On the Generalized Linear Equivalence of Functions over Finite Fields

Luca Breveglieri, Alessandra Cherubini, and Marco Macchetti

Politecnico di Milano, Milan, Italy
brevegli@elet.polimi.it
aleche@mate.polimi.it
macchett@elet.polimi.it

Abstract. In this paper we introduce the concept of generalized linear equivalence between functions defined over finite fields; this can be seen as an extension of the classical criterion of linear equivalence, and it is obtained by means of a particular geometric representation of the functions. After giving the basic definitions, we prove that the known equivalence relations can be seen as particular cases of the proposed generalized relationship and that there exist functions that are generally linearly equivalent but are not such in the classical theory. We also prove that the distributions of values in the Difference Distribution Table (DDT) and in the Linear Approximation Table (LAT) are invariants of the new transformation; this gives us the possibility to find some Almost Perfect Nonlinear (APN) functions that are not linearly equivalent (in the classical sense) to power functions, and to treat them accordingly to the new formulation of the equivalence criterion. This answers a question posed in [8].
Keywords: Boolean functions, linear equivalence, differential cryptanalysis, linear cryptanalysis, APN functions, S-boxes.

1 Introduction

The design criteria for symmetric key algorithms can be traced back to the work of Shannon [18], where the concepts of *confusion* and *diffusion* are formalized. Today, a significant number of block ciphers are built by alternating nonlinear substitution layers with linear diffusion layers, in the so called Substitution-Permutation Networks (SPNs). It has been proved that the usage of sufficiently strong substitution functions, or S-boxes, leads to construction of strong block ciphers, see for instance the Wide-Trail design technique [6]. The strength of each S-box is often measured by means of the resistance to differential [4] and linear [14],[3] cryptanalysis.

For a given function $f : F_{p^m} \rightarrow F_{p^n}$ with p prime and $m, n \geq 1$ we can build the DDT by computing the number $\delta_f(a, b)$ of solutions x of the equation

$$f(x + a) - f(x) = b \qquad a \in F_{p^m}, b \in F_{p^n} \tag{1}$$

The lower the value of the maximum entry in the table, $\Delta_f = \max_{a \neq 0, b}(\delta_f(a, b))$, the more robust function f is versus differential cryptanalysis.

In a similar way, we can construct the LAT of f by counting the number $\lambda_f(a,b)$ of solutions x of the equation

$$a \bullet x = b \bullet f(x) \qquad a \in {F_p}^m, b \in {F_p}^n \tag{2}$$

where the inner product is indicated with $\bullet$ and gives a value in F_p. The robustness to linear cryptanalysis is measured with the maximum value $\Lambda_f = \max_{a,b\neq 0}(||\lambda_f(a,b) - p^{m-1}||)$. Good S-boxes have both small Λ_f and Δ_f values, and usually have a complex algebraic expression; most of the results focus on the case $p = 2$ which is of interest for practical applications.

Two functions are said to be equivalent if they differ by a group operation on the input or output variables; Lorens [12] and Harrison [10],[11] have considered the special case of invertible n-bit vectorial Boolean functions and have derived the exact number of equivalence classes (along with asymptotic estimates) for $n \leq 5$ when different transformations such as complementation, permutation, linear and affine transformations are applied on the input and output bits. Similar results can be found in [1],[13] regarding the case of Boolean functions with 5 and 6 input bits and an asymptotic estimate for the number of equivalence classes of Boolean functions under the transformation $g(x) = f(Ax + b) + L(x)$ (where L is a linear transformation) can be found in [7]. We can say that, in the most general case of classical linear equivalence, two functions $f, g : {F_p}^m \to {F_p}^n$ are linearly equivalent if there are two non-singular matrices A, B and a matrix C over F_p such that

$$g(x) = Bf(Ax) + Cx \tag{3}$$

The fact that two functions belong to the same equivalence class is rather important from a cryptanalytic point of view; it is well known that the distributions of values in the DDT and LAT as defined by (1) and (2) are invariant under the transformation (3). It is also true that if f is invertible, then $g(x) = f^{-1}(x)$ has the same cryptographic robustness of f [15],[2]. This has motivated the fact that the inverse of a function is also quoted as being *equivalent* to it [8]; while this is understandable from the point of view of cryptography[1], there is not formal consistency in the theory, because clearly the operation of inversion is very different from the transformation in (3).

