mathbb{Q}(\zeta_{p^k})$$

where $W_u = \{x \in V_n \mid f_1(x) = u_1, \ldots, f_{k-1}(x) = u_{k-1}\}$.

On the other hand,

$$\widehat{\chi_{f_c}}(a) = \sum_{x\in V_n} \zeta_p^{f_c(x)-a\cdot x} = \sum_{u\in \mathbb{Z}_p^{k-1}} \zeta_p^{c\cdot u} \sum_{x\in W_u} \zeta_p^{f_k(x)-a\cdot x}$$

The two above decompositions of $\mathcal{H}_f(a)$ and $\widehat{\chi_{f_c}}(a)$ involve the same sums $S_u(a) = \sum_{x\in W_u} \zeta_p^{f_k(x)-a\cdot x} \in \mathbb{Q}(\zeta_p)$

Sketch of proof

$p^\star = \left(\frac{-1}{p}\right) p$ where $\left(\frac{\cdot}{\cdot}\right)$ denotes the Legendre symbol.

If $p = 2$, $k \geq 3$ otherwise k a positive integer

THEOREM (REGULARITY OF GENERALIZED PLATEAUED FUNCTIONS)

Let $f : V_n \to \mathbb{Z}_{p^k}$ be a generalized plateaued function with amplitude $p^{\frac{n+r}{2}}$. Then, for every $a \in V_n$,

$$\mathcal{H}_f(a) = \varepsilon(a)\sqrt{p^\star}^{n+r}\zeta_{p^k}^{g(a)}\zeta_p^{h(a)}$$

for some $\varepsilon : V_n \to \{-1, 0, 1\}$, $g : V_n \to \mathbb{Z}_{p^{k-1}}$ and $h : V_n \to \mathbb{Z}_p$.

REMARK

When $p = 2$, $p^\star = \left(\frac{-1}{2}\right) 2 = 2$.

Sketch of proof

In summary,

$$S_u(a) = \sum_{x \in W_u} \zeta_p^{f_k(x) - a \cdot x} \in \mathbb{Q}(\zeta_p) =: K$$

$$\mathcal{H}_f(a) = \sum_{u \in \mathbb{Z}_p^{k-1}} \zeta_{p^k}^u S_u(a) = \varepsilon(a) \left(\sqrt{p^\star}\right)^{n+r} \zeta_{p^k}^{g(a)} \zeta_p^{h(a)},$$

Sketch of proof

In summary,

$$S_u(a) = \sum_{x \in W_u} \zeta_p^{f_k(x) - a\cdot x} \in \mathbb{Q}(\zeta_p) =: K$$

$$\mathcal{H}_f(a) = \sum_{u \in \mathbb{Z}_p^{k-1}} \zeta_{p^k}^{u} S_u(a) = \varepsilon(a) \left(\sqrt{p^\star}\right)^{n+r} \zeta_{p^k}^{g(a)} \zeta_p^{h(a)},$$

The decomposition of $\nu := (\sqrt{p^\star})^{n+r}$ over the basis $\{\zeta_{p^k}^u,\ 0 \le u \le p^{k-1} - 1\}$ depends on the parity of p and $n + r$:

Sketch of proof

In summary,

$$S_u(a) = \sum_{x \in W_u} \zeta_p^{f_k(x) - a \cdot x} \in \mathbb{Q}(\zeta_p) =: K$$

$$\mathcal{H}_f(a) = \sum_{u \in \mathbb{Z}_p^{k-1}} \zeta_{p^k}^u S_u(a) = \varepsilon(a) \left(\sqrt{p^\star}\right)^{n+r} \zeta_{p^k}^{g(a)} \zeta_p^{h(a)},$$

The decomposition of $\nu := (\sqrt{p^\star})^{n+r}$ over the basis $\{\zeta_{p^k}^u, 0 \leq u \leq p^{k-1} - 1\}$ depends on the parity of p and $n + r$:

1. when p is odd : $\mathbb{Q}(\sqrt{p^\star}) \subset \mathbb{Q}(\zeta_p) \Rightarrow \nu \in K$.

