Construction and equivalence for generalized Boolean functions

Ayça Çeşmelioğlu

Özyeğin University

(joint work with Wilfried Meidl)

Generalized Boolean functions

Definition

A function $f : \mathbb{V}_n^{(p)} \to \mathbb{Z}_{p^k}$ is called a **generalized** p-ary **function**.
If $p = 2$, f is called a **generalized Boolean function**.

Any such function can be uniquely represented as

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

with $a_0, a_1, \cdots, a_{k-1} : \mathbb{V}_n^{(p)} \to \mathbb{F}_p$.

Generalized bent functions

Definition

The generalized Walsh transform of a function $f : \mathbb{V}_n^{(p)} \to \mathbb{Z}_{p^k}$ is defined as

$$\mathcal{H}_f(c, u) = \sum_{x \in \mathbb{V}_n^{(p)}} \zeta_{p^k}^{cf(x)} \zeta_p^{u.x}$$

for each nonzero $c \in \mathbb{Z}_{p^k}$ and $u \in \mathbb{V}_n^{(p)}$ where $\zeta_{p^k} = e^{2\pi i/p^k} and \zeta_p = e^{2\pi i/p}$.

Definition

f is a **generalized bent function** if

$$|\mathcal{H}_f(1, u)| = p^{n/2} \text{ for each } u \in \mathbb{V}_n^{(p)}.$$

Notation : $\mathcal{H}_f(1, u) = \mathcal{H}_f(u)$.

EA-equivalence in generalized Boolean functions

Definition

Two functions $f, g : \mathbb{V}_n^{(p)} \to \mathbb{Z}_{p^k}$ are **extended affine equivalent** if

$$g(x) = \phi_2(f(\phi_1(x) + a)) + \psi(x) + b$$

for a linear permutation ϕ_1 of $\mathbb{V}_n^{(p)}$, $\phi_2 \in Aut(\mathbb{Z}_{p^k})$, $\psi \in Hom(\mathbb{V}_n^{(p)}, \mathbb{Z}_{p^k})$, $a \in \mathbb{V}_n^{(p)}$, $b \in \mathbb{Z}_{p^k}$.
If $\psi = 0$, then f and g are **affine equivalent**, and **linear equivalent** if additionally $a = 0$, $b = 0$.

CCZ-equivalence in generalized Boolean functions

Definition

$f, g : \mathbb{F}_{p^n} \to \mathbb{Z}_{p^k}$ are **CCZ-equivalent** if

$$\{(x, g(x)) : x \in \mathbb{F}_{p^n}\} = \{\phi(A, z, c, \gamma)(x, f(x)) + \ (u, v) : x \in \mathbb{F}_{p^n}\}$$

where $\phi(A, z, c, \gamma) \in Aut(\mathbb{F}_{p^n} \times \mathbb{Z}_{p^k})$ and $(u, v) \in \mathbb{F}_{p^n} \times \mathbb{Z}_{p^k}$.

CCZ-equivalence in generalized Boolean functions

Definition

$f, g : \mathbb{F}_{p^n} \to \mathbb{Z}_{p^k}$ are **CCZ-equivalent** if

$$\{(x, g(x)) : x \in \mathbb{F}_{p^n}\} = \{\phi(A, z, c, \gamma)(x, f(x)) + \ (u, v) : x \in \mathbb{F}_{p^n}\}$$

where $\phi(A, z, c, \gamma) \in Aut(\mathbb{F}_{p^n} \times \mathbb{Z}_{p^k})$ and $(u, v) \in \mathbb{F}_{p^n} \times \mathbb{Z}_{p^k}$.

To understand the CCZ-equivalence for generalized p-ary functions, we need the description of $Aut(\mathbb{F}_{p^n} \times \mathbb{Z}_{p^k})$.