To fill this gap, in Sect. 2 we propose a re-definition of the criterion of linear equivalence that permits us to treat the classical case of linear equivalence and the inversion operation with a unified approach. The criterion of generalized linear equivalence can be applied to functions over finite fields, provided that they are represented geometrically by set of vectors in an appropriate linear space S. The set of vectors representing function f is denoted with $\mathcal{F}$ and called the implicit embedding of f (in the space S); the implicit embedding contains the information of the truth-table of the function.

Two functions f and g are said to be *generally linearly equivalent* if $\mathcal{G}$ can be obtained from $\mathcal{F}$ with an invertible linear transformation T that acts on the

[1] A significant example is that of power functions over F_{p^n}, as it happens that the inverse of a power monomial is again a power monomial, generally belonging to a different cyclotomic coset.

space S, i.e. $\mathcal{G} = T(\mathcal{F})$. We show that there exist couples of functions that are generally linearly equivalent but are not correlated in the classical theory of equivalence; thus the proposed criterion is in fact an *extension* of the classical concept of equivalence.

In Sect. 3 we prove that the cryptographic robustness of a function versus differential and linear cryptanalysis is invariant under the transformations considered in the framework of generalized linear equivalence, completing the proof for the classical case.

In Sect. 4 we apply the criterion to power functions; we give an example of an APN function that is not classically linearly equivalent to any power monomial, but is easily obtainable using the generalized equivalence criterion. This answers a question posed in [8].

Sect. 5 concludes the paper.

2 Extension of the Linear Equivalence Relation

2.1 A Geometric Representation

Let us consider a completely specified function $f : {F_p}^m \to {F_p}^n$, with no restrictions on the values of m, n. There are different possible representations for the *object* f; we are particularly interested in the truth table of f, that lists the output values of f associated with the corresponding (actually, all the possible) input values. If we view the truth table as a matrix, there are p^m rows, $m + n$ columns, and each entry belongs to the field F_p. The ordering of the rows is not important, in the sense that two truth tables that contain the same rows in different order specify the same function and thus can be considered as the same truth table.

We can build a geometric representation of the function in the following way. Let S be a linear space of dimension $k = m + n$, the elements (or vectors) of which are defined over the finite field $F_{p^{m+n}}$. Such vectors can thus be conceived both as elements of the extension field $F_{p^{m+n}}$ and as vectors of the space S, each vector consisting of $m + n$ components over the basic field F_p. Denote by $+$ and $\cdot$ (or nothing) the addition and multiplication of elements in $F_{p^{m+n}}$; by extension $+$ denotes vector addition in S, and $\cdot$ (or nothing) denotes scalar-vector multiplication in S. Consider the set $\mathcal{F}$ of p^m vectors in this space formed by the rows of the truth-table of f, i.e. the concatenation of the input vectors with the corresponding output vectors of f. Formally,

$$\mathcal{F} = \{(x|f(x)), x \in {F_p}^m, f(x) \in {F_p}^n\} \tag{4}$$

where with $|$ we indicate the simple concatenation of two vectors with components over F_p. Each vector of the set represents one complete row of the truth table and thus the same information is contained in both representations; since the vectors are not ordered, we can see that different orderings of the rows of the truth table, as we would write it down on a piece of paper, actually identify the same set of vectors, i.e. the same geometric entity. Two different functions have different information in the truth table and therefore they are represented with different set of vectors. We conclude that each function f can be unambiguously represented with a particular set of vectors $\mathcal{F}$, which we call its *implicit embedding* (in the linear space S).

