Invariants for equivalence relations on APN functions

Nikolay S. Kaleyski

University of Bergen

Boolean Functions and their Applications (BFA) 2020

Vectorial Boolean Functions

- *Vectorial Boolean Function*, or (n, m)-function: $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$;
- substitution of sequences of n bits with sequences of m bits;
- core component of cryptographic algorithms;
- $n = m$;
- finite field interpretation: $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$;
- unique representation as a univariate polynomial

$$F(x) = \sum_{i=0}^{2^n-1} \alpha_i x^i, \alpha_i \in \mathbb{F}_{2^n};$$

- *algebraic degree* $\deg(F)$: maximum binary weight of exponent with non-zero coefficient in univariate representation;
- affine, quadratic, cubic functions: of algebraic degree 1, 2, 3, respectively.

Equivalence relations on vectorial Boolean functions

- There are $(2^n)^{2^n}$ functions over $\mathbb{F}_{2^n}$;
- classification is done up to an equivalence relation preserving the properties of interest;
- two important cryptographic properties of an (n, n)-function are its differential uniformity Δ_F and its nonlinearity $\mathcal{NL}(F)$;
- the *differential uniformity* of F is

$$\Delta_F = \max_{a \in \mathbb{F}_{2^n}^*, b \in \mathbb{F}_{2^n}} \#\{x \in \mathbb{F}_{2^n} : F(x) + F(a + x) = b\};$$

- Δ_F should be as low as possible to resist differential cryptanalysis;
- $\Delta_F \geq 2$ for any F, with optimal functions called *almost perfect nonlinear (APN)*;
- the *nonlinearity* $\mathcal{NL}(F)$ of F is the minimum Hamming distance between a component function $F_c(x) = \mathrm{Tr}(cF(x))$ of F, and an affine $(n, 1)$-function;
- nonlineaity should be high to resist linear attacks, and we have $\mathcal{NL}(F) \leq 2^{n-1} - 2^{(n-1)/2}$, with functions attaining this bound with equality called *almost bent (AB)*.

CCZ-equivalence

- We say that $F_1, F_2 : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ are *Carlet-Charpin-Zinoviev (CCZ)-equivalent* if
$$\mathcal{A}(\Gamma_{F_1}) = \Gamma_{F_2}$$
for an affine bijection $\mathcal{A} : \mathbb{F}_{2^n}^2 \to \mathbb{F}_{2^n}^2$, where $\Gamma_F = \{(x, F(x)) : x \in \mathbb{F}_{2^n}\}$ is the graph of F;
- CCZ-equivalence is the most general known equivalence relation that preserves differential uniformity and nonlinearity;
- APN and AB functions are typically classified up to CCZ-equivalence;
- CCZ-equivalence does not preserve e.g. algebraic degree or bijectivity, and so can be used constructively;
- the only known APN permutation for even n was found by investigating the CCZ-equivalence class of the Kim function[1];
- can be tested via CCZ-equivalence of given F and G computationally via linear codes $\mathcal{C}_F$ and $\mathcal{C}_G$ associated to F and G.

[1] K.A. Browning, J.F. Dillon, M.T. McQuistan, A.J. Wolfe. *An APN permutation in dimension six*. Finite Fields: theory and applications, 2010, 518, pp.33-42.

EA-equivalence

- We say that $F_1, F_2 : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ are *extended affine (EA)-equivalent* if

$$A_1 \circ F_1 \circ A_2 + A = F_2$$

  for $A_1, A_2, A : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ affine, with A_1, A_2 bijective;
- EA-equivalence implies CCZ-equivalence;
- EA-equivalence (and taking inverses) is strictly less general than CCZ-equivalence;
- the two equivalence relations coincide for certain important classes of functions, such as for quadratic APN functions;
- EA-equivalence is easier to apply constructively, but also leaves more properties invariant (e.g. algebraic degree), and hence allows less freedom;
- can be tested via via linear codes[2] or by guessing A_1[3].