CCZ-equivalence in generalized Boolean functions

Theorem (Ç., Meidl, 2024)

The elements of $Aut(\mathbb{F}_{p^n} \times \mathbb{Z}_{p^k})$ *are* $\varphi(A, z, c, \gamma)$ *with*

$$\varphi(A, z, c, \gamma)(x, y) = (A(x) + \alpha_z(y), \beta_c(x) + \gamma y),$$

where A *is a linearized permutation of* $\mathbb{F}_{p^n}$, $\gamma \in \mathbb{Z}^*_{p^k}$, *and for* $z, c \in \mathbb{F}_{p^n}$, *the maps* $\alpha_z : \mathbb{Z}_{p^k} \to \mathbb{F}_{p^n}$ *and* $\beta_c : \mathbb{F}_{p^n} \to \mathbb{Z}_{p^k}$ *are given by*

$$\alpha_z(y) = z(y \bmod p),$$
$$\beta_c(x) = p^{k-1}\mathrm{Tr}_n(cx).$$

CCZ-equivalence in generalized Boolean functions

$f, g : \mathbb{F}_{p^n} \to \mathbb{Z}_{p^k}$ are **CCZ-equivalent** if

$$\{(x, g(x)) : x \in \mathbb{F}_{p^n}\} = \{ \underbrace{\phi(A, z, c, \gamma)(x, f(x))}_{(A(x)+\alpha_z(f(x)),\ \beta_c(x)+\gamma f(x))} + (u, v) : x \in \mathbb{F}_{p^n}\}$$

where

$$\phi(A, z, c, \gamma)(x, f(x)) = (A(x) + \overbrace{z(f(x)\ mod\ p)}^{\alpha_z(f(x))}, \overbrace{p^{k-1}\mathrm{Tr}_n(cx)}^{\beta_c(x)} + \gamma f(x))$$

with $(u, v) \in \mathbb{F}_{p^n} \times \mathbb{Z}_{p^k}$, A is a linearized permutation of $\mathbb{F}_{p^n}$, $\gamma \in \mathbb{Z}^*_{p^k}$, $z, c \in \mathbb{F}_{p^n}$.

CCZ-equivalence in generalized Boolean functions

$f, g : \mathbb{F}_{p^n} \to \mathbb{Z}_{p^k}$ are **CCZ-equivalent** if

$$\{(x, g(x)) : x \in \mathbb{F}_{p^n}\} = \{ \underbrace{\phi(A, z, c, \gamma)(x, f(x))}_{(A(x)+\alpha_z(f(x)),\ \beta_c(x)+\gamma f(x))} + (u, v) : x \in \mathbb{F}_{p^n}\}$$

where

$$\phi(A, z, c, \gamma)(x, f(x)) = (A(x) + \overbrace{z(f(x)\ mod\ p)}^{\alpha_z(f(x))}, \overbrace{p^{k-1}\mathrm{Tr}_n(cx)}^{\beta_c(x)} + \gamma f(x))$$

with $(u, v) \in \mathbb{F}_{p^n} \times \mathbb{Z}_{p^k}$, A is a linearized permutation of $\mathbb{F}_{p^n}$, $\gamma \in \mathbb{Z}_{p^k}^*$, $z, c \in \mathbb{F}_{p^n}$.

- $f(x) \mod p = a_0(x)$.

CCZ-equivalence in generalized Boolean functions

$f, g : \mathbb{F}_{p^n} \to \mathbb{Z}_{p^k}$ are **CCZ-equivalent** if

$$\{(x, g(x)) : x \in \mathbb{F}_{p^n}\} = \{ \underbrace{\phi(A, z, c, \gamma)(x, f(x))}_{(A(x)+\alpha_z(f(x)),\ \beta_c(x)+\gamma f(x))} + (u, v) : x \in \mathbb{F}_{p^n}\}$$

where

$$\phi(A, z, c, \gamma)(x, f(x)) = (A(x) + \overbrace{z(f(x)\ mod\ p)}^{\alpha_z(f(x))}, \overbrace{p^{k-1}\mathrm{Tr}_n(cx)}^{\beta_c(x)} + \gamma f(x))$$

with $(u, v) \in \mathbb{F}_{p^n} \times \mathbb{Z}_{p^k}$, A is a linearized permutation of $\mathbb{F}_{p^n}$, $\gamma \in \mathbb{Z}^*_{p^k}$, $z, c \in \mathbb{F}_{p^n}$.

- $f(x) \mod p = a_0(x)$.
- If $z = 0$, then f and g are **EA-equivalent**.

Equivalence of functions between elementary abelian groups

When we have functions between elementary abelian groups

- CCZ-equivalence is coarser than EA-equivalence.