Sketch of proof

In summary,

$$S_u(a) = \sum_{x \in W_u} \zeta_p^{f_k(x) - a \cdot x} \in \mathbb{Q}(\zeta_p) =: K$$

$$\mathcal{H}_f(a) = \sum_{u \in \mathbb{Z}_p^{k-1}} \zeta_{p^k}^u S_u(a) = \varepsilon(a) \left(\sqrt{p^\star}\right)^{n+r} \zeta_{p^k}^{g(a)} \zeta_p^{h(a)},$$

The decomposition of $\nu := (\sqrt{p^\star})^{n+r}$ over the basis $\{\zeta_{p^k}^u, 0 \leq u \leq p^{k-1} - 1\}$ depends on the parity of p and $n + r$:

1. when p is odd : $\mathbb{Q}(\sqrt{p^\star}) \subset \mathbb{Q}(\zeta_p) \Rightarrow \nu \in K$.
2. When $p = 2$: $\zeta_2 = -1$ and $K = \mathbb{Q}(\zeta_2) = \mathbb{Q}$.

   In that case, one has therefore to separate the two subcases :

Sketch of proof

In summary,

$$S_u(a) = \sum_{x \in W_u} \zeta_p^{f_k(x) - a\cdot x} \in \mathbb{Q}(\zeta_p) =: K$$

$$\mathcal{H}_f(a) = \sum_{u \in \mathbb{Z}_p^{k-1}} \zeta_{p^k}^u S_u(a) = \varepsilon(a)\left(\sqrt{p^\star}\right)^{n+r} \zeta_{p^k}^{g(a)} \zeta_p^{h(a)},$$

The decomposition of $\nu := (\sqrt{p^\star})^{n+r}$ over the basis $\{\zeta_{p^k}^u, 0 \leq u \leq p^{k-1} - 1\}$ depends on the parity of p and $n + r$:

1. when p is odd : $\mathbb{Q}(\sqrt{p^\star}) \subset \mathbb{Q}(\zeta_p) \Rightarrow \nu \in K$.
2. When $p = 2$: $\zeta_2 = -1$ and $K = \mathbb{Q}(\zeta_2) = \mathbb{Q}$.

   In that case, one has therefore to separate the two subcases :

   (a) $n + r$ even : $\nu = \sqrt{p^\star}^{n+r} = 2^{\frac{n+r}{2}} \in K$

Sketch of proof

In summary,

$$S_u(a) = \sum_{x \in W_u} \zeta_p^{f_k(x) - a \cdot x} \in \mathbb{Q}(\zeta_p) =: K$$

$$\mathcal{H}_f(a) = \sum_{u \in \mathbb{Z}_p^{k-1}} \zeta_{p^k}^u S_u(a) = \varepsilon(a) \left(\sqrt{p^\star}\right)^{n+r} \zeta_{p^k}^{g(a)} \zeta_p^{h(a)},$$

The decomposition of $\nu := (\sqrt{p^\star})^{n+r}$ over the basis $\{\zeta_{p^k}^u, \ 0 \le u \le p^{k-1} - 1\}$ depends on the parity of p and $n + r$:

1. when p is odd : $\mathbb{Q}(\sqrt{p^\star}) \subset \mathbb{Q}(\zeta_p) \Rightarrow \nu \in K$.
2. When $p = 2$: $\zeta_2 = -1$ and $K = \mathbb{Q}(\zeta_2) = \mathbb{Q}$.

