# Bent and generalized bent functions into the cyclic group $\mathbb{Z}_{2^k}$


Wilfried Meidl

Radon Institute for Computational and Applied Mathematics, OEAW, Linz, Austria


June 18, 2018

# Outline

- Bent functions
  - Definitions
  - Bent funtions into the cyclic group and the spread construction
- Gbent functions
  - Definition and summary of some results
  - Gbent functions and partitions
- Classes of gbent functions and their partitions
  - Spread functions
  - Octal gbent functions
  - Maiorana-McFarland functions

# Bent functions

Definition

Let $A$, $B$ be finite abelian groups, $f$ a function from $A$ to $B$. Then $f$ is called a bent function if

$$|\sum_{x \in A} \chi(x, f(x))| = \sqrt{|A|}$$

for every character $\chi$ of $A \times B$ which is nontrivial on $B$.

$R = \{(x, f(x)) : x \in A\}$ is a $(|A|, |B|, |A|, |A|/|B|)$ relative difference set in $A \times B$, relative to $B$.

# Bent functions

**Definition**

Let $A$, $B$ be finite abelian groups, $f$ a function from $A$ to $B$. Then $f$ is called a bent function if

$$|\sum_{x \in A} \chi(x, f(x))| = \sqrt{|A|}$$

for every character $\chi$ of $A \times B$ which is nontrivial on $B$.

$R = \{(x, f(x)) \, : \, x \in A\}$ is a $(|A|, |B|, |A|, |A|/|B|)$ relative difference set in $A \times B$, relative to $B$.

**Examples:**

Boolean bent function, $p$-ary bent function, $f : \mathbb{F}_p^n \to \mathbb{F}_p$.

$$|\mathcal{W}_f(u)| = |\sum_{x \in \mathbb{F}_p^n} \epsilon_p^{f(x) - u \cdot x}| = p^{n/2},$$

for all $u \in \mathbb{F}_p^n$. ($\epsilon_p = e^{2\pi i/p}$, $\epsilon_2 = -1$)

# Bent functions

Vectorial bent function $f : \mathbb{F}_p^n \to \mathbb{F}_p^m$.

$$|\mathcal{W}_f(a, b)| = |\sum_{x \in \mathbb{F}_p^n} \epsilon_p^{a \cdot f(x) - b \cdot x}| = p^{n/2},$$

for all nonzero $a \in \mathbb{F}_p^m$ and $b \in \mathbb{F}_p^n$. The component functions $\{a \cdot f(x) \ : \ a \neq 0\}$ form a linear space of $p$-ary (Boolean) bent functions of dimension $m$.

# Bent functions

Vectorial bent function $f : \mathbb{F}_p^n \to \mathbb{F}_p^m$.

$$|\mathcal{W}_f(a,b)| = |\sum_{x\in\mathbb{F}_p^n} \epsilon_p^{a\cdot f(x)-b\cdot x}| = p^{n/2},$$

for all nonzero $a \in \mathbb{F}_p^m$ and $b \in \mathbb{F}_p^n$. The component functions $\{a \cdot f(x) \,:\, a \neq 0\}$ form a linear space of $p$-ary (Boolean) bent functions of dimension $m$.

For a vectorial bent function $f : \mathbb{F}_2^n \to \mathbb{F}_2^m$ we have $m \leq n/2$ (Nyberg bound)
(Examples: Maiorana-McFarland vectorial bent functions, Spread vectorial bent functions, Dillons $\mathcal{H}$-class)

# Bent functions

Vectorial bent function $f : \mathbb{F}_p^n \to \mathbb{F}_p^m$.

$$|\mathcal{W}_f(a,b)| = |\sum_{x\in\mathbb{F}_p^n} \epsilon_p^{a\cdot f(x) - b\cdot x}| = p^{n/2},$$

for all nonzero $a \in \mathbb{F}_p^m$ and $b \in \mathbb{F}_p^n$. The component functions $\{a \cdot f(x) \ : \ a \neq 0\}$ form a linear space of $p$-ary (Boolean) bent functions of dimension $m$.

For a vectorial bent function $f : \mathbb{F}_2^n \to \mathbb{F}_2^m$ we have $m \leq n/2$ (Nyberg bound)
(Examples: Maiorana-McFarland vectorial bent functions, Spread vectorial bent functions, Dillons $\mathcal{H}$-class)

If $f : \mathbb{F}_p^n \to \mathbb{F}_p^m$, $p$ odd, then $m \leq n$
(If $m = n$, then $f$ is called planar, e.g Coulter-Matthews)

# Bent functions into the cyclic group

$f : \mathbb{F}_p^n \to \mathbb{Z}_{p^k}$ is bent if

$$\mathcal{H}_f^k(\alpha, u) = \sum_{x \in \mathbb{F}_p^n} \zeta_{p^k}^{\alpha f(x)} \zeta_p^{u \cdot x}, \quad \zeta_M = e^{2\pi i/M},$$

has absolute value $p^{n/2}$ for all $u \in \mathbb{F}_p^n$ and all nonzero $\alpha \in \mathbb{Z}_{p^k}$.

# Bent functions into the cyclic group

$f : \mathbb{F}_p^n \to \mathbb{Z}_{p^k}$ is bent if

$$\mathcal{H}_f^k(\alpha, u) = \sum_{x \in \mathbb{F}_p^n} \zeta_{p^k}^{\alpha f(x)} \zeta_p^{u \cdot x}, \quad \zeta_M = e^{2\pi i/M},$$

has absolute value $p^{n/2}$ for all $u \in \mathbb{F}_p^n$ and all nonzero $\alpha \in \mathbb{Z}_{p^k}$.

$p = 2$, $n$ even:

# Bent functions into the cyclic group

$f : \mathbb{F}_p^n \to \mathbb{Z}_{p^k}$ is bent if

$$\mathcal{H}_f^k(\alpha, u) = \sum_{x \in \mathbb{F}_p^n} \zeta_{p^k}^{\alpha f(x)} \zeta_p^{u \cdot x}, \quad \zeta_M = e^{2\pi i/M},$$

has absolute value $p^{n/2}$ for all $u \in \mathbb{F}_p^n$ and all nonzero $\alpha \in \mathbb{Z}_{p^k}$.

$p = 2$, $n$ even: $f : \mathbb{F}_2^n \to \mathbb{Z}_{2^k}$ is bent if

$$\mathcal{H}_f^k(\alpha, u) = \sum_{x \in \mathbb{F}_2^n} \zeta_{2^k}^{\alpha f(x)} (-1)^{u \cdot x}, \quad \zeta_{2^k} = e^{2\pi i/2^k},$$

has absolute value $2^{n/2}$ for all $u \in \mathbb{F}_2^n$ and all nonzero $\alpha \in \mathbb{Z}_{2^k}$.

Again the "Nyberg bound" applies for $p = 2$:
If $f : \mathbb{F}_2^n \to \mathbb{Z}_{2^k}$ is bent then $k \leq n/2$.

