Antiderivative Functions over F 2 n

Valentin Suder

Antiderivative Functions over $\mathbb{F}_{2^n}$

Valentin Suder

University of Waterloo, Communications Security Lab
valentin@suder.xyz

Abstract. In this paper, we use a linear algebra point of view to describe the derivatives and higher order derivatives over $\mathbb{F}_{2^n}$. On one hand, this new approach enables us to prove several properties of these functions, as well as the functions that have these derivatives. On the other hand, we provide a method to construct all of the higher order derivatives in given directions. We also demonstrate some properties of the higher order derivatives and their decomposition as a sum of functions with 0-linear structure. Moreover, we introduce a criterion and an algorithm to realize *discrete antidifferentiation* of vectorial Boolean functions. This leads us to define a new equivalence of functions, that we call *differential equivalence*, which links functions that share the same derivatives in directions given by some subspace. Finally, we discuss the importance of finding 2-*to*-1 functions.

Keywords: Derivative functions, higher order derivative functions, antidifferentiation over $\mathbb{F}_{2^n}$, antiderivative functions, linear structure, quadratic APN functions.

1 Introduction

In symmetric cryptography, confusion in block and stream ciphers is usually performed by non-linear functions over finite fields called Substitution boxes (or S-boxes). In order to behave securely against most of the known attacks against cryptographic primitives using S-boxes, these functions must satisfy some security criteria. After the introduction of differential attacks [4], which is one of the most powerful known cryptanalysis, differential properties of functions over $\mathbb{F}_{2^n}$ have attracted a lot of attention from researchers not only in cryptography, but also in other related areas such as coding theory [6] or finite geometry [8]. Indeed, the resistance of a function against differential attacks is closely related to the study of its discrete derivatives, especially of the size of their image sets [13]. The most resistant functions against this attack are called *Almost Perfect Nonlinear* (APN), and all of their derivatives have an image set of the largest possible size (see Definition 1 below). In terms of coding theory, these APN functions correspond to some binary codes having a minimal distance 5 [6].

The generalization of differential cryptanalysis has brought new concepts and attacks linked to the derivative functions such as the impossible differential

attacks [3] or the boomerang attacks [14] among others. Conversely, tools related to derivatives and their properties (*e.g.* algebraic degree), like higher order derivatives [12], are frequently used in cryptanalysis, higher order differential attacks [11], cube attacks [7], zero-sum distinguishers [5]. Therefore, building functions that fulfill differential criteria has become an important issue in discrete mathematics.

There already exist some efficient techniques to find APN functions, as the so-called *switching method* [9]. Moreover, there are also techniques that aim at finding quadratic APN functions experimentally [15, 17]. However, up to our knowledge, the idea of constructing such functions from the derivatives themselves has never been explored before. Indeed, the goal of the switching method, when applied to APN functions, is somehow to transform some Boolean component functions of an APN function in such a way that all the derivatives of these Boolean functions keep their differential properties.

In this paper, we introduce a method able to recover a function from a set of derivatives in given directions, with possibly some differential properties. In other words, we realize *discrete antidifferentiation* of functions over $\mathbb{F}_{2^n}$.

In a recent work [16], Xiong *et al.* gave a criterion to decide whether or not a function is a derivative in a given direction, how many such derivatives exist, and what could be one of the function's antiderivative. However, their results were not pushed far enough, and many problems still arise. Indeed, in this paper, we revisit this work with another approach which allows us to not only discuss the higher order derivatives and their set, but also the functions that are canceled when differentiated in given directions and several other properties. In fact, higher order derivatives play an important role in the reconstruction of an antiderivative function. Most notably, we give a necessary and sufficient condition for some derivatives to be compatible, that is to be integrated in a function over $\mathbb{F}_{2^n}$. We also provide an efficient algorithm that realizes this antidifferentiation. Then we introduce a new function equivalence over $\mathbb{F}_{2^n}$, that we call *differential equivalence*, and which is distinct from CCZ-equivalence [6]. Finally, we discuss the eventuality to recover APN functions from their derivatives. In particular, we show that the two presented recently [15, 17] very similar techniques for finding quadratic APN functions, are quite surprisingly equivalent to the first natural application of antidifferentiation over $\mathbb{F}_{2^n}$, which consists in gathering affine derivatives.

