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: \(F : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^m\);
- substitution of sequences of \(n\) bits with sequences of \(m\) bits;
- core component of cryptographic algorithms;
- \(n = m\);
- finite field interpretation: \(F : \mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^n}\);
- 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 \(\text{deg}(F)\): 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 \((2^n)^2\) 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 \(\Delta_F\) and its nonlinearity \(\mathcal{NL}(F)\);
- the differential uniformity of \(F\) is
  \[
  \Delta_F = \max_{a \in \mathbb{F}_{2^n}^*, b \in \mathbb{F}_{2^n}} \#\{x \in \mathbb{F}_{2^n} : F(x) + F(a + x) = b\};
  \]
  - \(\Delta_F\) 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 \(F_c(x) = \text{Tr}(cF(x))\) of \(F\), and an affine \((n, 1)\)-function;
- nonlinearity 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).
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 $C_F$ and $C_G$ associated to $F$ and $G$.

EA-equivalence

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

\[
A_1 \circ F_1 \circ A_2 + A = F_2
\]

for \( A_1, A_2, A : \mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^n} \) 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 \( A_1 \)\(^3\).

---


\(^3\) 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 $F : \mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^n}$ is $W_F : \mathbb{F}_{2^n}^2 \rightarrow \mathbb{Z}$ defined by

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

where $\chi(x) = (-1)^{\text{Tr}(x)}$ and $\text{Tr}(x) = \sum_{i=0}^{n-1} x^{2^i}$ 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);

<table>
<thead>
<tr>
<th>$n$</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>time</td>
<td>0.023</td>
<td>0.076</td>
<td>0.391</td>
<td>2.863</td>
<td>22.566</td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>$n$</th>
<th>all</th>
<th>classes</th>
</tr>
</thead>
<tbody>
<tr>
<td>$5^4$</td>
<td>3</td>
<td>2/1</td>
</tr>
<tr>
<td>$6^4$</td>
<td>14</td>
<td>13/1</td>
</tr>
<tr>
<td>$7^5$</td>
<td>490</td>
<td>489/1</td>
</tr>
<tr>
<td>$8^5$</td>
<td>8181</td>
<td>7681 / 487 / 12</td>
</tr>
<tr>
<td>$9^6$</td>
<td>11</td>
<td>10 / 1</td>
</tr>
<tr>
<td>$10^6$</td>
<td>16</td>
<td>15 / 1</td>
</tr>
<tr>
<td>$11^6$</td>
<td>13</td>
<td>12 / 1</td>
</tr>
</tbody>
</table>

---


6 Representatives from known infinite families
Invariants from associated designs

- 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: $\text{dev}(G_F)$, whose blocks are the sets

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

and $\text{dev}(D_F)$, 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 $\text{dev}(G_F)$, resp. $\text{dev}(D_F)$, is called the $\Gamma$-rank, resp. $\Delta$-rank of $F$;
- the $\Gamma$- and $\Delta$-rank are useful CCZ-invariants;
- their computations amounts to constructing a large matrix, and computing its rank.

<table>
<thead>
<tr>
<th>$n$</th>
<th>time</th>
<th>all</th>
<th>$\Gamma$-values</th>
<th>$\Delta$-values</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>2</td>
<td>14</td>
<td>9</td>
<td>3</td>
</tr>
<tr>
<td>7</td>
<td>15</td>
<td>490</td>
<td>14</td>
<td>6</td>
</tr>
<tr>
<td>8</td>
<td>138</td>
<td>8181</td>
<td>21</td>
<td>11</td>
</tr>
<tr>
<td>9</td>
<td>4229</td>
<td>11</td>
<td>10</td>
<td>8</td>
</tr>
<tr>
<td>10</td>
<td>899024</td>
<td>16</td>
<td>15</td>
<td>-</td>
</tr>
</tbody>
</table>

---

Invariants from associated designs (2)

