Relative Difference Sets and their Component Functions

Alexander Pott

Otto-von-Guericke-University Magdeburg

September 05, 2014

Outline

- Boolean and p-ary vectorial bent functions and their relative difference sets.
- Extendability.
- $p = 2$: Vectorial bent functions and their relative difference sets.
- Interpretation in terms of KNUTH cube.

Bent Functions

$f : \mathbb{Z}_2^n \to \mathbb{Z}_2$ is bent if one of the following holds:

- $x \mapsto f(x+a) - f(x)$ is balanced for all $a \neq 0$.
- $\left| \sum_x (-1)^{f(x)+\langle a,x \rangle} \right| = 2^{n/2}$ for all a, where $\langle \, , \, \rangle$ is standard inner product.

Bent Functions

$f : \mathbb{Z}_2^n \to \mathbb{Z}_2$ is bent if one of the following holds:

- $x \mapsto f(x+a) - f(x)$ is balanced for all $a \neq 0$.
- $|\sum_x (-1)^{f(x)+\langle a,x\rangle}| = 2^{n/2}$ for all a, where $\langle\ ,\ \rangle$ is standard inner product.
- $D_f := \{x \in \mathbb{Z}_2^n \ :\ f(x) = 1\}$ is a $(2^n, 2^{n-1} \pm 2^{(n-2)/2}, 2^{n-2} \pm 2^{(n-2)/2})$ difference set (support of f).

Bent Functions

$f : \mathbb{Z}_2^n \to \mathbb{Z}_2$ is bent if one of the following holds:

- $x \mapsto f(x+a) - f(x)$ is balanced for all $a \neq 0$.
- $|\sum_x (-1)^{f(x)+\langle a,x\rangle}| = 2^{n/2}$ for all a, where $\langle\ ,\ \rangle$ is standard inner product.
- $D_f := \{x \in \mathbb{Z}_2^n \ : \ f(x) = 1\}$ is a $(2^n, 2^{n-1} \pm 2^{(n-2)/2}, 2^{n-2} \pm 2^{(n-2)/2})$ difference set (support of f).
- $G_f := \{(x, f(x)) \ : \ x \in \mathbb{Z}_2^n\} \subseteq \mathbb{Z}_2^{n+1}$ is a relative $(2^n, 2, 2^n, 2^{n-1})$ difference set (graph of the function f).

An example

$$f(x_1, x_2, x_3, x_4) = x_1 x_2 + x_3 x_4.$$

The support:

$$D_f = \{ \begin{pmatrix}1\\1\\0\\0\end{pmatrix}, \begin{pmatrix}1\\1\\0\\1\end{pmatrix}, \begin{pmatrix}1\\1\\1\\0\end{pmatrix}, \begin{pmatrix}0\\0\\1\\1\end{pmatrix}, \begin{pmatrix}0\\1\\1\\1\end{pmatrix}, \begin{pmatrix}1\\0\\1\\1\end{pmatrix} \}.$$

The graph G_f:

$$\begin{pmatrix}0\\0\\0\\0\\0\end{pmatrix}, \begin{pmatrix}0\\0\\0\\1\\0\end{pmatrix}, \begin{pmatrix}0\\0\\1\\0\\0\end{pmatrix}, \begin{pmatrix}0\\0\\1\\1\\1\end{pmatrix}, \begin{pmatrix}0\\1\\0\\0\\0\end{pmatrix}, \begin{pmatrix}0\\1\\0\\1\\0\end{pmatrix}, \begin{pmatrix}0\\1\\1\\0\\0\end{pmatrix}, \begin{pmatrix}0\\1\\1\\1\\1\end{pmatrix}, \begin{pmatrix}1\\0\\0\\0\\0\end{pmatrix}, \begin{pmatrix}1\\0\\0\\1\\0\end{pmatrix}, \begin{pmatrix}1\\0\\1\\0\\0\end{pmatrix}, \begin{pmatrix}1\\0\\1\\1\\1\end{pmatrix}, \begin{pmatrix}1\\1\\0\\0\\1\end{pmatrix}, \begin{pmatrix}1\\1\\0\\1\\1\end{pmatrix}, \begin{pmatrix}1\\1\\1\\0\\1\end{pmatrix}, \begin{pmatrix}1\\1\\1\\1\\0\end{pmatrix}$$

(Relative) Difference Sets with Parameters (m, n, k, λ).

- group Γ of order $m \cdot n$
- subgroup Λ of order n
- subset $D \subseteq \Gamma$ of order k
- $x - y = b$ has $\begin{cases} k \text{ solutions if } b = 0 \\ 0 \text{ solutions if } b \in \Lambda \setminus \{0\} \\ \lambda \text{ solutions if } b \notin \Lambda \end{cases}$

  with $x, y \in D$.