   In that case, one has therefore to separate the two subcases :

   (a) $n + r$ even : $\nu = \sqrt{p^\star}^{n+r} = 2^{\frac{n+r}{2}} \in K$

   (b) $n + r$ odd : $\sqrt{p^\star}^{n+r} = 2^{\frac{n+r-1}{2}} \sqrt{2} = 2^{\frac{n+r-1}{2}} \left(\zeta_{2^k}^{2^{k-3}} - \zeta_{2^k}^{3 \cdot 2^{k-3}}\right) \in \mathbb{Q}(\zeta_{2^k}) \setminus K$

Sketch of proof

p odd or $n+r$ even, $k \geq 3$ if $p=2$ (Cases 1 or 2a)

$$\sum_{u \in \mathbb{Z}_p^{k-1}} \zeta_{p^k}^{u} \sum_{x \in W_u} \zeta_p^{f_k(x) - a \cdot x} = \varepsilon(a) \sqrt{p^\star}^{n+r} \zeta_{p^k}^{g(a)} \zeta_p^{h(a)}, \quad \sqrt{p^\star} \in \mathbb{Q}(\zeta_p)$$

Sketch of proof

p odd or $n+r$ even, $k \geq 3$ if $p = 2$ (Cases 1 or 2a)

$$\sum_{u \in \mathbb{Z}_p^{k-1}} \zeta_{p^k}^{u} \sum_{x \in W_u} \zeta_p^{f_k(x) - a \cdot x} = \varepsilon(a) \sqrt{p^\star}^{n+r} \zeta_{p^k}^{g(a)} \zeta_p^{h(a)}, \quad \sqrt{p^\star} \in \mathbb{Q}(\zeta_p)$$

Hence

$$S_u(a) = \sum_{x \in W_u} \zeta_p^{f_k(x) - a \cdot x} = \begin{cases} \varepsilon(a) \sqrt{p^\star}^{n+r} \zeta_p^{h(a)} & \text{if } u = g(a) \\ 0 & \text{otherwise} \end{cases}$$

Sketch of proof

p odd or $n+r$ even, $k \geq 3$ if $p=2$ (Cases 1 or 2a)

$$\sum_{u \in \mathbb{Z}_p^{k-1}} \zeta_{p^k}^{u} \sum_{x \in W_u} \zeta_p^{f_k(x) - a \cdot x} = \varepsilon(a) \sqrt{p^\star}^{n+r} \zeta_{p^k}^{g(a)} \zeta_p^{h(a)}, \quad \sqrt{p^\star} \in \mathbb{Q}(\zeta_p)$$

Hence

$$S_u(a) = \sum_{x \in W_u} \zeta_p^{f_k(x) - a \cdot x} = \begin{cases} \varepsilon(a) \sqrt{p^\star}^{n+r} \zeta_p^{h(a)} & \text{if } u = g(a) \\ 0 & \text{otherwise} \end{cases}$$

Thus

$$\widehat{\chi_{f_c}}(a) = \sum_{u \in \mathbb{Z}_p^{k-1}} \zeta_p^{u \cdot c} S_u(a) = S_{g(a)}(a) \zeta_p^{g(a) \cdot c}$$

f_c is plateaued with amplitude $p^{\frac{n+r}{2}}$

Sketch of proof

$p = 2$, $n + r$ odd and $k \geq 3$ (Case 2b)

$$\sum_{u \in \mathbb{Z}_2^{k-1}} \zeta_{2^k}^{u} \sum_{x \in W_u} (-1)^{f_k(x) - a \cdot x} = \varepsilon(a) 2^{\frac{n+r-1}{2}} (-1)^{h(a)} \left(\zeta_{2^k}^{g(a) + 2^{k-3}} - \zeta_{2^k}^{g(a) + 3 \cdot 2^{k-3}} \right)$$

Sketch of proof

$p=2$, $n+r$ odd and $k\geq 3$ (Case 2b)

$$\sum_{u\in\mathbb{Z}_2^{k-1}}\zeta_{2^k}^{u}\sum_{x\in W_u}(-1)^{f_k(x)-a\cdot x}=\varepsilon(a)2^{\frac{n+r-1}{2}}(-1)^{h(a)}\left(\zeta_{2^k}^{g(a)+2^{k-3}}-\zeta_{2^k}^{g(a)+3\cdot 2^{k-3}}\right)$$

