Generalized bent functions from spreads and their spectra

Wilfried Meidl, Alexander Pott

RICAM, Linz; Otto von Guericke University Magdeburg

July 4, 2017

Bent functions

Definition

Let A, B be (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 χ 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 (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 χ 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.

$f : \mathbb{F}_2^n \to \mathbb{Z}_{2^k} \quad (f : \mathbb{F}_p^n \to \mathbb{Z}_{p^k})$

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

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

Generalized Bent Functions

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 $u \in \mathbb{F}_2^n$.

Generalized Bent Functions

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 (bent function).

Generalized Bent Functions

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 (bent function).

Questions:

- Does this definition give anything interesting?

Not accepted: Cheating function: $f : \mathbb{F}_2^n \to \mathbb{Z}_{2^k}$, $f(x) = 2^{k-1} a(x)$, where $a : \mathbb{V}_2^n \to \mathbb{F}_2$ is bent.

Generalized Bent Functions, n even

Generalized Bent Functions, n even

Theorem (Hodzic, M.,Pasalic)

Let n be even. A gbent function

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

from $\mathbb{F}_2^n$ to $\mathbb{Z}_{2^k}$ is a $(k-1)$-dimensional affine space

$$\mathcal{A} = a_{k-1} \oplus \langle a_0, \ldots, a_{k-2} \rangle$$

of bent functions such that for $h_0, h_1, h_2, h_3 \in \mathcal{A}$ with $h_0 \oplus h_1 \oplus h_2 \oplus h_3 = 0$ we have $h_0^* \oplus h_1^* \oplus h_2^* \oplus h_3^* = 0$.

(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.)

Generalized Bent Functions, n even

Theorem (Hodzic, M.,Pasalic)

Let n be even. A gbent function

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

from $\mathbb{F}_2^n$ to $\mathbb{Z}_{2^k}$ is a $(k-1)$-dimensional affine space

$$\mathcal{A} = a_{k-1} \oplus \langle a_0, \ldots, a_{k-2} \rangle$$

of bent functions such that for $h_0, h_1, h_2, h_3 \in \mathcal{A}$ with $h_0 \oplus h_1 \oplus h_2 \oplus h_3 = 0$ we have $h_0^* \oplus h_1^* \oplus h_2^* \oplus h_3^* = 0$.

(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.)

Generalization to odd p. Mesnager, et al.

Generalized Bent Functions, n even

Theorem (Hodzic, M.,Pasalic)

Let n be even. A gbent function

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

from $\mathbb{F}_2^n$ to $\mathbb{Z}_{2^k}$ is a $(k-1)$-dimensional affine space

$$\mathcal{A} = a_{k-1} \oplus \langle a_0, \ldots, a_{k-2} \rangle$$

of bent functions such that for $h_0, h_1, h_2, h_3 \in \mathcal{A}$ with $h_0 \oplus h_1 \oplus h_2 \oplus h_3 = 0$ we have $h_0^* \oplus h_1^* \oplus h_2^* \oplus h_3^* = 0$.

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

Generalization to odd p. Mesnager, et al.

Important: A gbent function always has to be seen together with its dimension.

Gbent function and its dimension

Cheating function: $f(x) = 2^{k-1}a_{k-1}(x)$ satisfies $|\mathcal{H}_f^k(u)| = 2^{n/2}$ if a_{k-1} is a bent function. Value set: $\{0, 2^{k-1}\} \cong \mathbb{F}_2$; $\dim(\mathcal{L}) = 0$

Gbent function and its dimension

Cheating function: $f(x) = 2^{k-1}a_{k-1}(x)$ satisfies $|\mathcal{H}_f^k(u)| = 2^{n/2}$ if a_{k-1} is a bent function. Value set: $\{0, 2^{k-1}\} \cong \mathbb{F}_2$; $\dim(\mathcal{L}) = 0$