(Relative) Difference Sets with Parameters (m, n, k, λ).

- group Γ of order $m \cdot n$
- subgroup Λ of order n
- subset $D \subseteq \Gamma$ of order k
- $x - y = b$ has $\begin{cases} k \text{ solutions if } b = 0 \\ 0 \text{ solutions if } b \in \Lambda \setminus \{0\} \\ \lambda \text{ solutions if } b \notin \Lambda \end{cases}$

  with $x, y \in D$.

Remark

1. *Difference set relative to* Λ.

(Relative) Difference Sets with Parameters (m, n, k, λ).

- group Γ of order $m \cdot n$
- subgroup Λ of order n
- subset $D \subseteq \Gamma$ of order k
- $x - y = b$ has $\begin{cases} k \text{ solutions if } b = 0 \\ 0 \text{ solutions if } b \in \Lambda \setminus \{0\} \\ \lambda \text{ solutions if } b \notin \Lambda \end{cases}$

  with $x, y \in D$.

Remark

1. *Difference set relative to Λ.*
2. *If $n = 1$: (m, k, λ) difference set.*

(Relative) Difference Sets with Parameters (m, n, k, λ).

- group Γ of order $m \cdot n$
- subgroup Λ of order n
- subset $D \subseteq \Gamma$ of order k
- $x - y = b$ has $\begin{cases} k \text{ solutions if } b = 0 \\ 0 \text{ solutions if } b \in \Lambda \setminus \{0\} \\ \lambda \text{ solutions if } b \notin \Lambda \end{cases}$
  with $x, y \in D$.

Remark

1. *Difference set relative to Λ.*
2. *If $n = 1$: (m, k, λ) difference set.*
3. *D is a transversal of Λ if $k = m$.*

Examples

The following are equivalent:

- $f : \mathbb{Z}_2^n \to \mathbb{Z}_2$ is bent
- D_f is $(2^n, 2^{n-1} \pm 2^{(n-2)/2}, 2^{n-2} \pm 2^{(n-2)/2})$ difference set in $\mathbb{Z}_2^n$. $n = 4$: $(16, 6, 2)$ or $(16, 10, 6)$.
- G_f is $(2^n, 2, 2^n, 2^{n-1})$ difference set relative to $\{(0, y) \ : \ y \in \mathbb{Z}_2\}$. $n = 4$: $(16, 2, 16, 8)$

Examples

The following are equivalent:

- $f : \mathbb{Z}_2^n \to \mathbb{Z}_2$ is bent
- D_f is $(2^n, 2^{n-1} \pm 2^{(n-2)/2}, 2^{n-2} \pm 2^{(n-2)/2})$ difference set in $\mathbb{Z}_2^n$. $n = 4$: $(16, 6, 2)$ or $(16, 10, 6)$.
- G_f is $(2^n, 2, 2^n, 2^{n-1})$ difference set relative to $\{(0, y) \ : \ y \in \mathbb{Z}_2\}$. $n = 4$: $(16, 2, 16, 8)$

Example

1. $\{0, 1, 3\}$ is a $(7, 3, 1)$ difference set in $\mathbb{Z}_7$.
2. $\{1, 2, 4, 8\}$ is a $(5, 3, 4, 1)$ difference set in $\mathbb{Z}_{15}$ relative to $5\mathbb{Z}_{15}$.

Comment on Equivalence

Remark

- *Equivalent bent functions give rise to equivalent RDS* G_f.
- *Equivalent bent functions may give rise to inequivalent difference sets* D_f*!*

The General Case: p Prime

$f : \mathbb{Z}_p^n \to \mathbb{Z}_p$ is bent if one of the following holds:

- $f(x+a) - f(x) = b$ has p^{n-1} solutions for all $a \neq 0$ and all $b \in \mathbb{Z}_p$.

The General Case: p Prime

$f : \mathbb{Z}_p^n \to \mathbb{Z}_p$ is bent if one of the following holds:

- $f(x+a) - f(x) = b$ has p^{n-1} solutions for all $a \neq 0$ and all $b \in \mathbb{Z}_p$.
-
$$| \sum_x \zeta_p^{f(x)+\langle a,x\rangle} |= p^{n/2}$$

  for all $a \in \mathbb{Z}_p^n$. $\qquad (\zeta_p = e^{2\pi i/p})$

The General Case: p Prime

$f : \mathbb{Z}_p^n \to \mathbb{Z}_p$ is bent if one of the following holds:

- $f(x+a) - f(x) = b$ has p^{n-1} solutions for all $a \neq 0$ and all $b \in \mathbb{Z}_p$.
- $$|\sum_x \zeta_p^{f(x)+\langle a,x \rangle}| = p^{n/2}$$
  for all $a \in \mathbb{Z}_p^n$. $(\zeta_p = e^{2\pi \mathrm{i}/p})$
- $G_f := \{(x, f(x)) \ : \ x \in \mathbb{Z}_p^n\} \subseteq \mathbb{Z}_p^{n+1}$ is a (p^n, p, p^n, p^{n-1}) difference set relative to
  $$\Lambda = \{(0, y) \ : \ y \in \mathbb{Z}_p\}.$$

Quadratic Examples

1. $\mathbf{A} \in \mathrm{GL}(n, p)$ symmetric, full rank, p odd:
$$f(x) = x^T \cdot \mathbf{A} \cdot x$$

2. $\mathbf{A} \in \mathrm{GL}(n, 2)$ symmetric with zero diagonal (alternating), full rank:
$$f(x) = \sum_{i<j} a_{i,j} x_i x_j$$

These are quadratic examples: $x \mapsto f(x+a) - f(x) - f(a) + f(0)$ is linear!

Vectorial Bent

A mapping $F : \mathbb{Z}_p^n \to \mathbb{Z}_p^m$ is vecorial bent if

$$F(x + a) - F(x) = b$$

has p^{n-m} solutions for all $a \neq 0$ and all b.

Vectorial Bent

A mapping $F : \mathbb{Z}_p^n \to \mathbb{Z}_p^m$ is vecorial bent if

$$F(x+a) - F(x) = b$$

has p^{n-m} solutions for all $a \neq 0$ and all b.

Equivalently:

- $G_f : \{(x, F(x)) \ : \ x \in \mathbb{Z}_p^n\} \subseteq \mathbb{Z}_p^{n+m}$ is a (p^n, p^m, p^n, p^{n-m}) difference set relative to $\Lambda = \{(0, y) \ : \ y \in \mathbb{Z}_p^m\}$.
- All component functions $x \mapsto \langle b, F(x) \rangle$ with $a \neq 0$ are bent.

Vectorial Bent

A mapping $F : \mathbb{Z}_p^n \to \mathbb{Z}_p^m$ is vecorial bent if

$$F(x + a) - F(x) = b$$

has p^{n-m} solutions for all $a \neq 0$ and all b.

Equivalently:

- $G_f : \{(x, F(x)) \ : \ x \in \mathbb{Z}_p^n\} \subseteq \mathbb{Z}_p^{n+m}$ is a (p^n, p^m, p^n, p^{n-m}) difference set relative to $\Lambda = \{(0, y) \ : \ y \in \mathbb{Z}_p^m\}$.
- All component functions $x \mapsto \langle b, F(x)\rangle$ with $a \neq 0$ are bent.

Vectorial bent functions are vector spaces of bent functions!

Planar Functions: $n = m$

A vectorial bent function $F : \mathbb{Z}_p^n \to \mathbb{Z}_p^n$ is called planar:

$$\{(x, F(x)) \ : \ x \in \mathbb{Z}_p^n\}$$

is a relative

$$(p^n, p^n, p^n, 1) - \text{difference set in } \ \mathbb{Z}_p^{2n}.$$

Planar Functions: $n = m$

A vectorial bent function $F : \mathbb{Z}_p^n \to \mathbb{Z}_p^n$ is called planar:

$$\{(x, F(x)) \ : \ x \in \mathbb{Z}_p^n\}$$

is a relative

$$(p^n, p^n, p^n, 1) - \text{difference set in} \ \ \mathbb{Z}_p^{2n}.$$

Remark

1. *p must be odd.*
2. *Projective planes.*
3. *If F quadratic: Semifield planes.*
4. *Only one non-quadratic example known in $\mathbb{F}_{3^n}$ COULTER, MATTHEWS (1997): $x^{(3^a+1)/2}$ with $\gcd(a, n) = 1$, a odd.*

Examples and Bounds

$$F : \mathbb{Z}_p^n \to \mathbb{Z}_p^m \qquad \text{vectorial bent}$$

Theorem (Nyberg 1991)

*If $p = 2$ and n even and $m \leq \frac{n}{2}$, hence **no** planar functions.*

Example

1. $n = 2m$:
   $$F(x, y) = x \cdot \pi(y) + \sigma(y)$$
   for permutation π and any mapping σ on $\mathbb{F}_{p^m}$, where $x, y \in \mathbb{F}_{p^m}$.
2. p odd, $n = m$: Any semifield, for instance $F(x) = x^2$.

Motivation

- Geometers are interested in projective plane constructions.
- Connecting the geometers point of view with the "bent functions" point of view.
- Understand, how planar functions can be build from bent functions.
- $p = 2$: There are semifields, but no planar functions.

Projecting Vectorial Bent Functions

Observation

$F : \mathbb{Z}_p^n \to \mathbb{Z}_p^m$ is bent, then projection in the output yields vectorial bent functions $F' : \mathbb{Z}_p^n \to \mathbb{Z}_p^{m-1}$.