Hence

$$S_u(a)=\sum_{x\in W_u}(-1)^{f_k(x)-a\cdot x}=\begin{cases}\varepsilon(a)2^{\frac{n+r-1}{2}}(-1)^{h(a)} & \text{if } u=g(a)+2^{k-3}\\ -\varepsilon(a)2^{\frac{n+r-1}{2}}(-1)^{h(a)} & \text{if } u=g(a)+3\cdot 2^{k-3}\\ 0 & \text{otherwise}\end{cases}$$

Thus

$$\widehat{\chi_{f_c}}(a)\ =\ (-1)^{(g(a)+2^{k-3})\cdot c}S_{g(a)+2^{k-3}}(a)-(-1)^{(g(a)+3\cdot 2^{k-3})\cdot c}S_{g(a)+3\cdot 2^{k-3}}(a).$$

f_c is plateaued with amplitude $2\times 2^{\frac{n+r-1}{2}}=2^{\frac{n+r+1}{2}}$

Question

Let f be a function from V_n to $\mathbb{Z}_{p^k}$ where p odd or $p = 2$ and $n + r$ even

Question : if all the f_c's are plateaued with the same amplitude, is f a generalized plateaued function ?

Question

Let f be a function from V_n to $\mathbb{Z}_{p^k}$ where p odd or $p = 2$ and $n + r$ even

Question : if all the f_c's are plateaued with the same amplitude, is f a generalized plateaued function ?

Answer : it is NOT necessary true

Question

Let f be a function from V_n to $\mathbb{Z}_{p^k}$ where p odd or $p = 2$ and $n + r$ even

Question : if all the f_c's are plateaued with the same amplitude, is f a generalized plateaued function ?

Answer : it is NOT necessary true

Generalized bent function : $r = 0$
When $p = 2$, various characterizations involving the f_c's have been found

- $k = 2$: Solé, Tokereva (2009)
- $k = 3$: Stanica et *al* (2013)
- k a positive integer : Hodzic, Pasalic (2016), Tang, Qi, Xiang, Feng (2016)

Each of them require an additional statement on the f_c's.

An important remark

Let f be a generalized plateaued function from V_n to $\mathbb{Z}_{p^k}$

Cases 1 and 2a : p be odd or $n+r$ be even

We have proved that all the component functions f_c of f have all the same amplitude but above we have shown that

LEMMA

For all $a \in V_n$, $c \in \mathbb{Z}_p^{k-1}$ and $d \in \mathbb{Z}_p^{k-1}$, we have

$$|\widehat{\chi_{f_c}}(a)| = |\widehat{\chi_{f_d}}(a)|$$

An important remark

Let f be a generalized plateaued function from V_n to $\mathbb{Z}_{p^k}$

Cases 1 and 2a : one can extend all the preceding results and show that

THEOREM

For all $H \in \mathbb{Z}_p[X_1, \ldots, X_{k-1}]$, $f_H = f_k + H(f_1, \ldots, f_{k-1})$ is plateaued with amplitude $p^{\frac{n+r}{2}}$ and, for all a in V_n, H_1 ,H_2 in $\mathbb{Z}_p[X_1, \ldots, X_k]$, we have :

$$|\widehat{\chi_{f_{H_1}}}(a)| = |\widehat{\chi_{f_{H_2}}}(a)|.$$

REMARK

$f_c = f_H$ with $H(x_1, \ldots, x_{k-1}) = \sum_{i=1}^{k-1} c_i x_i$

Admissible (plateaued) functions

From now, suppose p is odd or $p = 2$ and $n + r$ is even.

Let $\mathcal{P} = \{P_1, \ldots, P_t\}$ be a partition of V_n : $\bigcup_{i=1}^{t} P_i = \mathbb{Z}_p^n$, $P_i \cap P_j = \emptyset$, $i \neq j$.

A function $g : V_n \to \mathbb{Z}_p$ is said to be piecewise constant over $\mathcal{P}$ if it locally constant on each element of $\mathcal{P}$.