A natural question is when a given set of vectors actually represents a function. The following three conditions must be satisfied:

1. The set must have cardinality p^m for some positive m. In fact, we consider completely specified functions, and the number of rows in the truth table must be p^m if the function has m input variables (belonging to F_p).
2. The dimension of the vectors must be $m+n$ for some positive n, i.e. the function must have at least one output variable.
3. If we consider the first m components of all the vectors, we must find all possible configurations once and only once. This is because there cannot be a missing configuration (there would be a missing row in the truth table, but the function must be completely specified) and there cannot be multiple instances of the same configuration (there would be some missing configurations because the cardinality of the set is p^m).

We can see that there are sets of vectors which do not represent functions; thus the representation defines a relation from the set of all functions $f : {F_p}^m \rightarrow {F_p}^n$ to the set of all the sets of vectors in the space ${F_p}^{m+n}$ that is one-to-one but not onto.

2.2 Linear Transformations over S

We have seen that all the information contained in the function specification (truth table) is contained also in its geometric counterpart; the *shape* of the set of vectors is thus a unique property of the represented function. If we apply a linear transformation of coordinates to the space that is invertible, the information contained in the set of vectors is not changed; instead, we change the way we are looking at every geometric object (curves, hyperplanes, etc...) that is contained in the linear space S, including the function represented as a set of vectors.

Every invertible linear transformation over the whole space is governed by a non-singular $(m+n) \times (m+n)$ matrix T over F_p. The non-singularity of the matrix assures that we do not loose information while transforming the coordinates, and also that the transformation has always an inverse.

Each vector of the implicit embedding of f is transformed into a new one, but the essential shape of the configuration is invariant (we shall study the cryptographic invariants of f in Sect. 3). Thus if one vector set is obtained from another one by a change of basis governed by matrix T, then the two corresponding functions are said to be *generally linearly equivalent*.

Definition 1. *Two functions $f, g : {F_p}^m \rightarrow {F_p}^n$ are called generally linearly equivalent*[2] *if and only if the implicit embedding $\mathcal{G}$ of g can be obtained from the*

[2] We observe that the concept of generalized affine equivalence could be defined along the same line, to remove the artificial restriction that if two S-boxes are equivalent and one maps 0 to 0, the other must also.

implicit embedding $\mathcal{F}$ of f with

$$\mathcal{G} = T(\mathcal{F})$$

where T is an invertible linear transformation over the space ${F_p}^{m+n}$ corresponding to the non-singular matrix T.

We can treat the classical notion of linear equivalence as a particular case of the generalized linear equivalence. We first consider the case $m > n$. Then:

1. If matrix T of the change of basis is defined as

$$T = \left(\begin{array}{c|c} A & 0 \\ \hline 0 & B \end{array}\right)$$

   where A is a non-singular $m \times m$ matrix and B is a non-singular $n \times n$ matrix over F_p, then:
   - Matrix T is non-singular
   - If we examine the transformed set of vectors, we see that it still describes a function g which has the following relation with function f:

$$g(x) = Bf(A^{-1}x)$$

   The relation is easy to prove, once we remember that the first m components of the vectors in the implicit embeddings of f and g represent the input values, and the last n components represent the corresponding output values. Thus carrying out the matrix-vector multiplication at block level, we obtain $y = Ax$ and $g(y) = Bf(x)$ and substituting we have the above relation between f and g. Obviously, if $A = I_m$ (the $m \times m$ identity matrix over F_p) and $B = I_n$ (the $n \times n$ identity matrix over F_p) we obtain again f because the global transformation is the identity.
2. If matrix T of the change of basis is defined as

$$T = \left(\begin{array}{c|c} A & 0 \\ \hline C & B \end{array}\right)$$

   where A is a non-singular $m \times m$ matrix, B is an $n \times n$ non-singular matrix and $C \neq 0$ is an $n \times m$ matrix over F_p, then
   - Matrix T is non-singular.
   - If we examine the transformed set of vectors, we see that it still describes a function g which has the following relation with function f:

$$g(x) = Bf(A^{-1}x) + CA^{-1}x$$

   Thus we obtain all the functions that are linearly equivalent (in the classical sense) to f, according to (3).