Equivalence of functions between elementary abelian groups

When we have functions between elementary abelian groups

- CCZ-equivalence is coarser than EA-equivalence.
- Algebraic degree and the number of bent components are invariant under EA-equivalence but not under CCZ-equivalence.

Equivalence of functions between elementary abelian groups

When we have functions between elementary abelian groups

- CCZ-equivalence is coarser than EA-equivalence.
- Algebraic degree and the number of bent components are invariant under EA-equivalence but not under CCZ-equivalence.
- Two Boolean or p-ary functions are CCZ-equivalent iff they are EA-equivalent.

Equivalence of functions between elementary abelian groups

When we have functions between elementary abelian groups

- CCZ-equivalence is coarser than EA-equivalence.
- Algebraic degree and the number of bent components are invariant under EA-equivalence but not under CCZ-equivalence.
- Two Boolean or p-ary functions are CCZ-equivalent iff they are EA-equivalent.
- Two (vectorial) bent functions are CCZ-equivalent iff they are EA-equivalent.

Equivalence of functions between elementary abelian groups

When we have functions between elementary abelian groups

- CCZ-equivalence is coarser than EA-equivalence.
- Algebraic degree and the number of bent components are invariant under EA-equivalence but not under CCZ-equivalence.
- Two Boolean or p-ary functions are CCZ-equivalent iff they are EA-equivalent.
- Two (vectorial) bent functions are CCZ-equivalent iff they are EA-equivalent.

Budaghyan, Carlet (2010, 2011), Budaghyan, Helleseth (2011)

Results on CCZ and EA Equivalence of generalized Boolean functions

Which of the above results can be generalized to generalized Boolean or p-ary functions? Can we identify classes of generalized Boolean (p-ary) functions such that EA- and CCZ-equivalence do (not) coincide?

Results on CCZ and EA Equivalence of generalized Boolean functions

Which of the above results can be generalized to generalized Boolean or p-ary functions? Can we identify classes of generalized Boolean (p-ary) functions such that EA- and CCZ-equivalence do (not) coincide?

Theorem

Let p be an arbitrary prime. For functions from $\mathbb{V}_n^{(p)}$ to $\mathbb{Z}_{p^k}$ CCZ-equivalence is more general than EA-equivalence.

CCZ-equivalence is coarser than EA-equivalence

- EA-equivalence preserves the algebraic degree of the components (and their linear combinations) and the number of bent components. CCZ-equivalence does not necessarily preserve them.
- To show that CCZ is coarser than EA-equivalence, we need to find an example where CCZ changes the algebraic degree.
- The CCZ equivalence should transform the graph of f to the graph of another function. That gives a special condition on a_0.

Even with that condition if $a_0(x)$ is linear then CCZ drops down to EA. So we need a special a_0 which is not linear to show CCZ is coarser than EA.

Example

Consider the extension field $\mathbb{F}_{2^4} = \mathbb{F}_2(w)$ where w is the root of the polynomial $x^4 + x + 1 \in \mathbb{F}_2[x]$. Choose the automorphism $\phi(A, z, c, \gamma)$ with the linear permutation $A(x) = x^8 + wx^2$ of $\mathbb{F}_{2^4}$ and $z = w$. Then $\delta = A^{-1}(z) = w^{14}$. We select

$$\begin{aligned} a_0(x) = &(w^3+1)x^{12} + (w^2+w)x^{10} + (w^3+w^2+1)x^9 + (w^3+1)x^8 \\ &+ (w^3+w+1)x^6 + (w^2+w+1)x^5 + (w^3+w+1)x^4 \\ &+ (w^3+w^2+w)x^3 + (w^3+w^2+w)x^2 + (w^3+w^2+1)x. \end{aligned}$$

so that $\wp(x) = A(x) + za_0(x) = x^8 + wx^2 + wa_0(x)$ is a permutation of $\mathbb{F}_{2^4}$. For a_1 we take the quadratic bent function

$$a_1(x) = \mathrm{Tr}_4(w^4x^3).$$

Then $f : \mathbb{F}_{2^4} \to \mathbb{Z}_4$ equals $f(x) = a_0(x) + 2a_1(x)$ where each of a_0, a_1 and $a_0 + a_1$ is quadratic.