Question

Are there bent functions $\mathbb{Z}_p^n \to \mathbb{Z}_p^m$ which are not "projection" of a bent function $\mathbb{Z}_p^n \to \mathbb{Z}_p^{m+1}$? non-extandable

Projecting Vectorial Bent Functions

Observation

$F : \mathbb{Z}_p^n \to \mathbb{Z}_p^m$ is bent, then projection in the output yields vectorial bent functions $F' : \mathbb{Z}_p^n \to \mathbb{Z}_p^{m-1}$.

Question

Are there bent functions $\mathbb{Z}_p^n \to \mathbb{Z}_p^m$ which are not "projection" of a bent function $\mathbb{Z}_p^n \to \mathbb{Z}_p^{m+1}$? non-extandable

I know no example if $m = 1$:
Classical constructions (Maiorana-McFarland, partial spreads, o-polynomials) are vectorial, hence non-extandable should hold at most for non-classical bent functions.

Özbudak, P. (2014)

Theorem

There are vectorial bent functions not extendable by quadratic bent functions, for instance

$$F(x) = \begin{pmatrix} trace(x^2) \\ trace(\omega x^{10}) \\ trace(\omega x^4) \end{pmatrix}$$

with $x \in \mathbb{F}_{3^4}$ *as a mapping* $\mathbb{Z}_3^4 \to \mathbb{Z}_3^3$, ω *primitive in* $\mathbb{F}_{3^4}$.

The proof uses classification of $3^4 - 3^4$ bent functions.

Remark

Extendability by a non-quadratic function would be a big surprise.

Number of Quadratic Bent Functions

Theorem

- q *even,* $m = n/2$*:* $q^{m(m-1)} \prod_{k=1}^{m}(q^{2k-1} - 1)$ *alternating matrices*
- q *odd,* $m = (n+1)/2$*,* n *odd:* $q^{m(m-1)} \prod_{k=1}^{m}(q^{2k-1} - 1)$ *symmetric matrices*
- q *odd,* $m = n/2$*,* n *even:* $q^{m(m+1)} \prod_{k=1}^{m}(q^{2k-1} - 1)$ *symmetric matrices*

of full rank and size $n \times n$*.*

Number of Quadratic Bent Functions

Theorem

- q *even,* $m = n/2$*:* $q^{m(m-1)} \prod_{k=1}^{m} (q^{2k-1} - 1)$ *alternating matrices*
- q *odd,* $m = (n+1)/2$*,* n *odd:* $q^{m(m-1)} \prod_{k=1}^{m} (q^{2k-1} - 1)$ *symmetric matrices*
- q *odd,* $m = n/2$*,* n *even:* $q^{m(m+1)} \prod_{k=1}^{m} (q^{2k-1} - 1)$ *symmetric matrices*

of full rank and size $n \times n$*.*

Remark

The number of quadratic bent functions are known!

P., Schmidt, Zhou (2014)

Theorem

q even, $m = n/2$, $v = q^{m(m-1)} \prod_{k=1}^{m}(q^{2k-1} - 1)$, $\begin{bmatrix} m \\ i \end{bmatrix}$ number of i-dimensional subspaces in $\mathbb{F}_{q^2}^m$. Then there are

$$\frac{v}{q^m} \sum_{i=0}^{m} (-1)^i q^{i(i-1)} \begin{bmatrix} m \\ i \end{bmatrix} \prod_{k=1}^{m-i} (q^{2k-1} - 1)^2$$

quadratic bent functions $\mathbb{Z}_2^n \to \mathbb{Z}_2^2$.

Proof and Problems

- Alternating forms graph: Two alternating matrices $\mathbf{A}$ and $\mathbf{B}$ are adjacent if $\mathbf{A} - \mathbf{B}$ has full rank.
- Strongly regular graph.
- Number of triangles.

Remark

1. *Larger cliques correspond to RDS $\mathbb{Z}_2^n \to \mathbb{Z}_2^{>2}$.*
2. *Number of bent-negabent functions are known.*

p Even and Odd: Differences

$F : \mathbb{Z}_p^n \to \mathbb{Z}_p^m$ vectorial bent:

$p = 2$	p odd
n even	any n
$m \leq n/2$	any $m \leq n$

p Even and Odd: Differences

$F : \mathbb{Z}_p^n \to \mathbb{Z}_p^m$ vectorial bent:

$p = 2$	p odd
n even	any n
$m \leq n/2$	any $m \leq n$

However: There are $(2^n, 2^n, 2^n, 1)$ difference sets in $\Gamma = \mathbb{Z}_4^n$ relative to $\Lambda = 2\Gamma \cong \mathbb{Z}_2^n$, hence also in

$$\mathbb{Z}_4 \times \mathbb{Z}_2 \times \ldots \times \mathbb{Z}_2$$

with n odd using projection.