3. If matrix T of the change of basis is defined as

$$T = \left(\begin{array}{c|c} A & D \\ \hline C & B \end{array}\right)$$

where $A \neq 0$ is an $m \times m$ matrix, B is an $n \times n$ matrix, C is an $n \times m$ matrix and $D \neq 0$ is an $m \times n$ matrix over F_p, then if matrix T is non-singular, we can examine the transformed set of vectors. Two possibilities arise:

   (a) It may happen that the transformed set does not describe a function anymore because the non-singularity of T does not always imply that condition 3 in Sect. 2.1 is satisfied.

   (b) The transformed set satisfies condition 3 in Sect. 2.1, and function g is generally equivalent to function f, although it is not obtainable within the classical theory. The link between g and f is non-trivial: the output vectors of g (the last n components of the transformed vectors) are obtained by mixing information contained in the input vectors of f by means of matrix C and information contained in the output vectors of f by means of matrix B. The difference from the previous case is that the same thing happens also to the input vectors of g by means of matrices A and D. As a result it is not possible to express the relation between f and g with a simple equation as before; nonetheless the two functions are generally linearly equivalent. The truth tables of the two functions can be expressed as:

$$f : x \rightarrow f(x)$$

$$g : Ax + Df(x) \rightarrow Cx + Bf(x)$$

   Note that the reason why the transformed vector set is still representing a function is simply that the function $h : x \rightarrow Ax+Df(x)$ is a permutation over ${F_p}^m$.

If $m = n$ holds, the above cases are still valid; however, if it happens that f is invertible, more cases can be considered. In particular:

4. If matrix T of the change of basis is defined as

$$T = \left(\begin{array}{c|c} 0 & D \\ \hline C & 0 \end{array}\right)$$

where C, D are non-singular $m \times m$ matrices over F_p, then:

   – Matrix T is non-singular
   – If we examine the transformed set of vectors, we see that it still describes a function g, and it holds that:

$$g(x) = Cf^{-1}(D^{-1}x)$$

This happens because the blocks C, D swap the input and the output parts of all the vectors belonging to the implicit embedding of f in the implicit embedding of g. Obviously, if $C = D = I_m$ we obtain the inverse of f. We have thus reduced the operation of inversion of a function to a linear transformation over the space where the implicit embedding of the function is defined. This is surely a convenient feature of the proposed formulation.

5. If matrix T of the change of basis is defined as

$$T = \left(\begin{array}{c|c} 0 & D \\ \hline C & B \end{array}\right)$$

where $B \neq 0$ is an $m \times m$ matrix and C, D are non-singular $m \times m$ matrices over F_p, then
   - Matrix T is non-singular
   - The relation between f and g is the following:

$$g(x) = Cf^{-1}(D^{-1}x) + BD^{-1}x$$

     i.e. we obtain all the functions that are linearly equivalent (in the classical sense) to the inverse of f.

Last, we consider the case $m < n$. The following considerations can be made:

- Cases 1,2,3 are still valid; however in the conditions for case 3 we should substitute $A \neq 0$ with $B \neq 0$.
- Case 4 is not applicable.
- Under some assumptions for matrix D and function f, case 5 can still be valid. However, we loose the relationship with the inverse transformation (which is not defined when the numbers of input and output variables are different); moreover this case in fact becomes a special instance of 3, thus it does not deserve a separate mention.

In all the remaining cases, either it can be proved that matrix T is singular, or the transformed set of vectors cannot represent a function, so we have no interest in examining them.

In the following, an example of a family of functions belonging to case 3 for $m > n$ is given.

Example 1. The family of functions $f : {F_p}^{2m} \to {F_p}^m$ with p prime and $m \geq 1$ is given, where the input vector x and $f(x)$ are defined as:

$$x = (x_1)|(x_2) \quad x \in {F_p}^{2m} \quad x_1, x_2 \in F_{p^m}$$

$$f(x) = f((x_1)|(x_2)) = x_1^{-1} + x_2^{-1}$$

where we indicate with | the simple concatenation of two vectors (actually, x_1 and x_2 represented as vectors over F_p are concatenated). When function f is transformed into function g using a suitable matrix T, we can simply write $g = T(f)$ as the same equation holds for the implicit embeddings of the two functions. The implicit embeddings of f and g can be *visually* represented, along with a block decomposition of T; we write explicitly:

$$g = T(f) = \left(\begin{array}{cc|c} I_m & 0 & 0 \\ 0 & 0 & I_m \\ \hline I_m & I_m & I_m \end{array}\right) \bullet \begin{pmatrix} x_1 \\ x_2 \\ x_1^{-1} + x_2^{-1} \end{pmatrix} = \begin{pmatrix} x_1 \\ x_1^{-1} + x_2^{-1} \\ x_1^{-1} + x_2^{-1} + x_1 + x_2 \end{pmatrix}$$

It can be observed that matrix T is non-singular and that the transformed set of vectors still represents a function, because the input part $(x_1)|(x_1^{-1} + x_2^{-1})$ is still a permutation over ${F_p}^{2m}$ when x_1, x_2 vary over F_{p^m} (i.e. all the possible input values for g are specified in the implicit embedding). We make here the underlying assumption that, with an abuse of notation, $0^{-1} = 0$.

By Def. 1 the two functions f, g are generally linearly equivalent, although there is no way to express the link using the classical theory of equivalence, since every function that is classically linearly equivalent to f is obtained with a matrix T characterized by a null upper-right block. The truth-table of g is written in compact form as

$$((x_1)|(x_1^{-1} + x_2^{-1})) \rightarrow (x_1^{-1} + x_2^{-1} + x_1 + x_2)$$

Any property that is invariant under the considered transformation is common between f and g. In the next Section we present a result on the invariance of cryptographic robustness.

3 Cryptographic Robustness of Generally Equivalent Functions

We start by recalling a fundamental result of the classical theory [15], [2]:

Theorem 1. *Given two functions f and g, if they are linearly equivalent i.e. if there exist two non-singular matrices A, B such that*

$$g(x) = Bf(Ax) \tag{5}$$

then the distributions of the values in DDTs and LATs of f and g are equal.

Corollary 1. *As a consequence of Theorem 1, we have that $\Delta_f = \Delta_g$ and $\Lambda_f = \Lambda_g$.*

It is also known that the same parameters are conserved when we consider the inverse of a function (the DDTs and LATs are merely transposed), or when we add a linear combination of the input variables of the function directly to its output variables [9].

Since we proved that these relations are particular occurrences of the generalized linear equivalence, it is therefore natural to ask whether the same parameters are also invariant in the general case. We answer with the following theorem.

Theorem 2. *Given two functions $f, g : {F_p}^m \rightarrow {F_p}^n$ and a non-singular $(m+n) \times (m+n)$ matrix T over F_p, if $g = T(f)$ then the distributions of values in the linear and differential tables of f and g are equal.*

*Proof. We first prove the relation regarding the DDTs of f and g.
A cell of the DDT of f located in the i-th row and j-th column contains the number of the input vector couples (x, y) such that $y = x+i$ and $f(y) = f(x)+j$, according to (1).
Thus, if we consider the geometric representation for function f we have that the cell contains the number of vector couples (w, z) belonging to the implicit embedding of f such that $w = z + k$ where $k = (i)|(j)$ (the concatenation of i and j); note that $i \in {F_p}^m$, $j \in {F_p}^n$ and $k \in {F_p}^{m+n}$.
These couples will be transformed by the change of basis into other couples (w', z') belonging to the implicit embedding of function g such that $w' = Tw$, $z' = Tz$ and $w' = z' + k'$ with $k' = Tk$.
Since matrix T is non-singular, there is a bijection between the values of k and those of k', i.e. the cells of the DDT of g are just a (linear) rearrangement of the cells of the DDT of f.*