More general: If

$$\tilde{f}(x) = b_0(x) + 2b_1(x) + \cdots + 2^{r-2}b_{r-2}(x) + 2^{r-1}b_{r-1}(x)$$

satisfies $|\mathcal{H}_f^r(u)| = 2^{n/2}$ and

$$\mathcal{A} = b_{r-1} \oplus \langle b_0, \ldots, b_{r-2} \rangle = a_{k-1} \oplus \langle a_0, \ldots, a_{k-2} \rangle,$$

with linearly independent $a_0, \ldots, a_{k-2}$, then

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

is a gbent function from $\mathbb{F}_2^n$ to $\mathbb{Z}_{2^k}$. Its dimension is $k-1$.

Questions

- How can I find meaningful examples.

Questions

- How can I find meaningful examples.
- What about the other characters?
  How many character sums can have the "correct" value without that we must have a bent function.
  How close can I be at a bent function from character values point of view, without being bent?

Spread Bent Functions

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

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

Spread Bent Functions

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

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

Partition of $\mathbb{V}_n$

Spread Bent Functions

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

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

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 even, $|B| = p^k$, $k \leq n/2$. $(B = \mathbb{Z}_p^k, \mathbb{Z}_{p^k})$

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

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.

Spread Bent Functions

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

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

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.

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

Spread Bent Functions

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

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

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.

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

Here $B = \mathbb{Z}_p^k$ or $B = \mathbb{Z}_{p^k}$.

Most interesting $k = n/2$: For every $c \in B$ the nonzero elements of exactly 1 of the U_i's, $1 \leq i \leq p^m$, are mapped to c.

Spread Bent Functions

Sketch of proof ($B = \mathbb{Z}_{p^k}$).

$$\begin{aligned}
\mathcal{H}_f^k(\alpha, u) &= \sum_{i=0}^{p^m} \sum_{z \in U_i \setminus \{0\}} \epsilon_{p^k}^{\alpha f(z)} \epsilon_p^{u \cdot z} + \epsilon_{p^k}^{\alpha f(0)} \\
&= \sum_{i=0}^{p^m} \sum_{z \in U_i} \epsilon_{p^k}^{\alpha c_i} \epsilon_p^{u \cdot z} - \sum_{i=1}^{p^m} \epsilon_{p^k}^{\alpha c_i} \\
&= \sum_{i=0}^{p^m} \epsilon_{p^k}^{\alpha c_i} \sum_{z \in U_i} \epsilon_p^{u \cdot z} - \sum_{i=1}^{p^m} \epsilon_{p^k}^{\alpha c_i}.
\end{aligned}$$

$u \in \mathbb{V}_n$, $u \neq 0$, then $u \cdot z$ is trivial on exactly one spread element U_{i_u}, i.e. $u \cdot z = 0$ for all $z \in U_{i_u}$.

Spread Bent Functions

Sketch of proof ($B = \mathbb{Z}_{p^k}$). $u \neq 0$:

$$\mathcal{H}_f^k(\alpha, u) = p^m \epsilon_{p^k}^{\alpha c_{i_u}} - \sum_{i=1}^{p^m} \epsilon_{p^k}^{\alpha c_i}.$$

$$\mathcal{H}_f^k(\alpha, 0) = p^m + (p^m - 1) \sum_{i=1}^{p^m} \epsilon_{p^k}^{\alpha c_i}.$$

($f(x) = c_i$ if $x \in U_i^*$, $1 \leq i \leq p^m$)

Spread Bent Functions

Sketch of proof ($B = \mathbb{Z}_{p^k}$). $u \neq 0$:

$$\mathcal{H}_f^k(\alpha, u) = p^m \epsilon_{p^k}^{\alpha c_{i_u}} - \sum_{i=1}^{p^m} \epsilon_{p^k}^{\alpha c_i}.$$

$$\mathcal{H}_f^k(\alpha, 0) = p^m + (p^m - 1) \sum_{i=1}^{p^m} \epsilon_{p^k}^{\alpha c_i}.$$

($f(x) = c_i$ if $x \in U_i^*$, $1 \leq i \leq p^m$)

$\sum_{i=1}^{p^m} \epsilon_{p^k}^{\alpha c_i} = 0$ for all nonzero $\alpha \in \mathbb{Z}_{2^k}$.