Example

Moreover, the Walsh spectrum of a_0 is $\{-8^1, 0^{12}, 8^3\}$, the Walsh spectrum of a_1 is $\{-4^6, 4^{10}\}$ (a_1 is a bent function), and $a_0 + a_1$ has Walsh spectrum $\{-8^1, 0^{12}, 8^3\}$.
We choose $c = 1$ and $\gamma = 1$ for simplicity and from f, with the automorphism $\varphi(A, z, c, \gamma)$, we obtain the CCZ-equivalent function

$$\begin{aligned} g(x) &= \gamma f(\wp^{-1}(x)) + 2\mathrm{Tr}_4(c\wp^{-1}(x)) \\ &= a_0(\wp^{-1}(x)) + 2(a_1(\wp^{-1}(x)) + \mathrm{Tr}_4(\wp^{-1}(x))) \\ &:= b_0(x) + 2b_1(x). \end{aligned}$$

Example continues

Then for the algebraic degrees and the Walsh spectra of $b_0(x) = a_0(\wp^{-1}(x))$, $b_1(x) = a_1(\wp^{-1}(x)) + \mathrm{Tr}_4(\wp^{-1}(x))$ and $b_0(x) + b_1(x)$ we have the following:

- b_0 has algebraic degree 2 and Walsh spectrum $\{-8^1, 0^{12}, 8^3\}$,
- b_1 has algebraic degree 3 and Walsh spectrum $\{-4^4, 0^6, 4^4, 8^2\}$,
- $b_0 + b_1$ has algebraic degree 3 and Walsh spectrum $\{-8^1, -4^2, 0^6, 4^6, 8\}$.

Example continues

Then for the algebraic degrees and the Walsh spectra of $b_0(x) = a_0(\wp^{-1}(x))$, $b_1(x) = a_1(\wp^{-1}(x)) + \mathrm{Tr}_4(\wp^{-1}(x))$ and $b_0(x) + b_1(x)$ we have the following:

- b_0 has algebraic degree 2 and Walsh spectrum $\{-8^1, 0^{12}, 8^3\}$,
- b_1 has algebraic degree 3 and Walsh spectrum $\{-4^4, 0^6, 4^4, 8^2\}$,
- $b_0 + b_1$ has algebraic degree 3 and Walsh spectrum $\{-8^1, -4^2, 0^6, 4^6, 8\}$.

The Walsh spectrum of all components of both f and g are $\{-8^2, -4^6, 0^{24}, 4^{10}, 8^6\}$ which is fixed under CCZ-equivalence. But the number of bent components changed!

CCZ-equivalence is coarser than EA-equivalence

We can extend the previous example to a function $f^{'} : \mathbb{F}_{2^4} \times G \to \mathbb{Z}_4$, where G is a finite abelian group, using a result from Pott, Zhou (2013). And by adding dummy components, we can extend the result to generalized Boolean functions.

Corollary

For the generalized Boolean functions $f : \mathbb{F}_{2^n} \to \mathbb{Z}_{2^k}$, CCZ-equivalence is coarser then EA-equivalence.

We obtain a similar result for $p = 3$ and we aim to extend the result to general p using the same method.

When does CCZ-equivalence drop down to EA?

Theorem

Let $f : \mathbb{V}_n^{(p)} \to \mathbb{Z}_{p^k}$ be given as $f(x) = \sum_{i=0}^{k-1} a_i(x)p^i$.
If

- *the Walsh transform of a_0 satisfies $\mathcal{W}_{a_0}(b) \neq 0$ for all $b \in \mathbb{V}_n^{(p)}$, or*
- *a_0 is linear,*

then CCZ-equivalence drops down to EA-equivalence.

Characterization of generalized bent functions

Recall f is a **generalized bent (gbent) function** if

$$|\mathcal{H}_f(1,u)| = p^{n/2} \text{ for each } u \in \mathbb{V}_n^{(p)}.$$

Theorem (Mesnager et al., 2018)

Let $p = 2$ **and** n **be even**, *or let* p **be odd and** n **be an arbitrary** *integer.*

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

$f : \mathbb{V}_n^{(p)} \to \mathbb{Z}_{p^k}$ *is a gbent function, if and only if for every* $C : \mathbb{V}_n^{(p)} \to \mathbb{F}_p$ *which is constant on the sets of the partition* $\mathcal{P}_a$*, the function* $a_{k-1}(x) + C(x)$ *is bent.*