This paper is thus organized as follows. After some basic definitions and notations (Section 2), in Section 3 we propose to see derivatives as linear applications described by matrices. By using techniques from linear algebra, we prove several properties concerning the set of derivatives and higher order derivatives. Then, in Section 4, we give the conditions that must be satisfied by the derivatives in order to be *integrated* into a *discrete antidifference function*, which we call *antiderivative*. We give also a simple algorithm that computes such *antiderivatives*. Finally, in Section 5, we talk about some applications and present the particular case of quadratic APN functions.

2 Definitions and notations

It is well known that any function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ has a unique univariate polynomial representation:

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

and its algebraic degree is given by $\deg(F) = \max\{wt(i) \mid f_i \neq 0\}$, where $wt(i)$ is the binary Hamming weight of the integer i. In the rest of this paper, we will use both 'function' and 'polynomial' indifferently to describe such an element F.

Definition 1. *The* discrete derivative *or simply* derivative *of a function* $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ *in a direction* $\alpha \in \mathbb{F}_{2^n}^*$ *is given by*

$$\begin{aligned} \Delta_\alpha F : \mathbb{F}_{2^n} &\to \mathbb{F}_{2^n} \\ x &\mapsto F(x) + F(x+\alpha) \end{aligned}$$

The differential uniformity *of* F*, denoted by* $\delta(F)$*, is defined as*

$$\delta(F) = \max_{\alpha \neq 0, \beta \in \mathbb{F}_{2^n}} \{x \mid \Delta_\alpha F(x) = \beta\} \geq 2.$$

The differential uniformity of a function measures its resistance to differential cryptanalysis. APN functions are the ones that have the lowest possible differential uniformity, *i.e.* 2. A derivative that has exactly two pre-images for each element in its image set is called a 2-*to*-1 function. It is clear that every derivative of an APN function is 2-*to*-1.

Definition 2. *Let* $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ *be a function and* $\alpha,\ c \in \mathbb{F}_{2^n}$*. We say that* α *is a* $c-$*linear structure of* F *if* $\Delta_\alpha F(x) = F(x) + F(x+\alpha) = c$*, for all* $x \in \mathbb{F}_{2^n}$*.*

Definition 3 ([12]). *Let* $L \subseteq \mathbb{F}_{2^n}$ *be the vector space over* $\mathbb{F}_2$ *spanned by the* $\mathbb{F}_2-$*linearly independent elements* $\alpha_1, \ldots, \alpha_m \in \mathbb{F}_{2^n}$ *and let* $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$*. Then,*

$$\Delta_L F(x) := \Delta_{\alpha_1,\ldots,\alpha_m} F(x) = \Delta_{\alpha_1}(\Delta_{\alpha_2,\ldots,\alpha_m} F(x)) = \sum_{c \in L} F(x+c).$$

Remark that there is a one-to-one correspondence between functions from $\mathbb{F}_{2^n}$ into $\mathbb{F}_{2^n}$ and the vector space $\mathbb{F}_{2^n}^{2^n}$.

Definition 4. *We denote by* φ *the bijective function that maps any function over* $\mathbb{F}_{2^n}$ *to the vector of its coefficients. More precisely, let* $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ *such that* $F(x) = \sum_{i=0}^{2^n-1} f_i x^i$*, then*

$$\varphi(F) = \begin{pmatrix} f_0 \\ f_1 \\ \vdots \\ f_{2^n-1} \end{pmatrix} \in \mathbb{F}_{2^n}^{2^n}.$$

For the sake of simplicity, we will denote $\varphi(F)$ *by* $\overrightarrow{F}$*.*

Thus, we have for all $x \in \mathbb{F}_{2^n}$, $F(x) = (0,\ x,\ x^2,\ x^3, \ldots,\ x^{2^n-1}) \cdot \overrightarrow{F}$.

Since our approach is mainly based on linear algebra, we also introduce the essential background on this topic. For more details, we invite the readers to refer to [10].

Definition 5. *The* image *and* kernel *of a linear application, given by its matrix M, between two vector spaces A and B, are denoted by* $\mathrm{Im}(M)$ *and by* $\ker(M)$ *respectively and are defined as follows:*

$$\mathrm{Im}(M) = \{y \in B \mid M \cdot x = y,\ \forall x \in A\} \quad \text{and} \quad \ker(M) = \{x \in A \mid M \cdot x = 0_B\},$$

where 0_B denotes the null vector of the vector space B. Both $\mathrm{Im}(M)$ *and* $\ker(M)$ *are vector spaces. The rank of a matrix M is defined as* $\mathrm{rank}(M) = \dim(\mathrm{Im}(M))$.