# Bent functions into the cyclic group

$f : \mathbb{F}_p^n \to \mathbb{Z}_{p^k}$ is bent if

$$\mathcal{H}_f^k(\alpha, u) = \sum_{x \in \mathbb{F}_p^n} \zeta_{p^k}^{\alpha f(x)} \zeta_p^{u \cdot x}, \quad \zeta_M = e^{2\pi i/M},$$

has absolute value $p^{n/2}$ for all $u \in \mathbb{F}_p^n$ and all nonzero $\alpha \in \mathbb{Z}_{p^k}$.

$p = 2$, $n$ even: $f : \mathbb{F}_2^n \to \mathbb{Z}_{2^k}$ is bent if

$$\mathcal{H}_f^k(\alpha, u) = \sum_{x \in \mathbb{F}_2^n} \zeta_{2^k}^{\alpha f(x)} (-1)^{u \cdot x}, \quad \zeta_{2^k} = e^{2\pi i/2^k},$$

has absolute value $2^{n/2}$ for all $u \in \mathbb{F}_2^n$ and all nonzero $\alpha \in \mathbb{Z}_{2^k}$.

Again the "Nyberg bound" applies for $p = 2$:
If $f : \mathbb{F}_2^n \to \mathbb{Z}_{2^k}$ is bent then $k \le n/2$.

Bent functions from the elementary abelian into the cyclic group $\mathbb{Z}_{2^k}$ ($\mathbb{Z}_{p^k}$) seem to be "rare".

# Spread Bent Functions

$f : \mathbb{V}_n \to B$, $\mathbb{V}_n \cong \mathbb{F}_p^n$, $n = 2m$ even, $|B| = p^k$, $k \leq n/2$. (e.g. $B = \mathbb{Z}_p^m, \mathbb{Z}_{p^m}$)

Let $U_0, U_1, \ldots, U_{p^m}$ be the elements of a spread of $\mathbb{V}_n$.

# Spread Bent Functions

$f : \mathbb{V}_n \to B$, $\mathbb{V}_n \cong \mathbb{F}_p^n$, $n = 2m$ even, $|B| = p^k$, $k \leq n/2$. (e.g. $B = \mathbb{Z}_p^m, \mathbb{Z}_{p^m}$)

Let $U_0, U_1, \ldots, U_{p^m}$ be the elements of a spread of $\mathbb{V}_n$.

Partition of $\mathbb{V}_n$

# Spread Bent Functions

$f : \mathbb{V}_n \to B$, $\mathbb{V}_n \cong \mathbb{F}_p^n$, $n = 2m$ even, $|B| = p^k$, $k \leq n/2$. (e.g. $B = \mathbb{Z}_p^m, \mathbb{Z}_{p^m}$)

Let $U_0, U_1, \ldots, U_{p^m}$ be the elements of a spread of $\mathbb{V}_n$.

## Partition of $\mathbb{V}_n$

Define a function $f : \mathbb{V}_n \to B$ by

- $f(x) = 0$ for $x \in U_0$.
- $f$ is constant on the nonzero elements of $U_i$, $1 \leq i \leq p^m$, such that:

# Spread Bent Functions

$f : \mathbb{V}_n \to B$, $\mathbb{V}_n \cong \mathbb{F}_p^n$, $n = 2m$ even, $|B| = p^k$, $k \leq n/2$. (e.g. $B = \mathbb{Z}_p^m, \mathbb{Z}_{p^m}$)

Let $U_0, U_1, \ldots, U_{p^m}$ be the elements of a spread of $\mathbb{V}_n$.

Partition of $\mathbb{V}_n$

Define a function $f : \mathbb{V}_n \to B$ by

- $f(x) = 0$ for $x \in U_0$.
- $f$ is constant on the nonzero elements of $U_i$, $1 \leq i \leq p^m$, such that: For every $c \in B$ the nonzero elements of exactly $p^{m-k}$ of the $U_i$'a are mapped to $c$.
  ($k = m = n/2$: For every $c \in B$ the nonzero elements of exactly 1 of the $U_i$'a are mapped to $c$.)

# Spread Bent Functions

$f : \mathbb{V}_n \to B$, $\mathbb{V}_n \cong \mathbb{F}_p^n$, $n = 2m$ even, $|B| = p^k$, $k \le n/2$. (e.g. $B = \mathbb{Z}_p^m, \mathbb{Z}_{p^m}$)

Let $U_0, U_1, \ldots, U_{p^m}$ be the elements of a spread of $\mathbb{V}_n$.

Partition of $\mathbb{V}_n$

Define a function $f : \mathbb{V}_n \to B$ by

- $f(x) = 0$ for $x \in U_0$.
- $f$ is constant on the nonzero elements of $U_i$, $1 \le i \le p^m$, such that: For every $c \in B$ the nonzero elements of exactly $p^{m-k}$ of the $U_i$'a are mapped to $c$.
  ($k = m = n/2$: For every $c \in B$ the nonzero elements of exactly 1 of the $U_i$'a are mapped to $c$.)

$f$ is then a bent function from $\mathbb{V}_n$ to $B$.

# Relaxing the conditions

**Definition**

K.U. Schmidt (2009) A function $f : \mathbb{F}_2^n \to \mathbb{Z}_{2^k}$ is called a generalized bent function (gbent function) if

$$\mathcal{H}_f^k(u) = \sum_{x \in \mathbb{F}_2^n} \zeta_{2^k}^{f(x)} (-1)^{u \cdot x},$$

has absolute value $2^{n/2}$ for all $u \in \mathbb{F}_2^n$.

# Relaxing the conditions

Definition

K.U. Schmidt (2009) A function $f : \mathbb{F}_2^n \to \mathbb{Z}_{2^k}$ is called a generalized bent function (gbent function) if

$$\mathcal{H}_f^k(u) = \sum_{x \in \mathbb{F}_2^n} \zeta_{2^k}^{f(x)} (-1)^{u \cdot x},$$

has absolute value $2^{n/2}$ for all $u \in \mathbb{F}_2^n$.

Note: $|\sum_{x \in \mathbb{F}_2^n} \chi(x, f(x))| = 2^{n/2}$ is required only for the characters of order $2^{k-1}$. In general NOT a relative difference set (not bent).

# Relaxing the conditions

Definition
K.U. Schmidt (2009) A function $f : \mathbb{F}_2^n \to \mathbb{Z}_{2^k}$ is called a generalized bent function (gbent function) if

$$\mathcal{H}_f^k(u) = \sum_{x \in \mathbb{F}_2^n} \zeta_{2^k}^{f(x)} (-1)^{u \cdot x},$$

has absolute value $2^{n/2}$ for all $u \in \mathbb{F}_2^n$.

Note: $|\sum_{x \in \mathbb{F}_2^n} \chi(x, f(x))| = 2^{n/2}$ is required only for the characters of order $2^{k-1}$. In general NOT a relative difference set (not bent).

Observation The function $f : \mathbb{F}_2^n \to \mathbb{Z}_{2^k}$ is bent if and only if $2^t f(x)$ is gbent (into $\mathbb{Z}_{2^{k-t}}$) for all $t$, $0 \leq t \leq k-1$.