Example

The set

$$\{\begin{pmatrix}0\\0\end{pmatrix}, \begin{pmatrix}1\\0\end{pmatrix}, \begin{pmatrix}0\\1\end{pmatrix}, \begin{pmatrix}3\\3\end{pmatrix}\}$$

is a $(4, 4, 4, 1)$ difference set in $\mathbb{Z}_4^2$ relative to $2\mathbb{Z}_4^2$

Relative Difference Sets and Symmetric Matrices: p Odd

A vector space V, $\dim V = m$, of regular symmetric matrices in $\mathbb{F}_p^{(n,n)}$ gives rise to a relative difference set with parameters

$$(p^n, p^m, p^n, p^{n-m}).$$

in

$$\Gamma = \mathbb{Z}_p^n \times \mathbb{Z}_p^m \text{ relative to } \Lambda = \{0\} \times \mathbb{Z}_p^m.$$

The Construction

- Choose basis $\mathbf{A}_1, \ldots \mathbf{A}_m$ of V.
- Construct the quadratic bent functions $f_i(x) = x^T \mathbf{A}_i x$.
- $$F(x) = \begin{pmatrix} f_1(x) \\ \vdots \\ f_m(x) \end{pmatrix}$$
- RDS is graph $G_F = \{(x, F(x)) \, : \, x \in \mathbb{Z}_p^n\}$ of F.

Relative Difference Sets and Symmetric Matrices: $p = 2$

Theorem

A vector space V, $\dim V = m$, of regular symmetric matrices in $\mathbb{F}_2^{(n,n)}$ gives rise to a relative difference set with parameters

$$(2^n, 2^m, 2^n, 2^{n-m}).$$

The group is

$$\Gamma = \mathbb{Z}_4^k \times \mathbb{Z}_2^{n+m-2k}$$

relative to

$$\Lambda = 2\mathbb{Z}_4^k \times \mathbb{Z}_2^{m-k}$$

where $m - k$ is the dimension of subspace of alternating matrices in V.

The Construction: $p = 2$, $m = 1$

$$\Gamma = \mathbb{Z}_4 \times \mathbb{Z}_2 \times \ldots \times \mathbb{Z}_2$$

can be realized as $\{(x, y) : x \in \mathbb{Z}_2^n, y \in \mathbb{Z}_2\}$ with

$$(x, y) + (x', y') = (x + x', y + y' + B(x, x'))$$

for some non-alternating bilinear form B.

The Construction: $p = 2$, $m = 1$

$$\Gamma = \mathbb{Z}_4 \times \mathbb{Z}_2 \times \ldots \times \mathbb{Z}_2$$

can be realized as $\{(x, y) : x \in \mathbb{Z}_2^n, y \in \mathbb{Z}_2\}$ with

$$(x, y) + (x', y') = (x + x', y + y' + B(x, x'))$$

for some non-alternating bilinear form B. A transversal of

$$\Lambda := 2\Gamma \quad \text{which has order } 2$$

is a function

$$f : \mathbb{Z}_2^n \to \mathbb{Z}_2$$

and can be also interpreted as

$$\widetilde{f} : \mathbb{Z}_2^{n-1} \to \mathbb{Z}_4.$$

The Construction: $p = 2$, $m = 1$

Theorem

$$G_f = \{(x, f(x)) : x \in \mathbb{Z}_2^n\}.$$

is a relative difference set with parameters $(2^n, 2, 2^n, 2^{n-1})$ *in* Γ *if and only if*

$$f(x + a) + f(x) + B(x, a)$$

is balanced for all $a \neq 0$.

The Construction: $p = 2$, $m = 1$

Theorem

$$G_f = \{(x, f(x)) : x \in \mathbb{Z}_2^n\}.$$

is a relative difference set with parameters $(2^n, 2, 2^n, 2^{n-1})$ *in* Γ *if and only if*

$$f(x + a) + f(x) + B(x, a)$$

is balanced for all $a \neq 0$.

Such an f gives rise to a $\mathbb{Z}_4$-bent function $\widetilde{f}$. If B were alternating, f gives rise to a bent function.

An Example

If $\mathbf{A}$ is symmetric and non-alternating, the diagonal gives rise to B and the non-diagonal gives rise to a quadratic function f:

Example

$$\mathbf{A} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$$

gives rise to

$$f\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = x_1 x_3$$

and

$$B(\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}, \begin{pmatrix} x_1' \\ x_2' \\ x_3' \end{pmatrix}) = x_1 x_1' + x_2 x_2'$$

.