Spread Gbent Functions

We only need the weaker condition for $\alpha = 1$,

$$\sum_{i=1}^{p^m} \epsilon_{p^k}^{c_i} = 0$$

$p = 2$: Note $\epsilon_{2^k}^{c} = -\epsilon_{2^k}^{c+2^{k-1}}$

Spread Gbent Functions

We only need the weaker condition for $\alpha = 1$,

$$\sum_{i=1}^{p^m} \epsilon_{p^k}^{c_i} = 0$$

$p = 2$: Note $\epsilon_{2^k}^{c} = -\epsilon_{2^k}^{c+2^{k-1}}$

Proposition

Gbent functions $f : \mathbb{V}_n \to \mathbb{Z}_{2^k}$ from spreads (M., Martinsen, Stanica (DCC))

Spread $U_0, U_1, \ldots, U_{2^m}$ of $\mathbb{V}_n$, $n = 2m$.

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

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

Spread Gbent Functions

We only need the weaker condition for $\alpha = 1$,

$$\sum_{i=1}^{p^m} \epsilon_{p^k}^{c_i} = 0$$

$p = 2$: Note $\epsilon_{2^k}^{c} = -\epsilon_{2^k}^{c+2^{k-1}}$

Proposition

Gbent functions $f : \mathbb{V}_n \to \mathbb{Z}_{2^k}$ from spreads (M., Martinsen, Stanica (DCC))

Spread $U_0, U_1, \ldots, U_{2^m}$ of $\mathbb{V}_n$, $n = 2m$.

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

- $f(x) = 0$ 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 $0 \leq c \leq 2^{k-1} - 1$. (**)

Spread Gbent Functions, p odd

Analog: Gbent functions $f : \mathbb{V}_n \to \mathbb{Z}_{p^k}$ from spreads, p odd.

Spread $U_0, U_1, \ldots, U_{p^m}$ of $\mathbb{V}_n \cong \mathbb{F}_p^n$, $n = 2m$.

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

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

Designing gbent functions with prescribed character values

Objective: Prescribe α for which $|\mathcal{H}_f^k(\alpha, u)| = 2^{n/2}$ for a meaningful function f from $\mathbb{V}_n \cong \mathbb{F}_2^n$ to the cyclic group $\mathbb{Z}_{2^k}$. Take $k = m = n/2$.

Designing gbent functions with prescribed character values

Objective: Prescribe α for which $|\mathcal{H}_f^k(\alpha, u)| = 2^{n/2}$ for a meaningful function f from $\mathbb{V}_n \cong \mathbb{F}_2^n$ to the cyclic group $\mathbb{Z}_{2^k}$. Take $k = m = n/2$.

Remark

$|\mathcal{H}_f^k(2^t r, u)| = |\mathcal{H}_f^k(2^t, u)|$ for all odd r. (Same order characters)

$\mathcal{H}_f^k(2^t, u) = \mathcal{H}_{2^t f}^{k-t}(1, u) \quad (2^t f : \mathbb{V}_n \to \mathbb{Z}_{2^{k-t}})$.

Designing gbent functions with prescribed character values

Objective: Prescribe α for which $|\mathcal{H}_f^k(\alpha, u)| = 2^{n/2}$ for a meaningful function f from $\mathbb{V}_n \cong \mathbb{F}_2^n$ to the cyclic group $\mathbb{Z}_{2^k}$. Take $k = m = n/2$.

Remark

$|\mathcal{H}_f^k(2^t r, u)| = |\mathcal{H}_f^k(2^t, u)|$ for all odd r. (Same order characters)

$\mathcal{H}_f^k(2^t, u) = \mathcal{H}_{2^t f}^{k-t}(1, u) \quad (2^t f : \mathbb{V}_n \to \mathbb{Z}_{2^{k-t}})$.