- The orders of the automorphism groups of \( \text{dev}(G_F) \) and \( \text{dev}(D_F) \) are also CCZ-invariant;
- computing these takes a significantly longer time (4 seconds for \( n = 6 \), 75 seconds for \( n = 7 \)) than the \( \Gamma \)- and \( \Delta \)-rank, and is only feasible for small dimensions;
- the multiplier group \( \mathcal{M}(G_F) \) is the subgroup of the automorphism group of \( \text{dev}(G_F) \) 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;

\[
\begin{array}{|c|c|c|c|c|}
\hline
n & \text{all} & \text{dev}(G_F) & \text{dev}(D_F) & \mathcal{M}(G_F) \\
\hline
5 & 3 & 2 & 3 & 2 \\
6 & 14 & 8 & 6 & 7 \\
7 & 490 & 5 & 6 & 5 \\
8 & 8181 & - & - & 10 \\
9 & 11 & - & - & 5 \\
10 & 16 & - & - & 9 \\
\hline
\end{array}
\]
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 $\Pi_F$;

let

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

for any $b, c \in \mathbb{F}_{2^n}$;

let $\Pi_F$ be the multiset $\Pi_F = \{ \#\Pi^c_F(b) : b, c \in \mathbb{F}_{2^n} \}$;

then the distance between $F$ and $G$ is at least $\lceil \min \Pi_F / 3 \rceil + 1$;

more importantly, the multiset $\Pi_F$ is a CCZ-invariant for APN functions;

the actual minimum distance is not a CCZ-invariant!

---

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.

<table>
<thead>
<tr>
<th>$n$</th>
<th>time $\Pi_F^0$</th>
<th>time $\Pi_F$</th>
<th>all</th>
<th>values</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>0.002</td>
<td>0.064</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>6</td>
<td>0.003</td>
<td>0.192</td>
<td>14</td>
<td>5</td>
</tr>
<tr>
<td>7</td>
<td>0.004</td>
<td>0.512</td>
<td>490</td>
<td>2</td>
</tr>
<tr>
<td>8</td>
<td>0.004</td>
<td>1.024</td>
<td>8181</td>
<td>6669</td>
</tr>
<tr>
<td>9</td>
<td>0.005</td>
<td>2.56</td>
<td>11</td>
<td>2</td>
</tr>
<tr>
<td>10</td>
<td>0.031</td>
<td>31.744</td>
<td>16</td>
<td>1</td>
</tr>
<tr>
<td>11</td>
<td>0.066</td>
<td>135.168</td>
<td>13</td>
<td>2</td>
</tr>
</tbody>
</table>

all representatives from known infinite families (besides the inverse function) have the same value of $\Pi_F$!
An EA-invariant from sums of values

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

let
\[ T_k(t) = \left\{ \{x_1, x_2, \ldots, x_k\} \subseteq \mathbb{F}_2^n : \#\{x_1, x_2, \ldots, x_k\} = k, \sum_{i=1}^{k} x_i = t \right\}; \]

consider the multiset
\[ \Sigma^F_k(t) = \left\{ \sum_{i=1}^{k} F(x_i) : \{x_1, x_2, \ldots, x_k\} \in T_k(t) \right\}; \]

the multiplicities with which the elements of \( \Sigma^F_k(t) \) occur is an EA-invariant for even values of \( k \);

if \( A_1 \circ F \circ A_2 + A = G \), then the elements in \( \Sigma^F_k(t) \) and in \( \Sigma^G_k(t) \) occur with the same multiplicities, and \( x \) and \( A_1(x) \) must have the same multiplicity for any \( x \in \mathbb{F}_2^n \).

\[ ^9 \text{N. Kaleyski. } Deciding \ EA\text{-equivalence via invariants}, \ SETA-2020. \]
An EA-invariant from sums of values (2)

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

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

- 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;

<table>
<thead>
<tr>
<th>$n$</th>
<th>all values</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>14</td>
</tr>
<tr>
<td>7</td>
<td>19</td>
</tr>
<tr>
<td>8</td>
<td>23</td>
</tr>
</tbody>
</table>

- upon closer examination, for APN functions, the multiplicities of $\Sigma^k_F(t)$ and the set $\Pi^0_F$ are exactly the same invariant;

- the partition of the functions from the switching classes looks very similar to the one for $\Pi_F$;

- in fact, the inverse function for odd dimensions has the same value of $\Pi^0_F$ as the remaining functions, and only $\Pi^c_F$ 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 $\Pi_F^0$ 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, $\Sigma_F^3(0)$ 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 $\Sigma_F^4(0)$, 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 \( S(F) = \{ b \in \mathbb{F}_{2^n} : (\exists a \in \mathbb{F}_{2^n}) W_F(a, b) = 0 \}; \)
- 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 \( S(F) \);
- then the numbers \( N_i \) for \( i = 1, 2, 3, \ldots n \) are an EA-invariant;
- the computation requires an exhaustive search over all subspaces in \( S(F) \), 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 \( \Pi^0_F \).

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 $\Sigma_F$ 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.

---

Thank you!