A new invariant for quadratic vectorial Boolean functions

Lukas Kölsch

University of South Florida

BFA 2024

Basics and Disclaimers

We consider functions $F : \mathbb{F}_p^n \to \mathbb{F}_p^n$.

Many results transfer to functions $F : \mathbb{F}_p^m \to \mathbb{F}_p^n$.

We only consider *DO* functions, i.e. functions F where the degree of every monomial is 2.

(With some extra care, all results hold for quadratic functions as well).

Why DO?

If F is DO, then

$$B_F(x, y) = F(x + y) - F(x) - F(y)$$

is bilinear.

We can thus define the algebra $A_F = (\mathbb{F}_p^n, +, *_F)$.

Here $+$ is the regular addition on $\mathbb{F}_p^n$ and

$$*_F := B_F(x, y) = F(x + y) - F(x) - F(y).$$

Since $*_F$ is bilinear, $*_F$ distributes over addition, so A_F is both commutative and distributive.

The algebra A_F

If F is a planar function then A_F has no zero divisors and is thus a semifield.

It turns out that several concepts for semifields still hold in the more general case for more arbitrary F.

Idea

Transfer ideas from semifield theory to gain knowledge on the function F from analysis of A_F.

Connection to rank metric codes

If $F\colon \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ is DO, then

$$R_y(x) := B_F(x,y) = F(x+y) - F(x) - F(y)$$

is linear over $\mathbb{F}_p$.

We can view $R_y(x)$ as a matrix over $\mathbb{F}_p$ and the multiset

$$\mathcal{C}_F = \{\{R_y : y \in \mathbb{F}_p^n\}\}$$

is a linear subspace of $M^{n\times n}(\mathbb{F}_p)$.

Idea

Transfer ideas from rank-metric code theory to gain knowledge on the function F from analysis of $\mathcal{C}_F$.

Equivalence of functions

Definition (EL-equivalence)

We say that two functions $F, G\colon \mathbb{F}_p^n \to \mathbb{F}_p^n$ are extended linear equivalent if there are bijective additive functions L, M and an additive function N on $\mathbb{F}_p^n$ such that $F = L \circ G \circ M + N$.

(For simplicity we only deal with EL equivalence here, EA equivalence can be done in the same way).

Determining if two functions are EL equivalent is hard. For small dimensions, invariants (e.g. via orthoderivatives) or code equivalence algorithms can be used.

For infinite families of functions, tools are much more limited. Special tools were developed using group theory for power functions (Yoshiara, Dempwolff) and biprojective functions (Gologlu, Koelsch).

Conceptual idea

The idea now is as follows:

1. Show that EL equivalent functions lead to equivalent algebras and equivalent rank-metric codes, and the other way round.

2. Use equivalence invariants on the algebras/codes as invariants for the functions.

3. Analyze if these invariants can be used efficiently to decide inequivalence of DO functions.

Transferring equivalence

Definition

We call two $\mathbb{F}_p$-algebras A, A' with the same dimension n and multiplications $*, *'$ isotopic if there exist three $\mathbb{F}_p$-linear bijective functions L, M, N such that

$$L(x * y) = M(x) *' N(y)$$

for all $x, y \in \mathbb{F}_{p^n}$. We call (L, M, N) an isotopism between A, A'.

Theorem

Let $F, G \colon \mathbb{F}_p^n \to \mathbb{F}_p^n$ be DO polynomials where $G = L \circ F \circ M^{-1}$ is equivalent to F. Then (L, M, M) is an isotopism between A_F and A_G. Conversely, if p is odd and (L, M, M) is an isotopism between A_F and A_G then $G = L \circ F \circ M^{-1}$.

Transferring equivalence

Theorem

Let $F, G \colon \mathbb{F}_p^n \to \mathbb{F}_p^n$ be DO polynomials. If A_F and A_G are isotopic via an isotopism (L, M, N) then $\mathcal{C}_G = L\mathcal{C}_F M^{-1}$. Conversely, if $\mathcal{C}_G = L\mathcal{C}_F M^{-1}$ then A_F and A_G are isotopic via an isotopism (L, M, N) for a suitable N.