Objective: Construct $f : \mathbb{V}_n \to \mathbb{Z}_{2^k}$ such that for a given subset $T \subset \{0, 1, \ldots k-1\}$ we have $|\mathcal{H}_f^k(2^t, u)| = 2^{n/2}$ if $t \in T$ and $|\mathcal{H}_f^k(2^t, u)| \neq 2^{n/2}$ if $t \notin T$.

Equivalently: Construct f such that for $2^t f : \mathbb{V}_n \to \mathbb{Z}_{2^{k-t}}$ the condition (**) is satisfied if and only if $t \in T$.

We will use spreads.

Bent $\mathbb{V}_{10} \to \mathbb{Z}_{32}$

j :	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
# :	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
j :	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
# :	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1

Bent $\mathbb{V}_{10} \to \mathbb{Z}_{32}$

j:	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
#:	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
j:	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
#:	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1

With this choice the distribution for $2f$, $4f$, $8f$, $16f$ is as follows:

j:	0	2	4	6	8	10	12	14	16	18	20	22	24	26	28	30
#:	3	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2

j:	0	4	8	12	16	20	24	28
#:	5	4	4	4	4	4	4	4

j:	0	8	16	24
#:	9	8	8	8

j:	0	16
#:	17	16

.

$\mathbb{V}_{10} \to \mathbb{Z}_{32}$, $2f$ not gbent

j :	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
# :	2	2	1	0	1	1	0	1	1	0	1	2	1	1	2	1
j :	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
# :	1	2	1	0	1	1	0	1	1	0	1	2	1	1	2	1

With this choice the distribution for $2f$, $4f$, $8f$, $16f$ is as follows:

j :	0	2	4	6	8	10	12	14	16	18	20	22	24	26	28	30
# :	3	4	2	0	2	2	0	2	2	0	2	4	2	2	4	2

j :	0	4	8	12	16	20	24	28
# :	5	4	4	4	4	4	4	4

j :	0	8	16	24
# :	9	8	8	8

j :	0	16
# :	17	16

.

Value set: 26

$\mathbb{V}_{10} \to \mathbb{Z}_{32}$, $2f$, $8f$ not gbent

j :	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
# :	2	0	2	2	1	0	1	2	1	0	0	2	1	0	1	2
j :	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
# :	1	0	2	2	1	0	1	2	1	0	0	2	1	0	1	2

With this choice the distribution for $2f$, $4f$, $8f$, $16f$ is as follows:

j :	0	2	4	6	8	10	12	14	16	18	20	22	24	26	28	30
# :	3	0	4	4	2	0	2	4	2	0	0	4	2	0	2	4

j :	0	4	8	12	16	20	24	28
# :	5	0	4	8	4	0	4	8

j :	0	8	16	24
# :	9	0	8	16

j :	0	16
# :	17	16

.

Value set: 22

j :	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
# :	3	0	2	0	2	0	2	0	2	0	2	0	2	0	2	0
j :	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
# :	2	0	2	0	2	0	2	0	2	0	2	0	2	0	2	0

With this choice the distribution for $2f$, $4f$, $8f$, $16f$ is as follows:

j :	0	2	4	6	8	10	12	14	16	18	20	22	24	26	28	30
# :	5	0	4	0	4	0	4	0	4	0	4	0	4	0	4	0

j :	0	4	8	12	16	20	24	28
# :	9	0	8	0	8	0	8	0

j :	0	8	16	24
# :	17	0	16	0

j :	0	16
# :	33	0

.