[2] Y. Edel and A. Pott, *On the equivalence of nonlinear functions*. In: Enhancing cryptographic primitives with techniques from error correcting codes. Vol. 23. NATO Sci. Peace Secur. Ser. D Inf. Commun. Secur. Amsterdam: IOS, 2009, pp. 87-103.

[3] N. Kaleyski, *Deciding EA-equivalence via invariants*, to be presented at SETA-2020

Desirable properties for invariants

1. Simple (not requiring any complicated algorithms or libraries);
2. efficient (fast computation time);
3. useful (taking many different values).

The Walsh transform

- The *Walsh transform* of $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is $W_F : \mathbb{F}_{2^n}^2 \to \mathbb{Z}$ defined by

$$W_F(a, b) = \sum_{x \in \mathbb{F}_{2^n}} \chi(bF(x) + ax),$$

  where $\chi(x) = (-1)^{\mathrm{Tr}(x)}$ and $\mathrm{Tr}(x) = \sum_{i=0}^{n-1} x^{2^i}$ is the absolute trace of $\mathbb{F}_{2^n}$;
- various properties, e.g. differential uniformity and nonlinearity, can be characterized using the Walsh transform;
- the multiset

$$\mathcal{W}_F = \{|W_F(a, b)| : a, b \in \mathbb{F}_{2^n}\},$$

  called the *extended Walsh spectrum*, is a CCZ-invariant;
- computation only requires basic arithmetic and bitwise operations (truth table representation);

n	6	7	8	9	10
time	0.023	0.076	0.391	2.863	22.566

The Walsh transform (2)

- The Walsh transform is not very useful for deciding CCZ-equivalence;
- experimentally, the known APN classes fall into only two or three distinct classes based on their extended Walsh spectra.

n	all	classes
5[4]	3	2/1
6[4]	14	13/1
7[5]	490	489/1
8[5]	8181	7681 / 487 / 12
9[6]	11	10 / 1
10[6]	16	15 / 1
11[6]	13	12 / 1

[4] Y. Edel and A. Pott, *On the equivalence of nonlinear functions*. In: Enhancing cryptographic primitives with techniques from error correcting codes. Vol. 23. NATO Sci. Peace Secur. Ser. D Inf. Commun. Secur. Amsterdam: IOS, 2009, pp. 87-103.

[5] Y., Yu, M. Wang, and Y., Li. *A matrix approach for constructing quadratic APN functions*. Designs, codes and cryptography, 2014, 73(2), pp.587-600.

[6] Representatives from known infinite families

Invariants from associated designs [7]

- The set of all pairs $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ can be used as the set of points for two combinatorial designs: $dev(G_F)$, whose blocks are the sets

$$\{(x + a, F(x) + b) : x \in \mathbb{F}_{2^n}\}; a, b \in \mathbb{F}_{2^n};$$

  and $dev(D_F)$, whose blocks are the sets

$$\{(x + y + a, F(x) + F(y) + b) : x, y \in \mathbb{F}_{2^n}, x \neq y\}; a, b \in \mathbb{F}_{2^n};$$

- the rank of the incidence matrix of $dev(G_F)$, resp. $dev(D_F)$, is called the Γ-*rank*, resp. Δ-*rank* of F;
- the Γ- and Δ-rank are useful CCZ-invariants;
- their computations amounts to constructing a large matrix, and computing its rank.

n	time	all	Γ-values	Δ-values
6	2	14	9	3
7	15	490	14	6
8	138	8181	21	11
9	4229	11	10	8
10	899024	16	15	-

[7] Y. Edel and A. Pott. *A new almost perfect nonlinear function which is not quadratic*. Advances in Mathematics of Communications, 2009, 3(1), p.59.