# Relaxing the conditions

Definition
K.U. Schmidt (2009) A function $f : \mathbb{F}_2^n \to \mathbb{Z}_{2^k}$ is called a generalized bent function (gbent function) if

$$\mathcal{H}_f^k(u) = \sum_{x \in \mathbb{F}_2^n} \zeta_{2^k}^{f(x)} (-1)^{u \cdot x},$$

has absolute value $2^{n/2}$ for all $u \in \mathbb{F}_2^n$.

Note: $|\sum_{x \in \mathbb{F}_2^n} \chi(x, f(x))| = 2^{n/2}$ is required only for the characters of order $2^{k-1}$. In general NOT a relative difference set (not bent).

Observation The function $f : \mathbb{F}_2^n \to \mathbb{Z}_{2^k}$ is bent if and only if $2^t f(x)$ is gbent (into $\mathbb{Z}_{2^{k-t}}$) for all $t$, $0 \leq t \leq k-1$.

Question: Is "gbent" still something interesting?

# Results on Generalized Bent Functions

$n$ even, $(p = 2)$. $f : \mathbb{F}_2^n \to \mathbb{Z}_{2^k}$,

$$f(x) = a_0(x) + 2a_1(x) + \cdots + 2^{k-1}a_{k-1}(x), \; a_i : \mathbb{F}_2^n \to \mathbb{F}_2. \quad (1)$$

# Results on Generalized Bent Functions

$n$ even, $(p = 2)$. $f : \mathbb{F}_2^n \to \mathbb{Z}_{2^k}$,

$$f(x) = a_0(x) + 2a_1(x) + \cdots + 2^{k-1}a_{k-1}(x),\ a_i : \mathbb{F}_2^n \to \mathbb{F}_2. \quad (1)$$

Sole, Tokareva 2009 $f(x) = a_0(x) + 2a_1(x)$ is generalized bent if and only if $a_1$ and $a_1 \oplus a_0$ are Boolean bent functions.

# Results on Generalized Bent Functions

$n$ even, $(p = 2)$. $f : \mathbb{F}_2^n \to \mathbb{Z}_{2^k}$,

$$f(x) = a_0(x) + 2a_1(x) + \cdots + 2^{k-1}a_{k-1}(x),\ a_i : \mathbb{F}_2^n \to \mathbb{F}_2. \quad (1)$$

Sole, Tokareva 2009 $f(x) = a_0(x) + 2a_1(x)$ is generalized bent if and only if $a_1$ and $a_1 \oplus a_0$ are Boolean bent functions.

Various Authors, 2015– If $f$ in (1) is generalized bent, then all functions in $\mathcal{A} = a_{k-1} \oplus \langle a_0, \ldots, a_{k-2} \rangle$ are Boolean bent functions.

# Results on Generalized Bent Functions

$n$ even, $(p = 2)$. $f : \mathbb{F}_2^n \to \mathbb{Z}_{2^k}$,

$$f(x) = a_0(x) + 2a_1(x) + \cdots + 2^{k-1}a_{k-1}(x),\ a_i : \mathbb{F}_2^n \to \mathbb{F}_2. \quad (1)$$

Sole, Tokareva 2009 $f(x) = a_0(x) + 2a_1(x)$ is generalized bent if and only if $a_1$ and $a_1 \oplus a_0$ are Boolean bent functions.

Various Authors, 2015– If $f$ in (1) is generalized bent, then all functions in $\mathcal{A} = a_{k-1} \oplus \langle a_0, \ldots, a_{k-2} \rangle$ are Boolean bent functions.

Tang, Xiang, Qi, Feng 2017 $f$ is generalized bent if and only if all functions in $\mathcal{A}$ are bent and the Walsh transforms of all those relate as follows: (technical conditions),

# Results on Generalized Bent Functions

$n$ even, $(p = 2)$. $f : \mathbb{F}_2^n \to \mathbb{Z}_{2^k}$,

$$f(x) = a_0(x) + 2a_1(x) + \cdots + 2^{k-1}a_{k-1}(x),\ a_i : \mathbb{F}_2^n \to \mathbb{F}_2. \quad (1)$$

Sole, Tokareva 2009 $f(x) = a_0(x) + 2a_1(x)$ is generalized bent if and only if $a_1$ and $a_1 \oplus a_0$ are Boolean bent functions.

Various Authors, 2015– If $f$ in (1) is generalized bent, then all functions in $\mathcal{A} = a_{k-1} \oplus \langle a_0, \ldots, a_{k-2} \rangle$ are Boolean bent functions.

Tang, Xiang, Qi, Feng 2017 $f$ is generalized bent if and only if all functions in $\mathcal{A}$ are bent and the Walsh transforms of all those relate as follows: (technical conditions), or

Hodzic, M.,Pasalic 2018 $f$ is generalized bent if and only if all functions in $\mathcal{A}$ are bent such that for any $h_0, h_1, h_2 \in \mathcal{A}$ and $h_3 = h_0 \oplus h_1 \oplus h_2$ we have $h_3^* = h_0^* \oplus h_1^* \oplus h_2^*$.

# Results on Generalized Bent Functions

$n$ even, $(p = 2)$. $f : \mathbb{F}_2^n \to \mathbb{Z}_{2^k}$,

$$f(x) = a_0(x) + 2a_1(x) + \cdots + 2^{k-1}a_{k-1}(x), \; a_i : \mathbb{F}_2^n \to \mathbb{F}_2. \quad (1)$$

Sole, Tokareva 2009 $f(x) = a_0(x) + 2a_1(x)$ is generalized bent if and only if $a_1$ and $a_1 \oplus a_0$ are Boolean bent functions.

Various Authors, 2015– If $f$ in (1) is generalized bent, then all functions in $\mathcal{A} = a_{k-1} \oplus \langle a_0, \ldots, a_{k-2} \rangle$ are Boolean bent functions.

Tang, Xiang, Qi, Feng 2017 $f$ is generalized bent if and only if all functions in $\mathcal{A}$ are bent and the Walsh transforms of all those relate as follows: (technical conditions), or

Hodzic, M.,Pasalic 2018 $f$ is generalized bent if and only if all functions in $\mathcal{A}$ are bent such that for any $h_0, h_1, h_2 \in \mathcal{A}$ and $h_3 = h_0 \oplus h_1 \oplus h_2$ we have $h_3^* = h_0^* \oplus h_1^* \oplus h_2^*$.

(Recall, $g : \mathbb{F}_2^n \to \mathbb{F}_2$ bent $\Rightarrow \mathcal{W}_f(b) = 2^{n/2}(-1)^{g^*(b)}$. The "dual" $g^*$ is also bent.)

# Gbent functions and partitions

Mesnager et *al.* 2018 A gbent function is

- a Boolean ($p$-ary) bent function $a(x)$ from $\mathbb{F}_2^n$ ($\mathbb{F}_p^n$) to $\mathbb{F}_2$ ($\mathbb{F}_p$) together with
- a partition $\mathcal{P} = \{A(0), A(1), \ldots, A(r-1)\}$ of $\mathbb{F}_2^n$ ($\mathbb{F}_p^n$)

with the property that $a(x) \oplus C(x)$ is bent for every $C : \mathbb{F}_2^n \to \mathbb{F}_2$ ($C : \mathbb{F}_p^n \to \mathbb{F}_p$) which is constant on the elements of $\mathcal{P}$.