$j:$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$\#:$	3	0	2	0	2	0	2	0	2	0	2	0	2	0	2	0

$j:$	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
$\#:$	2	0	2	0	2	0	2	0	2	0	2	0	2	0	2	0

With this choice the distribution for $2f$, $4f$, $8f$, $16f$ is as follows:

$j:$	0	2	4	6	8	10	12	14	16	18	20	22	24	26	28	30
$\#:$	5	0	4	0	4	0	4	0	4	0	4	0	4	0	4	0

$j:$	0	4	8	12	16	20	24	28
$\#:$	9	0	8	0	8	0	8	0

$j:$	0	8	16	24
$\#:$	17	0	16	0

$j:$	0	16
$\#:$	33	0

.

Not a gbent function from $\mathbb{V}_{10}$ to $\mathbb{Z}_{32}$, but a bent function from $\mathbb{V}_{10}$ to $\mathbb{Z}_{16}$.

$\mathbb{V}_{10} \to \mathbb{Z}_{32}$, only $16f$ not bent!

j :	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
# :	1	2	0	2	0	2	0	2	0	2	0	2	0	2	0	2
j :	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
# :	0	2	0	2	0	2	0	2	0	2	0	2	0	2	0	2

With this choice the distribution for $2f$, $4f$, $8f$, $16f$ is as follows:

j :	0	2	4	6	8	10	12	14	16	18	20	22	24	26	28	30
# :	1	4	0	4	0	4	0	4	0	4	0	4	0	4	0	4

j :	0	4	8	12	16	20	24	28
# :	1	8	0	8	0	8	0	8

j :	0	8	16	24
# :	1	16	0	16

j :	0	16
# :	1	32

.

Value set: 17

$\mathbb{V}_{10} \to \mathbb{Z}_{32}$, only $16f$ not bent!

j:	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
#:	1	2	0	2	0	2	0	2	0	2	0	2	0	2	0	2

j:	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
#:	0	2	0	2	0	2	0	2	0	2	0	2	0	2	0	2

With this choice the distribution for $2f$, $4f$, $8f$, $16f$ is as follows:

j:	0	2	4	6	8	10	12	14	16	18	20	22	24	26	28	30
#:	1	4	0	4	0	4	0	4	0	4	0	4	0	4	0	4

j:	0	4	8	12	16	20	24	28
#:	1	8	0	8	0	8	0	8

j:	0	8	16	24
#:	1	16	0	16

j:	0	16
#:	1	32

.

Value set: 17

$|\mathcal{H}_f^5(\alpha, u)| \neq 2^5$ only for $\alpha = 16$.

$f : \mathbb{F}_3^6 \to \mathbb{Z}_{27}$, bent

j :	0	1	2	3	4	5	6	7	8
# :	2	1	1	1	1	1	1	1	
j :	9	10	11	12	13	14	15	16	17
# :	1	1	1	1	1	1	1	1	1
j :	18	19	20	21	22	23	24	25	26
# :	1	1	1	1	1	1	1	1	1

With this choice the distribution for $3f$, $9f$ is as follows:

j :	0	3	6	9	12	15	18	21	24
# :	4	3	3	3	3	3	3	3	3

j :	0	9	18
# :	10	9	9

$f : \mathbb{F}_3^6 \to \mathbb{Z}_{27}$, gbent, not bent

j :	0	1	2	3	4	5	6	7	8
# :	2	2	1	1	1	1	1	0	1
j :	9	10	11	12	13	14	15	16	17
# :	1	2	1	1	1	1	1	0	1
j :	18	19	20	21	22	23	24	25	26
# :	1	2	1	1	1	1	1	0	1

With this choice the distribution for $3f$, $9f$ is as follows:

j :	0	3	6	9	12	15	18	21	24
# :	4	6	3	3	3	3	3	0	3

j :	0	9	18
# :	10	9	9

Value set: 24

Gbent functions and their partitions

Gbent functions are "spread-like" functions:

Let $f(x) = a_0(x) + \ldots + 2^{k-2}a_{k-2}(x) + 2^{k-1}a_{k-1}(x)$ be a gbent function (then a_{k-1} is bent). Define

$$P_z = \{x \in \mathbb{F}_2^n \,:\, f(x) - 2^{k-1}a_{k-1}(x) = z\}, \quad z \in \mathbb{Z}_{2^{k-1}}.$$