These theorems connecting equivalence are straightforward generalizations of known results, e.g. by Coulter, Henderson; Marino, Polverino; and others.

A new/old invariant

Theorem

Let $F\colon \mathbb{F}_p^n \to \mathbb{F}_p^n$ be a DO polynomial with differential uniformity at most $p^{n/2}$. Further, assume that $\mathcal{C}_F$ contains at least one bijective mapping. Then the sets

$$\mathcal{N}_s(F) = \{X \in \mathsf{End}(\mathbb{F}_{p^n})\colon \mathcal{C}_F X \subseteq \mathcal{C}_F\},$$
$$\mathcal{N}_m(F) = \{Y \in \mathsf{End}(\mathbb{F}_{p^n})\colon Y\mathcal{C}_F \subseteq \mathcal{C}_F\}$$

are both fields.

(The conditions can be replaced with some other mild conditions.)

We call the sets $\mathcal{N}_s(F)$ and $\mathcal{N}_m(F)$ in the Theorem the **side** and **middle** nuclei of F.

Nuclei as invariants

Theorem

Let $F, G\colon \mathbb{F}_p^n \to \mathbb{F}_p^n$ be EA-equivalent DO polynomials via $G = L \circ F \circ M^{-1}$. Then $L\mathcal{N}_s(F)L^{-1} = \mathcal{N}_s(G)$ and $M\mathcal{N}_m(F)M^{-1} = \mathcal{N}_m(G)$.

So, for instance, the size of a nucleus is an invariant for the DO functions F, G.

This mirrors the use of nuclei as an invariant for semifields and rank-metric codes.

An example

Using the identification $\mathbb{F}_p^n \cong \mathbb{F}_{p^n}$, some of the most simple DO functions are $F\colon \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ defined by $F(x) = x^{p^k+1}$.

Proposition

Let $F\colon \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ defined by $F(x) = x^{p^k+1}$. If $2k \neq n$, then $\mathcal{N}_s(F)$ is the set of all maps $N(x) = ax$ with $a \in \mathbb{F}_{p^{\gcd(k,n)}}$ and $\mathcal{N}_m(F)$ is the set of all maps $N(x) = ax$ with $a \in \mathbb{F}_{p^{\gcd(2k,n)}}$. In particular, $\mathcal{N}_s(F) \cong \mathbb{F}_{p^{\gcd(k,n)}}$ and $\mathcal{N}_m(F) \cong \mathbb{F}_{p^{\gcd(2k,n)}}$.

If $2k = n$ then $\mathcal{N}_s(F)$ is the set of all maps $N(x) = ax + bx^{p^k}$ with $a + b \in \mathbb{F}_{p^k}$ and $\mathcal{N}_m(F)$ is the set of all maps $N(x) = ax + bx^{p^k}$ with $a, b \in \mathbb{F}_{p^n}$.

A concrete application: APN functions

Theorem

Let $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ be an APN function such that $F(Ax) = F(x)$ for all x and a linear mapping $A \neq I$. Then n is even, A has order 3 and $\mathcal{N}_m \cong \mathbb{F}_4$.

In particular, this implies that all so far known 3-to-1 APN functions have middle nucleus $\mathbb{F}_4$. This includes for instance

- Gold functions in even dimension
- $F(x) = x^3 + \mathrm{Tr}(x^9)$ in even dimension
- Zhou-Pott functions
- Gologlu-Kolsch functions.

On the other hand, it is easy to prove for other APN functions that the middle nucleus is just $\mathbb{F}_2$ (for instance Taniguchi functions, and others).

Easy inequivalence results

So with *very little work*, we get inequivalence results like

Theorem

A Taniguchi APN function is EA-inequivalent to any known 3*-to-*1 *function.*

Pros of this method:

- Theoretical, can deal with infinite families
- Very easy proofs

Cons:

-Imprecise (many inequivalent functions have the same nuclei)

Theorem (Dempwolff, 2014)

If F is APN then the side nucleus is isomorphic to $\mathbb{F}_2$ and the middle nucleus is isomorphic to $\mathbb{F}_2$ or $\mathbb{F}_4$.

Thank you for your attention!