*A similar reasoning can be applied to prove the relation between the LATs.
A cell of the LAT table of f located in the i-th row and j-th column contains the number of the input vectors x such that $i^+ \bullet x + j^+ \bullet f(x) = 0$, where we denote the inner-product with $\bullet$ and, for sake of clearness, the transposed of a vector with $^+$.
Thus, if we consider the geometric representation for function f we have that the cell contains the number of vectors w belonging to the implicit embedding of f such that $k^+ \bullet w = 0$ where $k = (i)|(j)$; note that $i \in {F_p}^m$, $j \in {F_p}^n$ and $k \in {F_p}^{m+n}$.
These vectors will be transformed by the change of basis into other vectors w' belonging to the implicit embedding of function g such that $w' = Tw$. We can rewrite the equation as:*

$$k^+ \bullet Tw = 0 \quad \Leftrightarrow \quad (T^+k)^+ \bullet w = 0 \quad \Leftrightarrow \quad (k')^+ \bullet w = 0$$

Since matrix T is non-singular, there is a bijection between the values of k and those of $k' = T^+k$, i.e. the cells of the LAT of g are just a (linear) rearrangement of the cells of the LAT of f. □

Corollary 2. *As a consequence of Theorem 2 we have that if f and g are generally linearly equivalent, then $\Delta_g = \Delta_f$ and $\Lambda_g = \Lambda_f$.*

We thus conclude that two generally linearly equivalent functions are characterized by the same cryptographic robustness; since the general case extends the classical relation, we can justify the common robustness of previously unrelated functions, such as f and g in Example 1.

It is a rather computationally difficult problem to decide whether two given functions are linearly equivalent: besides exhaustive search on the space of all possible matrices, it is possible to classify the functions basing on the distribution of values in the Walsh-Hadamard transform. Recently, Fuller and Millan

[9] have developed a classification method which exploits the concept of connectivity between two functions $f, g : {F_2}^m \to F_2$. They applied the method to the case $m = 8$ and to the Rijndael S-box, being able to prove that all the output variables of the only nonlinear step of the algorithm are linearly equivalent. Also, a description of optimized algorithms being able to find out whether two given invertible S-boxes are equivalent under a linear (or affine) transformation can be found in [5].

The result of Theorem 2 states that the whole distributions of values in the cryptographic tables are equal, not only the maximum values; such information could be used as a necessary condition for the generalized equivalence of two functions: if the two distributions differ, it can be immediately concluded that the two functions are not generally equivalent[3]. The check of this condition is not considered in [5]; we think that the check could speed up considerably the algorithms in most cases of negative answer. Obviously the condition is not sufficient and further techniques are needed to conclude that the two functions are generally (or classically) linearly equivalent.

It may be useful, at the end of this Section, to give also the geometric meaning of the parameters that measure cryptographic robustness.

In particular, the entries in the DDT of function f represent the number of vector couples belonging to the implicit embedding of f, that sum up to the same fixed vector, i.e. the (composed) difference vector. We can mentally view the process if we figure that the usual parallelogram rule is used to sum the vectors, as it would be done in standard Euclidean spaces; in practice, we are searching the vector couples that lead to the same path in the space S. This is evidently a measure of the redundancy of the information that characterizes the particular set of function vectors, i.e. the function itself.

The entries in the LAT, instead, can be seen as the number of vectors belonging to the implicit embedding of f that are orthogonal to a given fixed vector, since the inner product is the scalar product in S; the fixed vector is obtained by concatenating the masks that are classically applied to the function input and output values to compute the LAT. This can also be thought as a measure of the redundancy of the directions of the function vectors, and eventually of the function itself.

Finally, note that when the classical notion of linear equivalence is considered, we have linear rearrangements of the rows and the columns of the cryptographic tables; when generalized equivalence is applied, we have a linear rearrangement of the *cells* within the tables. There may exist couples of functions where the distributions of the values in the cryptographic tables are equal, but the actual arrangements of the cells cannot be linearly correlated. In these cases we can prove that the functions are not generally equivalent if we show that there are no possible linear rearrangements of the cells of one table that lead exactly to the other table.

[3] Since the classical equivalence is a special case of the generalized equivalence, the two functions are not equivalent also in the classical theory.

4 Application of the Criterion to Power Functions

The set of monomial power functions over F_{p^m} is interesting, since significant examples of functions with minimum possible Δ_f can be found in this class.