Partition of $\mathbb{F}_2^n$: $\quad \mathcal{P} = \{P_z \,:\, z \in \mathbb{Z}_{2^{k-1}}\}.$

Gbent functions and their partitions

Gbent functions are "spread-like" functions:

Let $f(x) = a_0(x) + \ldots + 2^{k-2}a_{k-2}(x) + 2^{k-1}a_{k-1}(x)$ be a gbent function (then a_{k-1} is bent). Define

$$P_z = \{x \in \mathbb{F}_2^n \,:\, f(x) - 2^{k-1}a_{k-1}(x) = z\}, \quad z \in \mathbb{Z}_{2^{k-1}}.$$

Partition of $\mathbb{F}_2^n$: $\mathcal{P} = \{P_z \,:\, z \in \mathbb{Z}_{2^{k-1}}\}$.

Example (Spread)

j :	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
# :	2	0	2	2	1	0	1	2	1	0	0	2	1	0	1	2
j :	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
# :	1	0	2	2	1	0	1	2	1	0	0	2	1	0	1	2

Gbent functions and their partitions

Gbent functions are "spread-like" functions:

Let $f(x) = a_0(x) + \ldots + 2^{k-2}a_{k-2}(x) + 2^{k-1}a_{k-1}(x)$ be a gbent function (then a_{k-1} is bent). Define

$$P_z = \{x \in \mathbb{F}_2^n \, : \, f(x) - 2^{k-1}a_{k-1}(x) = z\}, \quad z \in \mathbb{Z}_{2^{k-1}}.$$

Partition of $\mathbb{F}_2^n$: $\mathcal{P} = \{P_z \, : \, z \in \mathbb{Z}_{2^{k-1}}\}$.

Example (Spread)

j :	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
# :	2	0	2	2	1	0	1	2	1	0	0	2	1	0	1	2

j :	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
# :	1	0	2	2	1	0	1	2	1	0	0	2	1	0	1	2

Partition into 11 sets.

Gbent functions and their partitions

Theorem

(Mesnager et al. also for odd characteristic):

Let $\mathcal{P}$ be the partition for the gbent function $f(x) = a_0(x) + \ldots + 2^{k-2}a_{k-2}(x) + 2^{k-1}a_{k-1}(x)$. For every function $F : \mathbb{F}_2^n \to \mathbb{Z}_{2^{k-1}}$ which is constant on the elements of $\mathcal{P}$ the function

$$g(x) = 2^{k-1}a_{k-1}(x) + F(x)$$

satisfies $|\mathcal{H}_f^k(u)| = 2^{n/2}$ for all $u \in \mathbb{F}_2^n$.

j :	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
# :	2	0	2	2	1	0	1	2	1	0	0	2	1	0	1	2
j :	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
# :	1	0	2	2	1	0	1	2	1	0	0	2	1	0	1	2

Gbent functions and their partitions

Theorem
(Mesnager et al. also for odd characteristic):
Let $\mathcal{P}$ be the partition for the gbent function $f(x) = a_0(x) + \ldots + 2^{k-2}a_{k-2}(x) + 2^{k-1}a_{k-1}(x)$. For every function $F : \mathbb{F}_2^n \to \mathbb{Z}_{2^{k-1}}$ which is constant on the elements of $\mathcal{P}$ the function

$$g(x) = 2^{k-1}a_{k-1}(x) + F(x)$$

satisfies $|\mathcal{H}_f^k(u)| = 2^{n/2}$ for all $u \in \mathbb{F}_2^n$.

j :	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
# :	2	0	2	0	1	2	1	2	1	0	0	2	1	0	1	2

j :	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
# :	1	0	2	0	1	2	1	2	1	0	0	2	1	0	1	2