# Gbent functions and partitions

Mesnager et *al.* 2018 A gbent function is

- a Boolean ($p$-ary) bent function $a(x)$ from $\mathbb{F}_2^n$ ($\mathbb{F}_p^n$) to $\mathbb{F}_2$ ($\mathbb{F}_p$) together with
- a partition $\mathcal{P} = \{A(0), A(1), \dots, A(r-1)\}$ of $\mathbb{F}_2^n$ ($\mathbb{F}_p^n$)

with the property that $a(x) \oplus C(x)$ is bent for every $C : \mathbb{F}_2^n \to \mathbb{F}_2$ ($C : \mathbb{F}_p^n \to \mathbb{F}_p$) which is constant on the elements of $\mathcal{P}$.

The partition $\mathcal{P}$?

# Gbent functions and partitions

Mesnager et *al.* 2018 A gbent function is

- a Boolean ($p$-ary) bent function $a(x)$ from $\mathbb{F}_2^n$ ($\mathbb{F}_p^n$) to $\mathbb{F}_2$ ($\mathbb{F}_p$) together with
- a partition $\mathcal{P} = \{A(0), A(1), \ldots, A(r-1)\}$ of $\mathbb{F}_2^n$ ($\mathbb{F}_p^n$)

with the property that $a(x) \oplus C(x)$ is bent for every $C : \mathbb{F}_2^n \to \mathbb{F}_2$ ($C : \mathbb{F}_p^n \to \mathbb{F}_p$) which is constant on the elements of $\mathcal{P}$.

The partition $\mathcal{P}$? Let

$$f(x) = a_0(x) + 2a_1(x) + \cdots + 2^{k-2}a_{k-2}(x) + 2^{k-1}a_{k-1}(x)$$

be "a representation" of the gbent function, then

$$\mathcal{P} = \{A(j), 0 \leq j \leq 2^{k-1} - 1\},$$
$$A(j) = \{x \in \mathbb{F}_2^n \ : \ f(x) - 2^{k-1}a_{k-1}(x) = j\}.$$

Note: $|\mathcal{P}| \leq 2^{k-1}$.

# Blowing up and playing with the partition

Mesnager et *al.* 2018 If $\mathbb{F}_2^n \to \mathbb{Z}_{2^k}$ is gbent, with

$$f(x) = a_0(x) + 2a_1(x) + \cdots + 2^{k-2}a_{k-2}(x) + 2^{k-1}a_{k-1}(x),$$

so is $\bar{f} : \mathbb{F}_2^n \to \mathbb{Z}_{2^l}$

$$\bar{f}(x) = F_0(a_0(x), \ldots, a_{k-2}(x)) + 2F_1(a_0(x), \ldots, a_{k-2}(x)) + \ldots \\ + 2^{l-2}F_{l-2}(a_0(x), \ldots, a_{k-2}(x)) + 2^{l-1}a_{k-1}(x)$$

for every integer $l$ and every $F_j : \mathbb{F}_2^{k-1} \to \mathbb{F}_2$, $0 \leq j \leq l-2$.

# Blowing up and playing with the partition

Mesnager et *al.* 2018 If $\mathbb{F}_2^n \to \mathbb{Z}_{2^k}$ is gbent, with

$$f(x) = a_0(x) + 2a_1(x) + \cdots + 2^{k-2}a_{k-2}(x) + 2^{k-1}a_{k-1}(x),$$

so is $\bar{f} : \mathbb{F}_2^n \to \mathbb{Z}_{2^l}$

$$\bar{f}(x) = F_0(a_0(x), \ldots, a_{k-2}(x)) + 2F_1(a_0(x), \ldots, a_{k-2}(x)) + \ldots$$
$$+ 2^{l-2}F_{l-2}(a_0(x), \ldots, a_{k-2}(x)) + 2^{l-1}a_{k-1}(x)$$

for every integer $l$ and every $F_j : \mathbb{F}_2^{k-1} \to \mathbb{F}_2$, $0 \leq j \leq l-2$.

Simplest example: If $f : \mathbb{F}_2^n \to \mathbb{F}_2$ is bent, then $\bar{f} : \mathbb{F}_2^n \to \mathbb{Z}_{2^l}$, with $\bar{f} = 2^{l-1}f(x)$ is gbent taking on only the values 0 and $2^{l-1}$.

# Gbent function and its dimension

Questions: What is

- the finest partition for a given bent function $a : \mathbb{F}_2^n \to \mathbb{F}_2$?
- the finest partition a bent function $a : \mathbb{F}_2^n \to \mathbb{F}_2$ can have?

# Gbent function and its dimension

Questions: What is

- the finest partition for a given bent function $a : \mathbb{F}_2^n \to \mathbb{F}_2$?
- the finest partition a bent function $a : \mathbb{F}_2^n \to \mathbb{F}_2$ can have?

Let $f : \mathbb{F}_2^n \to \mathbb{Z}_{2^l}$ be gbent, represented as $f(x) = a_0(x) + 2a_1(x) + \cdots + 2^{l-2}a_{l-2}(x) + 2^{l-1}a_{l-1}(x)$ with its partition $\mathcal{P} = \{A(j), 0 \leq j \leq 2^{l-1} - 1 \, : \, f(x) - 2^{l-1}a_{l-1}(x) = j\}$.

# Gbent function and its dimension

Questions: What is

- the finest partition for a given bent function $a : \mathbb{F}_2^n \to \mathbb{F}_2$?
- the finest partition a bent function $a : \mathbb{F}_2^n \to \mathbb{F}_2$ can have?

Let $f : \mathbb{F}_2^n \to \mathbb{Z}_{2^l}$ be gbent, represented as $f(x) = a_0(x) + 2a_1(x) + \cdots + 2^{l-2}a_{l-2}(x) + 2^{l-1}a_{l-1}(x)$ with its partition $\mathcal{P} = \{A(j), 0 \le j \le 2^{l-1} - 1 \,:\, f(x) - 2^{l-1}a_{l-1}(x) = j\}$.

- The dimension of $f$ is $k$ if the partition $\mathcal{P}$ contains $2^{k-2} + 1 \le \Omega \le 2^{k-1}$ (nonempty) sets.

# Gbent function and its dimension

Questions: What is

- the finest partition for a given bent function $a : \mathbb{F}_2^n \to \mathbb{F}_2$?
- the finest partition a bent function $a : \mathbb{F}_2^n \to \mathbb{F}_2$ can have?

Let $f : \mathbb{F}_2^n \to \mathbb{Z}_{2^l}$ be gbent, represented as $f(x) = a_0(x) + 2a_1(x) + \cdots + 2^{l-2}a_{l-2}(x) + 2^{l-1}a_{l-1}(x)$ with its partition $\mathcal{P} = \{A(j), 0 \leq j \leq 2^{l-1} - 1 \, : \, f(x) - 2^{l-1}a_{l-1}(x) = j\}$.