If $p = 2$ the minimum possible value for Δ_f when $f : \{0,1\}^m \to \{0,1\}^n$ is 2^{m-n}; functions reaching this limit are called Perfect Nonlinear (PN) [16] and exist only for m even and $m \geq 2n$. If we consider the important class of S-boxes, i.e. $f : \{0,1\}^m \to \{0,1\}^m$, then the minimum possible value for Δ_f is 2; functions reaching this limit are called Almost Perfect Nonlinear (APN) [17]. The only known examples of APN functions (up to classical linear equivalence) are power monomials; the list of known values for the exponent d such that $f(x) = x^d$ is APN can be found in [8]. Such functions find applications in symmetric key cryptography.

When $p > 2$ the minimum possible value for Δ_f is 1; functions reaching this limit are again called Perfect Nonlinear (PN). There are examples of PN and APN power functions over F_{p^m} and there is also one known example of a function that is not a power monomial but is PN over F_{3^m} for certain values of m [8].

Normally power monomials in even characteristic are classified into cyclotomic cosets, where a coset contains all the power monomials $\{x^d, x^{2d}, \ldots, x^{2^{m-1}d}\}$; the value d is called the coset leader and the power functions belonging to the same coset are classically linearly equivalent. Also, the inverse function $x^{d^{-1}}$ has the same cryptographic robustness of x^d, although it (in general) belongs to a different coset and is *not* linearly equivalent to x^d. Cosets, expanded with the usual classical equivalence criterion of Eq. 3, constitute the equivalence classes of power functions.

Using the criterion of generalized linear equivalence, different classical equivalence classes are merged into one: this is the case for instance of the classical equivalence classes of x^d and $x^{d^{-1}}$, since we have shown that in the new formalism the operation of inversion is nothing but a special case of linear transformation.

Moreover, we can show the existence of some functions that are not classically linearly equivalent to any power monomial, but still are APN.

Example 2. Consider the finite field F_{2^3}; the classification of all the possible exponents into cyclotomic cosets is given by:

$$C_0 = \{0\}$$
$$C_1 = \{1, 2, 4\}$$
$$C_3 = \{3, 6, 5\}$$

where the cosets C_i are numbered accordingly to the coset leader i. Coset C_0 contains only the constant function; coset C_1 contains the power monomials that are linear; coset C_3 contains non-linear APN power monomials. Since the inverse of x^6 is again x^6 and the inverse of x^3 is x^5 this coset is its own inverse[4].

[4] Note that this always happens to the coset that contains the inverse power function x^{-1} which in this case is actually x^6.

Coset C_3 can be expanded into a (classical) linear equivalence class of $f(x) = x^3$ by considering all the functions $g(x)$ such that

$$g(x) = T(f(x)) = \left(\begin{array}{c|c} A & 0 \\ \hline C & B \end{array}\right) \bullet \begin{pmatrix} x \\ x^3 \end{pmatrix}$$

Obviously, all these functions are APN and x^5, x^6 are some members of this class.

Now, consider the function $h(x)$ such that

$$h(x) = T'(f(x)) = \left(\begin{array}{c|c} I+S & I \\ \hline I & 0 \end{array}\right) \bullet \begin{pmatrix} x \\ x^3 \end{pmatrix}$$

where S is the matrix that gives the square of x (x^2 is a linear transformation in even characteristic, thus it can be represented by a matrix multiplication). The implicit embedding of h, and thus its truth-table, is described by:

$$x^3 + x^2 + x \quad \rightarrow \quad x$$

This implicit embedding still defines a function because $x^3 + x^2 + x$ is a permutation polynomial over F_{2^m} with m odd, see Corollary 2.10 of [19]. Since matrix T is non-singular, h is generally linearly equivalent to f and thus is APN. However, h does not belong to the classical equivalence class that extends C_3 because all the functions in this class are obtainable from $f(x)$ only using matrices T with a null upper-right block. We conclude that h belongs to a (classical) equivalence class that contains APN functions but is different from that of $f(x)$, which is the only one obtainable from power functions over F_{2^3}. Both these equivalence classes will be merged into one, when the general equivalence classes are considered; thus, this is another example of class merging.