Gbent functions and their partitions

Theorem
(Mesnager et al. also for odd characteristic):
Let $\mathcal{P}$ be the partition for the gbent function $f(x) = a_0(x) + \ldots + 2^{k-2}a_{k-2}(x) + 2^{k-1}a_{k-1}(x)$. For every function $F : \mathbb{F}_2^n \to \mathbb{Z}_{2^{k-1}}$ which is constant on the elements of $\mathcal{P}$ the function

$$g(x) = 2^{k-1}a_{k-1}(x) + F(x)$$

satisfies $|\mathcal{H}_f^k(u)| = 2^{n/2}$ for all $u \in \mathbb{F}_2^n$.

j :	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
# :	2	0	2	0	3	0	1	2	1	0	0	2	1	0	1	2
j :	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
# :	1	0	2	0	3	0	1	2	1	0	0	2	1	0	1	2

Gbent functions and their partitions

Theorem
(Mesnager et al. also for odd characteristic):
Let $\mathcal{P}$ be the partition for the gbent function $f(x) = a_0(x) + \ldots + 2^{k-2}a_{k-2}(x) + 2^{k-1}a_{k-1}(x)$. For every function $F : \mathbb{F}_2^n \to \mathbb{Z}_{2^{k-1}}$ which is constant on the elements of $\mathcal{P}$ the function

$$g(x) = 2^{k-1}a_{k-1}(x) + F(x)$$

satisfies $|\mathcal{H}_f^k(u)| = 2^{n/2}$ for all $u \in \mathbb{F}_2^n$.

j :	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
# :	2	0	2	0	3	0	1	2	1	0	0	2	1	0	1	2

j :	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
# :	1	0	2	0	3	0	1	2	1	0	0	2	1	0	1	2

NOTE: A spread can do more!

Questions

Is there something but (partial) spreads?

Questions

Is there something but (partial) spreads?

- Find gbent functions $f : \mathbb{F}_2^n \to \mathbb{Z}_{2^k}$ which do not come from (partial) spreads for $k \geq 3$.
- What is the largest k (depending on n?) for which there exists a gbent function $f : \mathbb{F}_2^n \to \mathbb{Z}_{2^k}$ not coming from spreads?

Questions

Is there something but (partial) spreads?

- Find gbent functions $f : \mathbb{F}_2^n \to \mathbb{Z}_{2^k}$ which do not come from (partial) spreads for $k \geq 3$.
- What is the largest k (depending on n?) for which there exists a gbent function $f : \mathbb{F}_2^n \to \mathbb{Z}_{2^k}$ not coming from spreads?
- Find bent functions $f : \mathbb{F}_2^n \to \mathbb{Z}_{2^k}$ which do not come from spreads for $3 \leq k \leq n/2$.
- What is the largest k (depending on n?) for which there exists a bent function $f : \mathbb{F}_2^n \to \mathbb{Z}_{2^k}$ not coming from spreads?

Questions

Is there something but (partial) spreads?

- Find gbent functions $f : \mathbb{F}_2^n \to \mathbb{Z}_{2^k}$ which do not come from (partial) spreads for $k \geq 3$.
- What is the largest k (depending on n?) for which there exists a gbent function $f : \mathbb{F}_2^n \to \mathbb{Z}_{2^k}$ not coming from spreads?
- Find bent functions $f : \mathbb{F}_2^n \to \mathbb{Z}_{2^k}$ which do not come from spreads for $3 \leq k \leq n/2$.
- What is the largest k (depending on n?) for which there exists a bent function $f : \mathbb{F}_2^n \to \mathbb{Z}_{2^k}$ not coming from spreads?

Is there a gbent function from $\mathbb{F}_2^n$ to $\mathbb{Z}_{2^k}$ for $k > n/2$?

- What is the largest k, for which there exists a gbent function from $\mathbb{F}_2^n$ to $\mathbb{Z}_{2^k}$?

All questions make also sense for functions from $\mathbb{F}_p^n$ to $\mathbb{Z}_{p^k}$.