- The dimension of $f$ is $k$ if the partition $\mathcal{P}$ contains $2^{k-2} + 1 \leq \Omega \leq 2^{k-1}$ (nonempty) sets.
- The dimension of $f$ is the smallest number $k$ for which there exists a gbent function $\tilde{f} : \mathbb{F}_2^n \to \mathbb{Z}_{2^k}$, $\tilde{f}(x) = \tilde{a}_0(x) + 2\tilde{a}_1(x) + \cdots + 2^{k-2}\tilde{a}_{k-2}(x) + 2^{k-1}a_{l-1}(x)$ which induces the same partition of $\mathbb{F}_2^n$.

# Gbent function and its dimension

Questions: What is

- the finest partition for a given bent function $a : \mathbb{F}_2^n \to \mathbb{F}_2$?
- the finest partition a bent function $a : \mathbb{F}_2^n \to \mathbb{F}_2$ can have?

Let $f : \mathbb{F}_2^n \to \mathbb{Z}_{2^l}$ be gbent, represented as $f(x) = a_0(x) + 2a_1(x) + \cdots + 2^{l-2}a_{l-2}(x) + 2^{l-1}a_{l-1}(x)$ with its partition $\mathcal{P} = \{A(j), 0 \le j \le 2^{l-1} - 1 \, : \, f(x) - 2^{l-1}a_{l-1}(x) = j\}$.

- The dimension of $f$ is $k$ if the partition $\mathcal{P}$ contains $2^{k-2} + 1 \le \Omega \le 2^{k-1}$ (nonempty) sets.
- The dimension of $f$ is the smallest number $k$ for which there exists a gbent function $\tilde{f} : \mathbb{F}_2^n \to \mathbb{Z}_{2^k}$, $\tilde{f}(x) = \tilde{a}_0(x) + 2\tilde{a}_1(x) + \cdots + 2^{k-2}\tilde{a}_{k-2}(x) + 2^{k-1}a_{l-1}(x)$ which induces the same partition of $\mathbb{F}_2^n$.
- The dimension of $f$ is the smallest number $k$ for which there exists a gbent function $\tilde{f} : \mathbb{F}_2^n \to \mathbb{Z}_{2^k}$ from which $f$ can be obtained by "blowing up and playing with the partition".

# Spread Functions

Let $U_0, U_1, \ldots, U_{2^m}$ be the elements of a spread of $\mathbb{F}_2^n$, $n = 2m$.

Then $f : \mathbb{V}_n \to \mathbb{Z}_{2^m}$ defined by

- $f(x) = 0$ for $x \in U_0$ (w.l.o.g.),
- $f$ is constant on the nonzero elements of $U_i$, $1 \leq i \leq p^m$, such that for every $c \in \mathbb{Z}_{2^m}$ the nonzero elements of exactly 1 of the $U_i$'a are mapped to $c$, is bent.

# Spread Functions

Let $U_0, U_1, \ldots, U_{2^m}$ be the elements of a spread of $\mathbb{F}_2^n$, $n = 2m$.

Then $f : \mathbb{V}_n \to \mathbb{Z}_{2^m}$ defined by

- $f(x) = 0$ for $x \in U_0$ (w.l.o.g.),
- $f$ is constant on the nonzero elements of $U_i$, $1 \leq i \leq p^m$, such that for every $c \in \mathbb{Z}_{2^m}$ the nonzero elements of exactly 1 of the $U_i$'a are mapped to $c$, is bent.

Relaxing the condition for gbent
(M., Martinsen, Stanica, 2017)

$f : \mathbb{V}_n \to \mathbb{Z}_{2^k}$:

- $f(x) = 0$ for $x \in U_0$.
- $f$ is constant on the nonzero elements of $U_i$, $1 \leq i \leq 2^m$, such that:

# Spread Functions

Let $U_0, U_1, \ldots, U_{2^m}$ be the elements of a spread of $\mathbb{F}_2^n$, $n = 2m$.

Then $f : \mathbb{V}_n \to \mathbb{Z}_{2^m}$ defined by

- $f(x) = 0$ for $x \in U_0$ (w.l.o.g.),
- $f$ is constant on the nonzero elements of $U_i$, $1 \leq i \leq p^m$, such that for every $c \in \mathbb{Z}_{2^m}$ the nonzero elements of exactly 1 of the $U_i$'a are mapped to $c$, is bent.

Relaxing the condition for gbent
(M., Martinsen, Stanica, 2017)

$f : \mathbb{V}_n \to \mathbb{Z}_{2^k}$:

- $f(x) = 0$ for $x \in U_0$.
- $f$ is constant on the nonzero elements of $U_i$, $1 \leq i \leq 2^m$, such that: The number of $U_i$ mapped to $c$ and to $c + 2^{k-1}$ is the same for every $0 \leq c \leq 2^{k-2} - 1$.

# Spread Functions

Let $f$ be such a gbent (bent) function from a spread of $\mathbb{F}_2^n$, and $\mathcal{P}$ its partition.

- $|\mathcal{P}| \leq 2^{m-1}$, (hence $f = a_0 + 2a_1 + \cdots + 2^{m-1}a_{m-1}$, $\mathcal{P} = \{A(d) : 0 \leq d \leq 2^{m-1} - 1\}$)
- $|\mathcal{P}| = 2^{m-1}$ if and only if $f : \mathbb{F}_2^n \to \mathbb{Z}_{2^m}$ is bent.

# Spread Functions

Let $f$ be such a gbent (bent) function from a spread of $\mathbb{F}_2^n$, and $\mathcal{P}$ its partition.

- $|\mathcal{P}| \le 2^{m-1}$, (hence $f = a_0 + 2a_1 + \cdots + 2^{m-1}a_{m-1}$, $\mathcal{P} = \{A(d) \,:\, 0 \le d \le 2^{m-1} - 1\}$)
- $|\mathcal{P}| = 2^{m-1}$ if and only if $f : \mathbb{F}_2^n \to \mathbb{Z}_{2^m}$ is bent.
- For $f$ bent, $A(d)$ is the union of 2 spread elements, $1 \le d \le 2^{m-1} - 1$, $A(0)$ (w.l.o.g) contains 3.

# Spread Functions

Let $f$ be such a gbent (bent) function from a spread of $\mathbb{F}_2^n$, and $\mathcal{P}$ its partition.

- $|\mathcal{P}| \leq 2^{m-1}$, (hence $f = a_0 + 2a_1 + \cdots + 2^{m-1}a_{m-1}$, $\mathcal{P} = \{A(d) \,:\, 0 \leq d \leq 2^{m-1} - 1\}$)
- $|\mathcal{P}| = 2^{m-1}$ if and only if $f : \mathbb{F}_2^n \to \mathbb{Z}_{2^m}$ is bent.
- For $f$ bent, $A(d)$ is the union of 2 spread elements, $1 \leq d \leq 2^{m-1} - 1$, $A(0)$ (w.l.o.g) contains 3. For only gbent, all $A(d)$ but one ($A(0)$) contain an even number of spread elements.