Invariants from associated designs (2)

- The orders of the automorphism groups of $dev(G_F)$ and $dev(D_F)$ are also CCZ-invariant;
- computing these takes a significantly longer time (4 seconds for $n = 6$, 75 seconds for $n = 7$) than the Γ- and Δ-rank, and is only feasible for small dimensions;
- the multiplier group $\mathcal{M}(G_F)$ is the subgroup of the automorphism group of $dev(G_F)$ consisting of automorphisms of a special form;
- computing the order of $\mathcal{M}(G_F)$ is quite fast, and appears to be useful for discriminating between CCZ-classes;

n	all	$dev(G_F)$	$dev(D_F)$	$\mathcal{M}(G_F)$
5	3	2	3	2
6	14	8	6	7
7	490	5	6	5
8	8181	-	-	10
9	11	-	-	5
10	16	-	-	9

The distance invariant[8]

- A lower bound on the Hamming distance between a given APN F and any other APN function G is given in terms of a set Π_F;
- let

$$\Pi_F^c(b) = \{a \in \mathbb{F}_{2^n} : (\exists x \in \mathbb{F}_{2^n}) F(x) + F(a+x) + F(a+c) = b\}$$

  for any $b, c \in \mathbb{F}_{2^n}$;
- let Π_F be the multiset $\Pi_F = \{\#\Pi_F^c(b) : b, c \in \mathbb{F}_{2^n}\}$;
- then the distance between F and G is at least $\lceil \min \Pi_F / 3 \rceil + 1$;
- more importantly, the multiset Π_F is a CCZ-invariant for APN functions;
- the actual minimum distance is not a CCZ-invariant!

[8] L. Budaghyan, C. Carlet, T. Helleseth, N. Kaleyski. *On the distance between APN functions*. IEEE Transactions on Information Theory, 2020.

The distance invariant (2)

- computation requires only basic arithmetic operations, and can be efficiently implemented via a truth table
- for F quadratic, $\Pi_F^c(b)$ does not depend on c, so computation is even more efficient.

n	time Π_F^0	time Π_F	all	values
5	0.002	0.064	3	2
6	0.003	0.192	14	5
7	0.004	0.512	490	2
8	0.004	1.024	8181	6669
9	0.005	2.56	11	2
10	0.031	31.744	16	1
11	0.066	135.168	13	2

- all representatives from known infinite families (besides the inverse function) have the same value of Π_F!

An EA-invariant from sums of values[9]

- While studying an approach for reconstructing the EA-equivalence of two given functions, the following EA-invariant is introduced;
- let

$$\mathcal{T}_k(t) = \left\{ \{x_1, x_2, \dots, x_k\} \subseteq \mathbb{F}_{2^n} : \#\{x_1, x_2, \dots, x_k\} = k, \sum_{i=1}^{k} x_i = t \right\};$$

- consider the *multiset*

$$\Sigma_k^F(t) = \left\{ \sum_{i=1}^{k} F(x_i) : \{x_1, x_2, \dots, x_k\} \in \mathcal{T}_k(t) \right\};$$

- the multiplicities with which the elements of $\Sigma_k^F(t)$ occur is an EA-invariant for even values of k;
- if $A_1 \circ F \circ A_2 + A = G$, then the elements in $\Sigma_k^F(t)$ and in $\Sigma_k^G(t)$ occur with the same multiplicities, and x and $A_1(x)$ must have the same multiplicity for any $x \in \mathbb{F}_{2^n}$.

[9] N. Kaleyski. *Deciding EA-equivalence via invariants*, SETA-2020.

An EA-invariant from sums of values (2)

- The multiplicity of $s \in \mathbb{F}_{2^n}$ in $\Sigma_k^F(t)$ can be computed as

$$2^{-2n} \sum_{a \in \mathbb{F}_{2^n}} \chi(at) \sum_{b \in \mathbb{F}_{2^n}} \chi(bs) W_F^k(a,b);$$

- the complexity does not depend on k;
- computing the number of distinct combinations of multiplicities for small dimensions for e.g. $k = 4$ gives the following picture;

n	all	values
6	14	5
7	19	1
8	23	5

- upon closer examination, for APN functions, the multiplicities of $\Sigma_F^k(t)$ and the set Π_F^0 are exactly the same invariant;
- the partition of the functions from the switching classes looks very similar to the one for Π_F;
- in fact, the inverse function for odd dimensions has the same value of Π_F^0 as the remaining functions, and only Π_F^c with $c \neq 0$ can differentiate it.