Characterization of generalized bent functions

Recall f is a **generalized bent (gbent) function** if

$$|\mathcal{H}_f(1,u)| = p^{n/2} \text{ for each } u \in \mathbb{V}_n^{(p)}.$$

Theorem (Mesnager et al., 2018)

Let $p = 2$ **and** n **be even**, *or let* p **be odd and** n **be an arbitrary** *integer.*

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

$f : \mathbb{V}_n^{(p)} \to \mathbb{Z}_{p^k}$ *is a gbent function, if and only if for every* $C : \mathbb{V}_n^{(p)} \to \mathbb{F}_p$ *which is constant on the sets of the partition* $\mathcal{P}_a$*, the function* $a_{k-1}(x) + C(x)$ *is bent.*

The partition $\mathcal{P}_a = \{P_{\mathbf{c}} : \mathbf{c} = (c_0, \cdots, c_{k-2}) \in \mathbb{F}_p^{k-1}\}$ where $P_{\mathbf{c}} = \{x \in \mathbb{V}_n^{(p)} : a_0(x) = c_0, \cdots, a_{k-2}(x) = c_{k-2}\}$.

Characterization of generalized bent functions

Recall f is a **generalized bent (gbent) function** if

$$|\mathcal{H}_f(1,u)| = p^{n/2} \text{ for each } u \in \mathbb{V}_n^{(p)}.$$

Theorem (Mesnager et al., 2018)

Let $p = 2$ **and** n **be even**, *or let* p **be odd and** n **be an arbitrary** *integer.*

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

$f : \mathbb{V}_n^{(p)} \to \mathbb{Z}_{p^k}$ *is a gbent function, if and only if for every* $C : \mathbb{V}_n^{(p)} \to \mathbb{F}_p$ *which is constant on the sets of the partition* $\mathcal{P}_a$*, the function* $a_{k-1}(x) + C(x)$ *is bent.*

The partition $\mathcal{P}_a = \{P_{\mathbf{c}} : \mathbf{c} = (c_0, \cdots, c_{k-2}) \in \mathbb{F}_p^{k-1}\}$ where
$P_{\mathbf{c}} = \{x \in \mathbb{V}_n^{(p)} : a_0(x) = c_0, \cdots, a_{k-2}(x) = c_{k-2}\}$.
In this case, $a(x) := a_{k-1}(x)$ is called **admissible relative to the partition** $\mathcal{P}_a$, and the gbent function is denoted by $(a, \mathcal{P}_a)$.

Affine space of bent functions

The set

$$\{a_{k-1}(x) + C(x) : C : \mathbb{V}_n^{(p)} \to \mathbb{F}_p \quad \text{is constant on the sets of } \mathcal{P}_a\}$$

can also be described as the set

$$\mathcal{A} = \{a_{k-1}(x) + F(a_0(x), a_1(x), \ldots, a_{k-2}(x)) \,:\, F : \mathbb{F}_p^{k-1} \to \mathbb{F}_p\},$$

where $F(x_0, \cdots, x_{k-2})$ is arbitrary.
$\mathcal{A}$ is an affine space of bent functions of dimension $|\mathcal{P}_a|$.

Affine bent space constructions

Target: Given such affine spaces of bent functions, we construct another affine space of bent functions $(h, \mathcal{P}_h)$ using the known secondary constructions of bent functions to obtain generalized bent functions.

Direct-sum construction

Theorem

Let $f : \mathbb{V}_m^{(p)} \to \mathbb{Z}_{p^k}, f(x) = \sum_{i=0}^{k-1} a_i(x)p^i$ *and* $g : \mathbb{V}_n^{(p)} \to \mathbb{Z}_{p^k}, g(x) = \sum_{i=0}^{k-1} b_i(x)p^i$ *be gbent.*

Then the bent functions $a(x) := a_{k-1}(x)$ *and* $b(x) := b_{k-1}(x)$ *are admissible relative to the partitions*

$$\mathcal{P}_a = \{P_0, P_1, \cdots, P_{p^{k-1}-1}\} \text{ where } P_i = \{x \in \mathbb{V}_m^{(p)} : f(x) \equiv i \mod p^{k-1}\}$$

and

$$\mathcal{P}_b = \{Q_0, Q_1, \cdots, Q_{p^{k-1}-1}\} \text{ where } Q_i = \{x \in \mathbb{V}_n^{(p)} : g(x) \equiv i \mod p^{k-1}\}.$$