The General Case

Theorem

- $f_i : \mathbb{Z}_2^n \to \mathbb{Z}_2$, $i = 1, \dots, m$, **not necessarily quadratic!**
- B_i, $i = 1, \dots, m$ *symmetric bilinear forms.*

Assume that

$$F(x) := \sum_i \lambda_i f_i(x)$$

satisfies

$$F(x+a) + F(x) + \sum_i \lambda_i B_i(x,a) \quad \textit{is balanced}$$

for all $\lambda_1, \dots, \lambda_m$*, then there is a difference set with parameters* $(2^n, 2^m, 2^n, 2^{n-m})$ *in* $\Gamma = \mathbb{Z}_4^s \times \mathbb{Z}_2^t$ *relative to* $\mathbb{Z}_2^m$ *(containing* 2Γ*). Conversely, such a relative difference set gives rise to functions* f_i *and* B_i*.*

Main Observations

- Difference sets in $\mathbb{Z}_4^s \times \mathbb{Z}_2^t$ are the same objects as vector spaces of bent and $\mathbb{Z}_4$ bent functions.
- No canonical way to represent $\Gamma = \mathbb{Z}_4^n$ relative to $\Lambda = 2\Gamma$. One has to use bilinear forms B_i.
- Possible realization of $\mathbb{Z}_4^n = \{(x, y) \,:\, x, y \in \mathbb{F}_{2^n}\}$ such that

$$(x, y) + (x', y') = (x + x', y + y' + x \cdot x').$$

Two special cases

Problem: Representation depends on B_i.

Two special cases

Problem: Representation depends on B_i.

- $m = 1$: $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ such that

$$f(x+a) + f(x) + \mathrm{trace}(ax)$$

  is balanced for all $a \neq 0$.

Two special cases

Problem: Representation depends on B_i.

- $m = 1$: $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ such that

  $$f(x+a) + f(x) + \mathrm{trace}(ax)$$

  is balanced for all $a \neq 0$.
- $m = n$: $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ such that

  $$F(x+a) + F(x) + a \cdot x$$

  is a permutation for all $a \neq 0$. planar. Zhou (2013)

Satz 4.14 *Sei G eine abelsche Gruppe der Ordnung 2^{2a+2}, die eine Untergruppe $E =< \alpha > \times H$ enthalte mit $|H| = 2^a$ und $max\{4, exp(H)\} = o(\alpha) = 2^e \leq 2^{a+2}$. Dann gibt es eine $(2^{2a+1}, 2, 2^{2a+1}, 2^{2a})$-Differenzmenge in G relativ zu $N =< \alpha^{2^{e-1}} >$.*

Beweis. Schreibe $H = \bigotimes_{j=1}^{t} < \beta_j >$ mit $o(\beta_j) = 2^{b_j}$ und $b_1 = max\{b_j : j = 1, 2, ..., t\}$ (beachte $b_1 = 1$ oder e). Wir setzen

$$D_{i_1,i_2,...,i_t} = \bigotimes_{j=1}^{t} < \beta_j \alpha^{i_j 2^{e-b_j}} > \cup\ \alpha^{2^{e-2}} \bigotimes_{j=1}^{t} < \beta_j \alpha^{i_j 2^{e-b_j}} >$$

und wählen $g_{i_1,i_2,...,i_t} \in G$ mit
(a) falls $b_1 = 1$ (und damit $e = 2$), so ist

$$\{g_{i_1,i_2,...,i_t} : i_k = 0, 1, ..., 2^{b_k} - 1 \text{ für } 1 \leq k \leq t\}$$

ein vollständiges System (verschiedener) Nebenklassenrepräsentanten von E in G und
(b) falls $b_1 = e \geq 2$, so ist

$$\{g_{i_1,i_2,...,i_t} : 0 \leq i_k \leq 2^{b_k} - 1 \text{ für } 2 \leq k \leq t,\ 0 \leq i_1 \leq 3\}$$

ein vollständiges System (verschiedener) Nebenklassenrepräsentanten von E in G und

$$g_{i_1,i_2,...,i_t} = \alpha^m g_{n,i_2,...,i_t},$$

wobei m und n durch $i_1 = 4m + n$ und $0 \leq n \leq 3$ bestimmt sind.
Dann ist

$$R = \bigcup_{i_1=0}^{2^{b_1}-1} \bigcup_{i_2=0}^{2^{b_2}-1} \cdots \bigcup_{i_t=0}^{2^{b_t}-1} D_{i_1,i_2,...,i_t} g_{i_1,i_2,...,i_t}$$

die gesuchte relative Differenzmenge, was man wie im Beweis von Satz 4.1 nachrechnet.

□

Es folgt eine weitere Variation der K-Matrix-Methode.