Definition

Let $f : V_n \to \mathbb{Z}_p$. Then, f is said to be r-admissible for $\mathcal{P}$ if and only if, for every piecewise constant function $g : V_n \to \mathbb{Z}_p$ over $\mathcal{P}$, $f + g$ is plateaued with amplitude $p^{\frac{n+r}{2}}$ and $|\widehat{\chi_f}(a)| = |\widehat{\chi_{f+g}}(a)|$ for all $a \in V_n$.

Example

Let f be a function from $\mathbb{Z}_2^{2k+1} = \mathbb{Z}_2^k \times \mathbb{Z}_2^{k+1}$ to $\mathbb{Z}_2$, defined as

$$f(\mathbf{x}, \mathbf{y}) = \sum_{i=1}^{k} x_i y_i + y_{k+1},$$

where $\mathbf{x} = (x_1, \cdots, x_k) \in \mathbb{Z}_2^k$ and $\mathbf{y} = (y_1, \cdots, y_{k+1}) \in \mathbb{Z}_2^{k+1}$. Let $\mathcal{P} = \{P_{\{y_1,\ldots,y_k\}} : (y_1, \cdots, y_k) \in \mathbb{Z}_2^k\}$, where $P_{\{y_1,\ldots,y_k\}} = \{(\mathbf{x}, y_1, \cdots, y_k, y_{k+1}) \in \mathbb{Z}_2^{2k+1} : \mathbf{x} \in \mathbb{Z}_2^k, y_{k+1} \in \mathbb{Z}_2\}$. Then f is 1-admissible for $\mathcal{P}$.

Admissible (plateaued) functions

Let $f : V_n \to \mathbb{Z}_p$ be a r-admissible function for a partition $\mathcal{P} = \{P_1, \ldots, P_t\}$ of V_n.

Define

$$S_i(a) = \sum_{x \in P_i} \zeta_p^{f(x) - a \cdot x}$$

Proposition

For every $1 \leq i < j \leq t$ *and* $a \in V_n$, $S_i(a)S_j(a) = 0$

Remark

The proof relies strongly on the fact that $|\widehat{\chi_f}(a)| = |\widehat{\chi_{f+g}}(a)|$ *for all* $a \in V_n$ *for every piecewise constant function* $g : V_n \to \mathbb{Z}_p$ *over* $\mathcal{P}$.

Characterization of generalized plateaued function

Let k a positive integer

Let $f : V_n \to \mathbb{Z}_{p^k}$ and f_i denotes the ith-digit of f

Let us construct a particular partition of $\mathbb{Z}_p^n$ involving the $(k-1)$st digits of f :

$$P_a = \bigcap_{i=1}^{k-1} f_i^{-1}(a_i)$$

and

$$\mathcal{P}_{f_1,\ldots,f_{k-1}} = \{P_a,\, a \in \mathbb{Z}_p^{k-1}\}.$$

Characterization of generalized plateaued function

In that case, every function g which piecewise constant for $\mathcal{P}$ can be expressed in the form $g(x) = H(f_1(x), \ldots, f_{k-1}(x))$ for some $H \in \mathbb{Z}_p[X_1, \ldots, X_{k-1}]$ and the preceding proposition rewrites as follows :

PROPOSITION

For all $a \in V_n$ *and* $(u, v) \in \left(\mathbb{Z}_p^{k-1}\right)^2$, $S_u(a)S_v(a) = 0$ *where*

$$S_u(a) = \sum_{x \in W_u} \zeta^{f(x) - a \cdot x}.$$

Characterization of generalized plateaued function

Thanks to this result, one can establish the following characterization :

Theorem

Let $f : V_n \to \mathbb{Z}_{p^k}$. Then, f is a generalized plateaued function with amplitude $p^{\frac{n+r}{2}}$ if and only if f_k is r-admissible with respect to $\mathcal{P}_{f_1,\ldots,f_{k-1}}$.