An EA-invariant from sums of values (3)

- So $\Sigma_F^4(t)$ partitions the switching class representatives exactly as Π_F^0 does;
- this is no surprise: since $\Pi_F^0 = \{\#\{a \in \mathbb{F}_{2^n} : F(x) + F(a+x) + F(a) = b\} : b \in \mathbb{F}_{2^n}\}$, for an APN function F, this is the same as counting the number of pairs (a, x) for which $F(x) + F(a+x) + F(a) = b$;
- at the same time, $\Sigma_3^F(0)$ expresses the multiplicities in

$$\{F(x_1)+F(x_2)+F(x_1+x_2) : x_1, x_2\} = \{F(x)+F(a)+F(x+a) : x, a \in \mathbb{F}_{2^n}\};$$

- for $\Sigma_4^F(0)$, we are considering sums of the form

$$F(x_1) + F(x_2) + F(x_3) + F(x_1 + x_2 + x_3) = D_c F(x_1) + D_c F(x_3)$$

for $c = x_1 + x_2$, that is

$$D_c F(x_1 + x_3) + D_c F(0) = F(x_1 + x_2) + F(x_1 + x_3) + F(x_2 + x_3) + F(0)$$

for quadratic F;

- on the other hand, the multiplicities in $\Sigma_F^4(0)$ are an EA-invariant regardless of whether F is APN or not.

An EA-invariant using dimensions of suspaces[10]

- Let $\mathcal{S}(F) = \{b \in \mathbb{F}_{2^n} : (\exists a \in \mathbb{F}_{2^n}) W_F(a, b) = 0\}$;
- the elements of b represent the component functions of F that are not bent;
- let N_i^F denote the number of i-dimensional subspaces contained in $\mathcal{S}(F)$;
- then the numbers N_i for $i = 1, 2, 3, \dots n$ are an EA-invariant;
- the computation requires an exhaustive search over all subspaces in $\mathcal{S}(F)$, which can be fairly large, but does not require any operations beyond basic arithmetics and algebraic closure;
- for $n = 6$, $(N_i)_i$ takes 6 distinct values, so it appears to be somewhat more discriminating than Π_F^0.

[10] L. Budaghyan, M. Calderini, C. Carlet, R. Coulter, I. Villa. *Generalized Isotopic Shift Construction for APN Functions*. To appear in Designs, Codes and Cryptography.
F. Gologlu, J. Pavlu. *Search for APN permutations among known APN functions*. BFA-2019.

Thickness spectrum [11]

- The thickness spectrum of a function F is defined in terms of subspaces in the set of Walsh zeros

$$Z_F = \{(a,b) : a, b \in \mathbb{F}_{2^n} \mid W_F(a,b) = 0\} \cup \{(0,0)\};$$

- the *thickness* of a subspace $V \subseteq Z_F$ is the dimension of the projection of V on $\{(0,x) : x \in \mathbb{F}_{2^n}\}$;
- let Σ_F be the set of n-dimensional subspaces of Z_F, for F over $\mathbb{F}_{2^n}$;
- for every i, we record the number N_i of $V \in \Sigma_F$ such that $t(V) = i$;
- the list of N_i for all i, called the *thickness spectrum of F*, is then invariant under EA-equivalence;
- it can have distinct values for distinct EA-classes within the same CCZ-equivalence class;
- computation involves counting subspaces.

[11] A. Canteaut, L. Perrin. *On CCZ-equivalence, extended-affine equivalence, and function twisting*. Finite Fields and Their Applications, 2019, 56, pp.209-246.

Thank you!