Satz 4.15 *Sei G eine abelsche Gruppe der Ordnung 2^{2a+2}, die eine Untergruppe $< \alpha > \times E$ enthalte mit $|H| = 2^{a+2}$ und $4 \leq exp(H) = o(\alpha) \leq 2^a$, und sei $N' =< \beta >$ eine beliebige zyklische Untergruppe der Ordnung 4 von H. Dann gibt es eine $(2^{2a+1}, 2, 2^{2a+1}, 2^{2a})$-Differenzmenge in G relativ zu $N =< \beta^2 >$.*

Beweis. Wir definieren eine Äquivalenzrelation auf G^* durch

$$\chi \sim \chi' \iff Kern\chi|_H = Kern\chi'|_H.$$

Seien $[\chi_1], [\chi_2], ..., [\chi_n]$ die Äquivalenzklassen mit $\chi_i \not\in N^\perp$. Wir schreiben $K_t = Kern\chi_t|_H$. Wie im Beweis von Satz 4.2 sehen wir, daß es für $t = 1, 2, ..., n$ Elemente $h_t \in H \setminus K_t$, $y_t, z_t \in G \setminus H$ gibt, so daß die durch $m_{ij}^{(t)} = y_t z_t^j h_t^{i-(4i+1)j}$ definierten $2^{s_t} \times 2^{s_t}$-Matrizen $M_t = (m_{ij}^{(t)})$ (dabei ist $2^{s_t} = 2^a/|K_t| = o(\chi_t|_H)/4$) die Bedingungen (2) und (3) aus dem Beweis von Satz 4.2 und außerdem folgende Bedingung erfüllen:
(1') Falls $\chi \in (K_t^\perp \cap N'^\perp) \setminus [\chi_0]$, wobei χ_0 der triviale Charakter von G ist, so ist die Summe der Werte von χ über jede Spalte von M_t gleich 0.
Ebenfalls wie im Beweis von Satz 4.2 überzeugt man sich davon, daß

$$R = \bigcup_{t=1}^{n} \bigcup_{i,j=0}^{2^{s_t}-1} m_{ij}^{(t)}(K_t \cup \beta K_t)$$

die gesuchte relative Differenzmenge ist.

□

Schließlich benötigen wir wie in Abschnitt 4.1 noch eine rekursive Konstruktion.

Satz 4.16 *Sei $G =< \alpha > \times B$ eine abelsche Gruppe der Ordnung 2^{2a+2}, wobei B eine Untergruppe H der Ordnung 2^a enthalte mit $4 \leq exp(H) < o(\alpha) \leq 2^{a+2}$, und sei $N' =< \beta >$ eine Untergruppe der Ordnung 4 von H, die in einem zyklischen direkten Faktor von H enthalten ist. Falls eine $(2^{2a-1}, 2, 2^{2a-1}, 2^{2a-2})$-Differenzmenge in $< \alpha^4 > \times B$ relativ zu $N =< \beta^2 >$ existiert, so gibt es auch eine $(2^{2a+1}, 2, 2^{2a+1}, 2^{2a})$-Differenzmenge in G relativ zu N.*

Beweis. Sei R_0 eine $(2^{2a-1}, 2, 2^{2a-1}, 2^{2a-2})$-Differenzmenge in $< \alpha^4 > \times B$ relativ zu N. Wir schreiben $o(\alpha) = 2^e$ und setzen

$$R_1 = \{\alpha^{2i}\gamma : 0 \leq i < 2^{e-2},\ \gamma \in B \text{ und } \alpha^{4i}\gamma \in R_0\}.$$

Sei $H = \bigotimes_{j=1}^{t} < \beta_j >$ mit $o(\beta_j) = 2^{b_j}$ und $\beta = \beta_1^{2^{b_1-2}}$. Ferner sei $b_s = max\{b_j : j = 1, 2, ..., t\}$. Für $0 \leq i_j \leq 2^{b_j} - 1$, $j = 1, 2, ..., t$ und $(i_1, 2) = 1$ setzen wir

$$D_{i_1,i_2,...,i_t} = \left(\bigotimes_{j=1}^{t} < \beta_j \alpha^{i_j 2^{e-b_j}} >\right) \cup \left(\beta_1^{2^{b_1-2}} \bigotimes_{j=1}^{t} < \beta_j \alpha^{i_j 2^{e-b_j}} >\right)$$

Kantor's result

Quadratic planar functions describe commutative semifields. and vice versa. Many examples due to Kantor (2003):

KANTOR's result

Quadratic planar functions describe commutative semifields. and vice versa. Many examples due to KANTOR (2003):

Theorem

$\mathbb{K} = \mathbb{K}_0 \supset \mathbb{K}_1 \supset \cdots \supset \mathbb{K}_n$ of characteristic 2 with $[\mathbb{K} : \mathbb{K}_n]$ odd. Let tr_i be the relative trace from $\mathbb{K}$ to $\mathbb{K}_i$. Then, for all nonzero $\zeta_1, \ldots, \zeta_n \in \mathbb{K}$, the mapping $F : \mathbb{K} \to \mathbb{K}$ given by

$$F(x) = \left(x \sum_{i=1}^{n} \mathrm{tr}_i(\zeta_i x) \right)^2$$

is planar. Examples are inequivalent.