# Spread Functions

Let $f$ be such a gbent (bent) function from a spread of $\mathbb{F}_2^n$, and $\mathcal{P}$ its partition.

- $|\mathcal{P}| \leq 2^{m-1}$, (hence $f = a_0 + 2a_1 + \cdots + 2^{m-1}a_{m-1}$, $\mathcal{P} = \{A(d) \,:\, 0 \leq d \leq 2^{m-1} - 1\}$)
- $|\mathcal{P}| = 2^{m-1}$ if and only if $f : \mathbb{F}_2^n \to \mathbb{Z}_{2^m}$ is bent.
- For $f$ bent, $A(d)$ is the union of 2 spread elements, $1 \leq d \leq 2^{m-1} - 1$, $A(0)$ (w.l.o.g) contains 3. For only gbent, all $A(d)$ but one ($A(0)$) contain an even number of spread elements.
- All functions $a_{m-1}(x) + C(x)$ are partial spread bent functions.

# Spread Functions

Let $f$ be such a gbent (bent) function from a spread of $\mathbb{F}_2^n$, and $\mathcal{P}$ its partition.

- $|\mathcal{P}| \leq 2^{m-1}$, (hence $f = a_0 + 2a_1 + \cdots + 2^{m-1}a_{m-1}$, $\mathcal{P} = \{A(d) \,:\, 0 \leq d \leq 2^{m-1} - 1\}$)
- $|\mathcal{P}| = 2^{m-1}$ if and only if $f : \mathbb{F}_2^n \to \mathbb{Z}_{2^m}$ is bent.
- For $f$ bent, $A(d)$ is the union of 2 spread elements, $1 \leq d \leq 2^{m-1} - 1$, $A(0)$ (w.l.o.g) contains 3. For only gbent, all $A(d)$ but one ($A(0)$) contain an even number of spread elements.
- All functions $a_{m-1}(x) + C(x)$ are partial spread bent functions.
- A spread bent function has many such partitions corresponding to *different* gbent functions. (Spread is more!)

# Spread Functions

Let $f$ be such a gbent (bent) function from a spread of $\mathbb{F}_2^n$, and $\mathcal{P}$ its partition.

- $|\mathcal{P}| \leq 2^{m-1}$, (hence $f = a_0 + 2a_1 + \cdots + 2^{m-1}a_{m-1}$, $\mathcal{P} = \{A(d) : 0 \leq d \leq 2^{m-1} - 1\}$)
- $|\mathcal{P}| = 2^{m-1}$ if and only if $f : \mathbb{F}_2^n \to \mathbb{Z}_{2^m}$ is bent.
- For $f$ bent, $A(d)$ is the union of 2 spread elements, $1 \leq d \leq 2^{m-1} - 1$, $A(0)$ (w.l.o.g) contains 3. For only gbent, all $A(d)$ but one ($A(0)$) contain an even number of spread elements.
- All functions $a_{m-1}(x) + C(x)$ are partial spread bent functions.
- A spread bent function has many such partitions corresponding to *different* gbent functions. (Spread is more!)
- Construct $f : \mathbb{F}_2^n \to \mathbb{Z}_{2^m}$ for which $|\mathcal{H}_f^m(\alpha, u)| = 2^{n/2}$ exactly for any fixed set of $\alpha' s \in \mathbb{Z}_{2^m}$. (BFA Talk 2017, Note that $|\mathcal{H}_f^k(2^t r, u)| = |\mathcal{H}_f^k(2^t, u)|$ for all odd $r$)

# Small $k$

$k = 1$ Bent function $f : \mathbb{F}_2^n \to \mathbb{F}_2$, $\mathcal{P} = \mathbb{F}_2^n$.

# Small $k$

$k = 1$ Bent function $f : \mathbb{F}_2^n \to \mathbb{F}_2$, $\mathcal{P} = \mathbb{F}_2^n$.

$k = 2$ With Sole, Tokareva, $g_0, g_1 : \mathbb{F}_2^n \to \mathbb{F}_2$ bent, if and only if $f : \mathbb{F}_2^n \to \mathbb{Z}_4$, $f = (g_0 \oplus g_1) + 2g_0$ is gbent.

Partition:
$A(0) = \{x \,:\, g_0(x) = g_1(x)\}$, $A(1) = \{x \,:\, g_0(x) \neq g_1(x)\}$.

Obtained Boolean bent functions: $g_0, g_0 \oplus 1, g_1, g_1 \oplus 1$

# Small $k$

$k = 1$ Bent function $f : \mathbb{F}_2^n \to \mathbb{F}_2$, $\mathcal{P} = \mathbb{F}_2^n$.

$k = 2$ With Sole, Tokareva, $g_0, g_1 : \mathbb{F}_2^n \to \mathbb{F}_2$ bent, if and only if $f : \mathbb{F}_2^n \to \mathbb{Z}_4$, $f = (g_0 \oplus g_1) + 2g_0$ is gbent.

Partition:
$A(0) = \{x \,:\, g_0(x) = g_1(x)\}$, $A(1) = \{x \,:\, g_0(x) \neq g_1(x)\}$.

Obtained Boolean bent functions: $g_0, g_0 \oplus 1, g_1, g_1 \oplus 1$

Bent function $f : \mathbb{F}_2^n \to \mathbb{Z}_4$, $f(x) = h_0(x) + 2h_1(x)$ is bent if and only if $h_1, h_0, h_1 \oplus h_0$ are Boolean bent functions.

Relative difference set in $\mathbb{F}_2^n \times \mathbb{F}_2^2 \longleftrightarrow$ Relative difference set in $\mathbb{F}_2^n \times \mathbb{Z}_4$.

# $k = 3$ Carlet's construction, 2006, LNCS 3857

# $k = 3$ Carlet's construction, 2006, LNCS 3857

Let $h_0, h_1, h_2$ be Boolean bent functions such that $h_3 = h_0 \oplus h_1 \oplus h_2$ is bent. Then $h_0 h_1 \oplus h_0 h_2 \oplus h_1 h_2$ is bent if and only if $h_3^* = h_0^* \oplus h_1^* \oplus h_2^*$ (Mesnager 2014)

# $k = 3$ Carlet's construction, 2006, LNCS 3857

Let $h_0, h_1, h_2$ be Boolean bent functions such that $h_3 = h_0 \oplus h_1 \oplus h_2$ is bent. Then $h_0 h_1 \oplus h_0 h_2 \oplus h_1 h_2$ is bent if and only if $h_3^* = h_0^* \oplus h_1^* \oplus h_2^*$ (Mesnager 2014)

M. 2018 For Boolean functions $h_0, h_1, h_2$ the function $f : \mathbb{F}_2^n \to \mathbb{Z}_8$

$$f = (h_0 \oplus h_1) + 2(h_0 \oplus h_2) + 4h_0$$

is gbent if and only if $h_0, h_1, h_2$ and $h_3 = h_0 \oplus h_1 \oplus h_2$ are bent such that $h_3^* = h_0^* \oplus h_1^* \oplus h_2^*$.