Admissible (bent) functions

0-admissible $\rightarrow$ bent functions

In that case, the equality $|\widehat{\chi_f}(a)| = |\widehat{\chi_{f+g}}(a)|$ of the modulus of Walsh coefficients is always true and the definition rewrites

DEFINITION

Let $f : V_n \rightarrow \mathbb{Z}_p$. Then, f is said to be 0-admissible for $\mathcal{P}$ if and only if, for every piecewise constant function $g : V_n \rightarrow \mathbb{Z}_p$ over $\mathcal{P}$, $f + g$ is bent.

Admissible (bent) functions

0-admissible $\rightarrow$ bent functions

In that case, the equality $|\widehat{\chi_f}(a)| = |\widehat{\chi_{f+g}}(a)|$ of the modulus of Walsh coefficients is always true and the definition rewrites

DEFINITION

Let $f : V_n \rightarrow \mathbb{Z}_p$. Then, f is said to be 0-admissible for $\mathcal{P}$ if and only if, for every piecewise constant function $g : V_n \rightarrow \mathbb{Z}_p$ over $\mathcal{P}$, $f + g$ is bent.

Thus, the preceding characterization rewrites for generalized bent functions as follows :

COROLLARY

Let $f : V_n \rightarrow \mathbb{Z}_{p^k}$. Then, f is a generalized bent function if and only if $f_k + F(f_1, \ldots, f_{k-1})$ is bent for all $F \in \mathbb{Z}_p[X_1, \ldots, X_{k-1}]$.

Case 2b

Let $f : V_n \to \mathbb{Z}_{p^k}$ be a generalized bent function with amplitude $2^{\frac{n+r}{2}}$

Let r be a nonnegative integer

Case 2b : $p = 2$ and $n + r$ odd

In that case, a component function f_c is plateaued with amplitude $2^{\frac{n+r+1}{2}}$

The preceding notion of admissible functions can not be simply adapted since, one may have for some $a \in V_n$ and $(c, d) \in \mathbb{Z}_p^{k-1}$:

$$|\widehat{\chi_{f_c(a)}}| \neq |\widehat{\chi_{f_d(a)}}|$$

The preceding characterization of generalized plateaued function when p is odd or $n + r$ is even relies strongly on the fact that $|\widehat{\chi_{f_c(a)}}| = |\widehat{\chi_{f_d(a)}}|$ for all a, c and d.

Generalized plateaued functions from other ones

Let $f : V_n \to \mathbb{Z}_{p^k}$

Suppose p is odd or $n + r$ even

Let t be a positive integer

Let $H_1, \ldots, H_t$ be functions from $\mathbb{Z}_p^{k-1}$ to $\mathbb{Z}_p$

Define

$$g(x) = p^{t-1} f_k(x) + \sum_{i=1}^{t} H_i(f_1(x), \ldots, f_{k-1}(x)) p^{i-1}$$

Then,

THEOREM

If f is a generalized plateaued function with amplitude $p^{\frac{n+r}{2}}$ the g is a generalized plateaued function with amplitude $p^{\frac{n+r}{2}}$.

Generalized plateaued functions from other ones

Let $f : V_n \to \mathbb{Z}_{p^k}$

Suppose p is odd or $n + r$ even

Let t be a positive integer

Let $H_1, \ldots, H_t$ be functions from $\mathbb{Z}_p^{k-1}$ to $\mathbb{Z}_p$

Define

$$g(x) = p^{t-1} f_k(x) + \sum_{i=1}^{t} H_i(f_1(x), \ldots, f_{k-1}(x)) p^{i-1}$$

Proof.