Power mappings $F(x) = \alpha \cdot x^d$

$F(x + a) - F(x) + a \cdot x$ permutation.

Power mappings $F(x) = \alpha \cdot x^d$

$$F(x+a) - F(x) + a \cdot x \quad \text{permutation.}$$

Known power mappings αx^d which are planar:

d	condition	
2^k	no	folklore
$2^k + 1$	$n = 2k$	Schmidt, Zhou
$4^k(4^k + 1)$	$n = 6k$	Scherr, Zieve

Power mappings $F(x) = \alpha \cdot x^d$

$$F(x+a) - F(x) + a \cdot x \quad \text{permutation.}$$

Known power mappings αx^d which are planar:

d	condition	
2^k	no	folklore
$2^k + 1$	$n = 2k$	SCHMIDT, ZHOU
$4^k(4^k + 1)$	$n = 6k$	SCHERR, ZIEVE

Theorem (MÜLLER, ZIEVE (2013))
Let d be a positive integer such that $d^4 \leq 2^m$ and let $c \in \mathbb{F}_{2^m}$ be nonzero. Then the function $x \mapsto \alpha x^d$ is planar on $\mathbb{F}_{2^m}$ if and only if d is a power of 2.

Some Questions

Question

1. *Is it possible to find* $F : \mathbb{Z}_2^n \to \mathbb{Z}_2^n$ *which is non-quadratic but planar?*
2. *Can we extend the* $\textsc{Kantor}$ *result to APN or AB functions?*
3. *Can we extend the* $\textsc{Kantor}$ *result to* p *odd?*

Knuth Operation

A semifield is an n-dimensional vector space of invertible $n \times n$ matrices. If

$$(a_{i,j}^{(k)}) \in \mathrm{GL}(n, \mathbb{Z}_p), k = 1, \ldots, n$$

is basis, then the 5 sets defined by the matrices

$$(a_{j,i}^{(k)}), (a_{i,k}^{(j)}), (a_{k,i}^{(j)}), (a_{k,j}^{(i)}), (a_{j,k}^{(i)})$$

also generate vector spaces of invertible matrices.

The Symmetric Case: p Odd

If $(a_{i,j}^{(k)})_{i,j}$ are symmetric, they describe quadratic forms $f_k : \mathbb{Z}_p^n \to \mathbb{Z}_p$. The mapping

$$F(x) = \begin{pmatrix} f_1(x) \\ \vdots \\ f_n(x) \end{pmatrix} \quad \text{is planar:}$$

It satisfies for p odd:

$$F(x+a) - F(x) - F(a) + F(0)$$

are (linear) permutations for all $a \neq 0$. F gives another vector space of invertible matrices which are not symmetric. Transposing them gives a third vector space.

Knuth and Planar Functions: p Odd

If F is quadratic and planar, then the component functions are quadratic and define symmetric matrices (symplectic spread).

Transposing the linear mappings

$$x \mapsto F(x+a) - F(x) - F(a) + F(0)$$

can be described in terms of F.

The three semifields in the Knuth orbit of a commutative semifield (symplectic spread) have a unified description.

The Symmetric Case: p Even

If $(a_{i,j}^{(k)})_{i,j}$ are symmetric, then

$$F(x+a) - F(x) + \begin{pmatrix} \sum_i a_{i,i}^{(1)} x_i \\ \vdots \\ \sum_i a_{i,i}^{(n)} x_i \end{pmatrix}$$

are (linear) permutations for all $a \neq 0$, where the components of F are given by the quadratic forms defined by the $(a_{i,j}^{(k)})_{i,j}$.

F gives another vector space of invertible matrices which are not symmetric. Transposing them gives a third vector space.

Knuth and Planar Functions: p Even

If F is quadratic and planar and $p = 2$, then the component functions are quadratic and define, together with the bilinear forms, symmetric matrices of full rank.

Transposing the linear mappings corresponding to F can be described in terms of F.

The three semifields in the Knuth orbit of a commutative semifield have a unified description very similar to the p odd case.

Conclusion

- Relative difference sets in elementary-abelian groups are equivalent to vector spaces of bent functions.
- Notion of non-extendable bent functions.
- Difference sets in $\Gamma = \mathbb{Z}_4^s \times \mathbb{Z}_2^t$ relative to 2Γ are equivalent to $\mathbb{Z}_4$ bent functions, depending on the representation of Γ.
- Explanation of KNUTH cube in terms of planar functions.