# $k = 3$ Carlet's construction, 2006, LNCS 3857

Let $h_0, h_1, h_2$ be Boolean bent functions such that $h_3 = h_0 \oplus h_1 \oplus h_2$ is bent. Then $h_0 h_1 \oplus h_0 h_2 \oplus h_1 h_2$ is bent if and only if $h_3^* = h_0^* \oplus h_1^* \oplus h_2^*$ (Mesnager 2014)

M. 2018 For Boolean functions $h_0, h_1, h_2$ the function $f : \mathbb{F}_2^n \to \mathbb{Z}_8$

$$f = (h_0 \oplus h_1) + 2(h_0 \oplus h_2) + 4h_0$$

is gbent if and only if $h_0, h_1, h_2$ and $h_3 = h_0 \oplus h_1 \oplus h_2$ are bent such that $h_3^* = h_0^* \oplus h_1^* \oplus h_2^*$.

What are the bent functions $h_0(x) \oplus C(x)$?

# $k = 3$ Carlet's construction, 2006, LNCS 3857

Let $h_0, h_1, h_2$ be Boolean bent functions such that $h_3 = h_0 \oplus h_1 \oplus h_2$ is bent. Then $h_0 h_1 \oplus h_0 h_2 \oplus h_1 h_2$ is bent if and only if $h_3^* = h_0^* \oplus h_1^* \oplus h_2^*$ (Mesnager 2014)

M. 2018 For Boolean functions $h_0, h_1, h_2$ the function $f : \mathbb{F}_2^n \to \mathbb{Z}_8$

$$f = (h_0 \oplus h_1) + 2(h_0 \oplus h_2) + 4h_0$$

is gbent if and only if $h_0, h_1, h_2$ and $h_3 = h_0 \oplus h_1 \oplus h_2$ are bent such that $h_3^* = h_0^* \oplus h_1^* \oplus h_2^*$.

What are the bent functions $h_0(x) \oplus C(x)$?

$\{h_0, h_1, h_2, h_3, h_0 h_1 \oplus h_0 h_2 \oplus h_1 h_2, h_0 h_1 \oplus h_0 h_3 \oplus h_1 h_3, h_0 h_2 \oplus h_0 h_3 \oplus h_2 h_3, h_1 h_2 \oplus h_1 h_3 \oplus h_2 h_3\} \oplus \{0, 1\}$

# $k = 3$ Carlet's construction, 2006, LNCS 3857

Let $h_0, h_1, h_2$ be Boolean bent functions such that $h_3 = h_0 \oplus h_1 \oplus h_2$ is bent. Then $h_0 h_1 \oplus h_0 h_2 \oplus h_1 h_2$ is bent if and only if $h_3^* = h_0^* \oplus h_1^* \oplus h_2^*$ (Mesnager 2014)

M. 2018 For Boolean functions $h_0, h_1, h_2$ the function $f : \mathbb{F}_2^n \to \mathbb{Z}_8$

$$f = (h_0 \oplus h_1) + 2(h_0 \oplus h_2) + 4h_0$$

is gbent if and only if $h_0, h_1, h_2$ and $h_3 = h_0 \oplus h_1 \oplus h_2$ are bent such that $h_3^* = h_0^* \oplus h_1^* \oplus h_2^*$.

What are the bent functions $h_0(x) \oplus C(x)$?

$\{h_0, h_1, h_2, h_3, h_0 h_1 \oplus h_0 h_2 \oplus h_1 h_2, h_0 h_1 \oplus h_0 h_3 \oplus h_1 h_3, h_0 h_2 \oplus h_0 h_3 \oplus h_2 h_3, h_1 h_2 \oplus h_1 h_3 \oplus h_2 h_3\} \oplus \{0, 1\}$

Recall Hodzic, M.,Pasalic 2018: $f$ is gbent if and only if all functions in $\mathcal{A} = a_{k-1} + \langle a_0, \ldots, a_{k-2} \rangle$ are bent such that for $h_0, h_1, h_2 \in \mathcal{A}$ and $h_0 \oplus h_1 \oplus h_2 = h_3$ we have $h_0^* \oplus h_1^* \oplus h_2^* = h_3^*$.

# Constructions for $k = 3$

## Mesnager 2014

I For $g$ bent, put

$$h_0(x) = g(x), h_1(x) = g(x) \oplus u \cdot x, h_2(x) = g(x) \oplus v \cdot x$$

such that $D_u D_v g^*(x) = 0$;

II For $g_0, g_1$ bent, put

$$h_0(x) = g_0(x), h_1(x) = g_0(x) \oplus u \cdot x, h_2(x) = g_1(x)$$

such that $D_u g_0^*(x) \oplus D_u g_1^*(x) = 0$.

# Constructions for $k = 3$

## Mesnager 2014

I For $g$ bent, put

$$h_0(x) = g(x), h_1(x) = g(x) \oplus u \cdot x, h_2(x) = g(x) \oplus v \cdot x$$

such that $D_u D_v g^*(x) = 0$;

II For $g_0, g_1$ bent, put

$$h_0(x) = g_0(x), h_1(x) = g_0(x) \oplus u \cdot x, h_2(x) = g_1(x)$$

such that $D_u g_0^*(x) \oplus D_u g_1^*(x) = 0$.

Remark

Among Mesnager's concrete examples, one (from II) provides bent functions from $\mathbb{F}_{2^n}$ to $\mathbb{Z}_8$. One from $\mathbb{F}_2^{12}$ to $\mathbb{Z}_8$ does not come from a spread of $\mathbb{F}_2^{12}$, hence gives a relative difference set in $\mathbb{F}_2^{12} \times \mathbb{Z}_8$ which does not come from a spread of $\mathbb{F}_2^{12}$.

(The only one I know for $k \geq 3$)

# Maiorana-McFarland Functions

Carlet's secondary construction, 1994 If $g$ is a bent function which is affine on an $n/2$-dimensional affine subspace, then we can change the values of $g$ on this subspace and again get a bent function.

# Maiorana-McFarland Functions

Carlet's secondary construction, 1994 If $g$ is a bent function which is affine on an $n/2$-dimensional affine subspace, then we can change the values of $g$ on this subspace and again get a bent function.

Kolomeec 2012; DCC, 2017 Two bent functions in dimension $n$ differ at least at $2^{n/2}$ positions. Two bent functions with minimal distance $2^{n/2}$ always differ on an affine subspace (of dimension $n/2$), restricted to which they are affine functions.

Potapov, 2016 The analog result holds for bent functions $g : \mathbb{F}_p^n \to \mathbb{F}_p$, $p$ odd, $n$ even.

# Maiorana-McFarland Functions

Carlet's secondary construction, 1994 If $g$ is a bent function which is affine on an $n/2$-dimensional affine subspace, then we can change the values of $g$ on this subspace and again get a bent function.

Kolomeec 2012; DCC, 2017 Two bent functions in dimension $n$ differ at least at $2^{n/2}$ positions. Two bent functions with minimal distance $2^{n/2}$ always differ on an affine subspace (of dimension $n/2$), restricted to which they are affine functions.