Direct-sum construction

Theorem

Let $f : \mathbb{V}_m^{(p)} \to \mathbb{Z}_{p^k}, f(x) = \sum_{i=0}^{k-1} a_i(x)p^i$ *and* $g : \mathbb{V}_n^{(p)} \to \mathbb{Z}_{p^k}, g(x) = \sum_{i=0}^{k-1} b_i(x)p^i$ *be gbent.*

Then the bent functions $a(x) := a_{k-1}(x)$ *and* $b(x) := b_{k-1}(x)$ *are admissible relative to the partitions*

$$\mathcal{P}_a = \{P_0, P_1, \cdots, P_{p^{k-1}-1}\} \text{ where } P_i = \{x \in \mathbb{V}_m^{(p)} : f(x) \equiv i \mod p^{k-1}\}$$

and

$$\mathcal{P}_b = \{Q_0, Q_1, \cdots, Q_{p^{k-1}-1}\} \text{ where } Q_i = \{x \in \mathbb{V}_n^{(p)} : g(x) \equiv i \mod p^{k-1}\}.$$

For the direct sum $f(x) + g(y)$, $\mathcal{H}_{f+g}(u, v) = \mathcal{H}_f(u)\mathcal{H}_g(v)$. *Therefore,* $f + g$ *is gbent.*

Direct-sum construction

Let $(h, \mathcal{P}_h)$ be the affine bent function space associated with $f(x) + g(y)$.
Question: What is the partition $\mathcal{P}_h$ of $\mathbb{V}_m^{(p)} \times \mathbb{V}_n^{(p)}$ relative to which h is admissible?
And what is the corresponding function h?

Direct-sum construction

Theorem

The function $h : \mathbb{V}_m^{(p)} \times \mathbb{V}_n^{(p)} \to \mathbb{F}_p$ *given by*

$$h(x,y) = r \text{ if } (f(x)+g(y)) \bmod p^k \in \{rp^{k-1}, rp^{k-1}+1, \ldots, (r+1)p^{k-1}-1\}$$

is bent and admissible to the partition $\mathcal{P}_h = \{R_1, \ldots, R_{p^{k-1}-1}\}$ *of* $\mathbb{V}_m^{(p)} \times \mathbb{V}_n^{(p)}$*, where for* $0 \leq j \leq p^{k-1} - 1$*,*

$$R_j = \bigcup_{i=0}^{p^{k-1}-1} P_i \times Q_{j-i} \quad \text{(indices are determined modulo } p^{k-1}\text{)}.$$

A representation of $(h, \mathcal{P}_h)$ *is the direct sum* $H(x,y) = f(x) + g(y) = \sum_{i=0}^{k-1} h_i(x,y)p^i$*, for which* $h_{k-1} = h$*.*

Direct-sum construction

In general, $h(x, y) \neq a(x) + b(y)$, and $\{R_0, R_1, \cdots, R_{p^{k-1}-1}\}$ is not a partition for $a(x) + b(y)$.

References

A. Pott and Y. Zhou, CCZ and EA equivalence between mappings over finite Abelian groups, *Des. Codes Cryptogr.*, **66** (2013), 99–109.

A. Çeşmelioğlu, W. Meidl, Equivalence for generalized Boolean functions. Adv. Math. Commun., (2024), 18(6), 1590–1604.

L. Budaghyan, C. Carlet, CCZ-equivalence of single and multi output Boolean functions. Finite fields: theory and applications, 43-54, Contemp. Math., 518, Amer. Math. Soc., Providence, RI, 2010.

L. Budaghyan, C. Carlet, CCZ-equivalence of bent vectorial functions and related constructions. Des. Codes Cryptogr. 59 (2011), 69–87.

L. Budaghyan and T. Helleseth, Tor, On isotopisms of commutative presemifields and CCZ-equivalence of functions, *Internat. J. Found. Comput. Sci.*, **22** (2011), 1243–1258.

S. Mesnager, C. Tang, Y. Qi, L. Wang, B. Wu, K. Feng, Further results on generalized bent functions and their complete characterization. IEEE Trans. Inform. Theory 64 (2018), 5441–5452,