Note that function h can actually be obtained from function f using classical *means*, i.e. by first transforming f into a classically linear equivalent function g and then inverting, since:

$$\left(\begin{array}{c|c} I+S & I \\ \hline I & 0 \end{array}\right) = \left(\begin{array}{c|c} 0 & I \\ \hline I & 0 \end{array}\right) \bullet \left(\begin{array}{c|c} I & 0 \\ \hline I+S & I \end{array}\right)$$

However, this does not lead to a function that is classically equivalent to f; while this may be difficult to prove classically, it becomes evident when general linear equivalence is introduced and one considers that matrix T' cannot belong to the family of matrices T indicated in the example.

5 Conclusions

In this paper we have presented the criterion of generalized linear equivalence. We have shown that the criterion extends the classical notion of linear equivalence; all the known cases of transformations that lead to invariance of the cryptographic robustness can be treated as special instances of the proposed relation. Also, it can be shown that there are functions that cannot be correlated using the classical theory but become equivalent under the proposed criterion. We have used general equivalence to show that there are APN functions that are not classically linearly equivalent to power monomials, and that these equivalence classes are merged under the extended criterion.

References

1. Berlekamp, E.R., Welch, L.R.: Weight Distributions of the Cosets of the (32,6) Reed-Muller Code. IEEE Transactions on Information Theory, 18(1):203–207, 1972.
2. Beth, T., Ding, C.: On Almost Perfect Nonlinear Permutations. Proceedings of EUROCRYPT '93, 65–76, 1994.
3. Biham, E.: On Matsui's Linear Cryptanalysis. Proceedings of EUROCRYPT '94, 341–355, 1994.
4. Biham, E., Shamir, A.: Differential Cryptanalysis of DES-like Cryptosystems. Journal of Cryptology, 4(1):3–72, 1991.
5. Biryukov, A., De Canniere, C., Braeken, A., Preneel, B.: A Toolbox for Cryptanalysis: Linear and Affine Equivalence Algorithms. Proceedings of EUROCRYPT 2003, 33–50, 2003.
6. Daemen, J., Rijmen, V.: The Design of Rijndael: AES-The Advanced Encryption Standard. Springer-Verlag, 2002.
7. Denev, J.D., Tonchev, V.D.: On the Number of Equivalence Classes of Boolean Functions under a Transformation Group. IEEE Transactions on Information Theory, 26(5):625–626, 1980.
8. Dobbertin, H., Mills, D., Muller, E.N., Pott, A., Willems, W.: APN functions in odd characteristic. Discrete Mathematics, 267(1-3):95–112, 2003.
9. Fuller, J., Millan, W.,: On linear Redundancy in the AES S-Box. Available online on http://eprint.iacr.org, 2002.
10. Harrison, M.A.: The Number of Classes of Invertible Boolean Functions. Journal of ACM, 10:25–28, 1963.
11. Harrison, M.A.: On Asymptotic Estimates in Switching and Automata Theory. Journal of ACM, 13(1):151–157, 1966.
12. Lorens, C.S.: Invertible Boolean Functions. IEEE Transactions on Electronic Computers, EC-13:529–541, 1964.
13. Maiorana, J.A.: A Classification of the Cosets of the Reed-Muller code r(1,6). Mathematics of Computation, 57(195):403–414, 1991.
14. Matsui, M.: Linear Cryptanalysis method for DES cipher. Proceedings of EUROCRYPT '93, 386–397, 1994.
15. Nyberg, K.: Differentially Uniform Mappings for Cryptography. Proceedings of EUROCRYPT '93, 55–64, 1994.
16. Nyberg, K.: Perfect Nonlinear S-Boxes. Proceedings of EUROCRYPT '91, 378–386, 1991.
17. Nyberg, K., Knudsen, L. R.: Provable security against differential cryptanalysis. Proceedings of CRYPTO '92, 566–574, 1992.
18. Shannon, C.E.: Communication Theory of Secrecy Systems. Bell System Technical Journal, 28:656–715, 1949.
19. Small, C.: Arithmetics of Finite Fields. Dekker, New York, 1991.