Potapov, 2016 The analog result holds for bent functions $g : \mathbb{F}_p^n \to \mathbb{F}_p$, $p$ odd, $n$ even.

Observation If $a_0 + 2a_1 + \ldots + 2^{k-1}a_{k-1}$ is gbent with partition $\mathcal{P}$ and $A(d) \in \mathcal{P}$. Then $a_{k-1}$ and $a_{k-1} \oplus \mathcal{I}(A(d))$ are bent ($\mathcal{I}$ Indicator function).

# Maiorana-McFarland Functions

## Corollary

*Let* $f(x) = a_0(x) + 2a_1(x) + \cdots + 2^{k-1}a_{k-1}(x)$ *a gbent function with partition* $\mathcal{P} = \{A(d) : 0 \leq d \leq 2^{k-1} - 1\}$.

- $|A(d)| \geq 2^{n/2}$, $0 \leq d \leq 2^{k-1} - 1$.
- *If* $|A(d)| = 2^{n/2}$, *then* $A(d)$ *is an affine subspace on which* $a_{k-1}$ *is affine.*
- $\mathcal{P}$ *can contain at most* $2^{n/2}$ *(nonempty) sets.*

# Maiorana-McFarland Functions

## Corollary

*Let $f(x) = a_0(x) + 2a_1(x) + \cdots + 2^{k-1}a_{k-1}(x)$ a gbent function with partition $\mathcal{P} = \{A(d) : 0 \leq d \leq 2^{k-1} - 1\}$.*

- $|A(d)| \geq 2^{n/2}$, $0 \leq d \leq 2^{k-1} - 1$.
- *If $|A(d)| = 2^{n/2}$, then $A(d)$ is an affine subspace on which $a_{k-1}$ is affine.*
- *$\mathcal{P}$ can contain at most $2^{n/2}$ (nonempty) sets.*

## Remark

Without blowing up, we have $k \leq n/2 + 1$. The dimension of $f$ is at most $n/2 + 1$.

# Maiorana-McFarland Functions

## Corollary

*If the partition $\mathcal{P}$ of a gbent function $f : \mathbb{F}_2^n \rightarrow \mathbb{Z}_{2^{n/2+1}}$ has this maximal possible number $2^{n/2}$ elements, then $a_{k-1}$ is in the completed Maiorana-McFarland class.*
*Conversely, every function in the completed Maiorana-McFarland class has such a (finest possible) partition, with an according gbent function from $\mathbb{F}_2^n$ to $\mathbb{Z}_{2^{n/2+1}}$.*

# Maiorana-McFarland Functions

## Corollary

*If the partition $\mathcal{P}$ of a gbent function $f : \mathbb{F}_2^n \to \mathbb{Z}_{2^{n/2+1}}$ has this maximal possible number $2^{n/2}$ elements, then $a_{k-1}$ is in the completed Maiorana-McFarland class.*
*Conversely, every function in the completed Maiorana-McFarland class has such a (finest possible) partition, with an according gbent function from $\mathbb{F}_2^n$ to $\mathbb{Z}_{2^{n/2+1}}$.*

## Remark

The set of bent functions $a_{n/2}(x) + C(x)$ is exactly the set of all bent functions one obtains from $a_{n/2}$ applying Carlet's construction (changing the values on the subspaces) repeatedly with the affine subspaces $A(d)$, $0 \leq d \leq 2^{n/2} - 1$.

# Maiorana-McFarland Functions

## Corollary

*If the partition $\mathcal{P}$ of a gbent function $f : \mathbb{F}_2^n \to \mathbb{Z}_{2^{n/2+1}}$ has this maximal possible number $2^{n/2}$ elements, then $a_{k-1}$ is in the completed Maiorana-McFarland class.*
*Conversely, every function in the completed Maiorana-McFarland class has such a (finest possible) partition, with an according gbent function from $\mathbb{F}_2^n$ to $\mathbb{Z}_{2^{n/2+1}}$.*

## Remark

The set of bent functions $a_{n/2}(x) + C(x)$ is exactly the set of all bent functions one obtains from $a_{n/2}$ applying Carlet's construction (changing the values on the subspaces) repeatedly with the affine subspaces $A(d)$, $0 \leq d \leq 2^{n/2} - 1$.

## Remark

The analolg result holds for gbent functions from $\mathbb{F}_p^n$ to $\mathbb{Z}_{p^k}$, $n$ even. In particular, there is no bent function from $\mathbb{F}_p^n$ to $\mathbb{Z}_{p^n}$.

# Maiorana-McFarland Functions

Kolomeec DCC, 2017 The only bent function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ with the properties

I $f$ is affine on some $n/2$-dimensional affine subspace of $\mathbb{F}_2^n$,

II if $f$ is affine on an $n/2$-dimensional affine subspace $L$ of $\mathbb{F}_2^n$, then $f$ is affine on every coset of $L$,

is the quadratic bent function (invariant under EA-equivalence).

# Maiorana-McFarland Functions

Kolomeec DCC, 2017 The only bent function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ with the properties

I $f$ is affine on some $n/2$-dimensional affine subspace of $\mathbb{F}_2^n$,

II if $f$ is affine on an $n/2$-dimensional affine subspace $L$ of $\mathbb{F}_2^n$, then $f$ is affine on every coset of $L$,

is the quadratic bent function (invariant under EA-equivalence).

**Corollary**

*For a quadratic bent function $q : \mathbb{F}_2^n \to \mathbb{F}_2$ there are $K = (2^1 + 1)(2^2 + 1) \cdot \cdots \cdot (2^{\frac{n}{2}} + 1)$ distinct partitions of $\mathbb{F}_2^n$ for gbent functions from $\mathbb{F}_2^n$ to $\mathbb{Z}_{2^{n/2+1}}$, i.e. K different gbent functions from $\mathbb{F}_2^n$ to $\mathbb{Z}_{2^{n/2+1}}$. This is the maximal number of such partitions a bent function can have.*

# Questions

- Show that there is only the spread relative difference set in $\mathbb{F}_2^n \times \mathbb{Z}_{2^{n/2}}$ $(\mathbb{F}_p^n \times \mathbb{Z}_{p^{n/2}})$
- Show that there is only the spread relative difference set in $\mathbb{F}_2^n \times \mathbb{Z}_{2^m}$ for $? \leq m \leq n/2$, or:
  What is the largest $m$ for which there exists a NOT-spread relative difference set in $\mathbb{F}_2^n \times \mathbb{Z}_{2^m}$?
- Find a class (from Maiorana-McFarland?) of NOT-spread relative difference sets in $\mathbb{F}_2^n \times \mathbb{Z}_{2^m}$ for some $n$ and $m \geq 3$
- Find "best partitions" (gbent functions into $\mathbb{Z}_{2^m}$, "large" $m$) for classes of bent functions different from spread, Maiorana-McFarland.
- What about relative difference sets in $\mathbb{F}_p^n \times B$, other $B$ with $|B| = p^k$?