It is a direct consequence of the fact that at most one sum $S_u(a) = \sum_{x \in W_u} \zeta_p^{f(x) - a \cdot x}$ is non zero and whose modulus is equal to $p^{\frac{n+r}{2}}$:

$$\mathcal{H}_g(a) = \sum_{x \in V_n} \zeta_{p^t}^{g(x)} \zeta_p^{-a \cdot x} = \sum_{u \in \mathbb{Z}_p^{k-1}} \zeta_{p^t}^{\sum_{i=1}^{t} H_i(u) p^{i-1}} S_u(a) = \zeta_{p^t}^{\sum_{i=1}^{t} H_i(u) p^{i-1}} S_u(a^\star)$$

for some $a^\star \in V_n$. □

Generalized plateaued functions from other ones in lower dimension

Let $f : V_n \to \mathbb{Z}_{2^k}$
Suppose $p = 2$, $k \geq 3$ and $n + r$ odd

Define $g : \mathbb{Z}_2^n \times \mathbb{Z}_2 \to \mathbb{Z}_{2^k}$ as

$$g(x,z) = (f_k(\mathbf{x}) + zf_{k-1}(\mathbf{x}))2^{k-1} + z2^{k-2} + \sum_{i=1}^{k-2} f_i(\mathbf{x})2^{i-1}$$

$$\zeta_{2^k}^{f(x)} = (-1)^{f_k(x)}\,\zeta_4^{f_{k-1}(x)}\,\zeta_{2^k}^{\sum_{i=1}^{k-2} f_i(\mathbf{x})2^{i-1}},$$

$$\zeta_{2^k}^{g(x,0)} = \zeta_4^{-f_{k-1}(x)}\zeta_{2^k}^{f(x)} \quad \text{and} \quad \zeta_{2^k}^{g(x,1)} = (-1)^{f_{k-1}(x)}\zeta_4^{1-f_{k-1}(x)}\zeta_{2^k}^{f(x)}$$

THEOREM

f is a generalized plateaued function with amplitude $2^{\frac{n+r}{2}}$ if and only if g is a generalized plateaued function with amplitude $2^{\frac{n+r}{2}}$.

Generalized plateaued functions from other ones in lower dimension

Let $f : V_n \to \mathbb{Z}_{2^k}$

Suppose $p = 2$, $k \geq 3$ and $n + r$ even

Define $g : \mathbb{Z}_2^n \times \mathbb{Z}_2 \to \mathbb{Z}_{2^t}$ as

$$g(x,z) = 2^{t-1} f_k(x) + \sum_{i=1}^{t-1} H_i(f_1(x), \ldots, f_{k-1}(x)) 2^{i-1} + 2^{t-2} z I(f_1(x), \ldots, f_{k-1}(x))$$

where the H_i's are maps from $\mathbb{Z}_2^{k-1}$ to $\mathbb{Z}_2$ and $I : \mathbb{Z}_2^{k-1} \to \mathbb{Z}_4$.

Generalized plateaued functions from other ones in lower dimension

Let $f : V_n \to \mathbb{Z}_{2^k}$
Observe that

$$\zeta_{p^t}^{g(x,0)} = \zeta_{p^t}^{h(x)} \quad \text{and} \quad \zeta_{p^t}^{g(x,1)} = \zeta_4^{I(f_1(x),\ldots,f_{k-1}(x))}\zeta_{p^t}^{h(x)}.$$

where

$$h(x) = 2^{t-1}f_k(x) + \sum_{i=1}^{t} H_i(f_1(x),\ldots,f_{k-1}(x))2^{i-1}$$

Now, if I is equal to 0 or 2 $\zeta_4^{I(f_1(x),\ldots,f_{k-1}(x))} \in \{-1,1\}$ while, if it equal to 1 or 3, $\zeta_4^{I(f_1(x),\ldots,f_{k-1}(x))} \in \{-\zeta_4,\zeta_4\}$.

Generalized plateaued functions from other ones in lower dimension

Let $f : V_n \to \mathbb{Z}_{2^k}$

THEOREM

Suppose that f is a generalized plateaued function with amplitude $p^{\frac{n+r}{2}}$. Then

1. *If I takes only the values 1 and 3, g is a generalized plateaued function with amplitude $p^{\frac{n+r}{2}}$*
2. *If I takes only the values 0 and 2, g is a generalized plateaued function with amplitude $p^{\frac{n+r+1}{2}}$*

REMARK

If I can take three values then g cannot be plateaued.