Definition 6. *Let M be a matrix defining an endomorphism of a vector space A and let A' be a subspace of A:*

1. *A' is said* invariant *under the action of M if $x \in A'$ implies $Mx \in A'$.*
2. *$A' + v = \{a + v \mid a \in A'\}$, with $v \in A$, is an* affine space *(or* coset*) of A.*

3 Derivatives and higher order derivatives

3.1 A matrix point of view

First of all, note that any positive integer a can be uniquely written as $a = \sum_{i \geq 0} a_i 2^i$ where a_i's lie in $\mathbb{F}_2$. We define the following relation:

Definition 7. *Let a and b be two positive integers. We will say that a is covered (resp. strictly covered) by b, and denote $a \preceq b$ (resp. $a \prec b$), if*

$$\{i \mid a_i \neq 0\} \subseteq \{j \mid b_j \neq 0\} \qquad (\textit{resp.} \quad \{i \mid a_i \neq 0\} \subset \{j \mid b_j \neq 0\}).$$

We give a more precise expression of the derivative of a function $F(x) = \sum_i f_i x^i \in \mathbb{F}_{2^n}[x]$, in a direction $\alpha \in \mathbb{F}_{2^n}^*$. For all $x \in \mathbb{F}_{2^n}$, we have:

$$\begin{aligned}
\Delta_\alpha F(x) = F(x) + F(x+\alpha) &= \sum_{i=0}^{2^n-1} f_i x^i + \sum_{i=0}^{2^n-1} f_i (x+\alpha)^i \\
&= \sum_{i=0}^{2^n-1} f_i x^i + \sum_{i=0}^{2^n-1} f_i \sum_{j,\, j \preceq i} x^j \alpha^{i-j} \\
&= \sum_{i=0}^{2^n-1} f_i x^i + \sum_{i=0}^{2^n-1} \sum_{j,\, j \preceq i} f_i x^j \alpha^{i-j} \\
&= \sum_{i=0}^{2^n-1} f_i x^i + \sum_{j=0}^{2^n-1} x^j \sum_{i,\, i \succeq j} f_i \alpha^{i-j} \\
&= \sum_{j=0}^{2^n-1} x^j \sum_{i,\, i \succ j} f_i \alpha^{i-j}.
\end{aligned}$$

We can thus write $\Delta_\alpha F(x) = \sum_{j=0}^{2^n-1} \delta_j(\alpha) x^j$, where $\delta_j(\alpha) = \sum_{i \succ j} f_i \alpha^{i-j}$. Notice that each coefficient of $\Delta_\alpha F(x) \in \mathbb{F}_{2^n}[x]$, $\delta_j(\alpha)$, can be written as a vectorial product between coefficients f_i's and α^{i-j} with $i \succ j$. Then, from Definition 4, we have

$$\overrightarrow{\Delta_\alpha F} = \begin{pmatrix} \delta_0(\alpha) \\ \delta_1(\alpha) \\ \vdots \\ \delta_{2^n-1}(\alpha) \end{pmatrix} = M(\alpha) \cdot \overrightarrow{F} = M(\alpha) \cdot \begin{pmatrix} f_0 \\ f_1 \\ \vdots \\ f_{2^n-1} \end{pmatrix},$$

where the matrix $M(\alpha)$ is defined as

$$M(\alpha) = \left(a_{i,j}\right)_{0 \le i,j \le 2^n-1}, \qquad a_{i,j} = \begin{cases} \alpha^{i-j} & \text{if } i \succ j \\ 0 & \text{otherwise} \end{cases}.$$

We can now define the differentiation function over $\mathbb{F}_{2^n}^{2^n}$, which gives the coefficients of the derivative of F in a direction $\alpha \in \mathbb{F}_{2^n}$:

$$\begin{aligned} \overrightarrow{\Delta_\alpha} : \mathbb{F}_{2^n}^{2^n} &\to \mathbb{F}_{2^n}^{2^n} \\ \overrightarrow{F} &\mapsto M(\alpha) \cdot \overrightarrow{F} \end{aligned}$$

We can adapt some well known facts about derivatives and higher order derivatives [12] to our matrix point of view:

Proposition 1. *Let $\alpha_1, \ldots, \alpha_m \in \mathbb{F}_{2^n}^*$, and $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be any function:*

1. $\overrightarrow{\Delta_{\alpha_1,\ldots,\alpha_m} F} = M(\alpha_1) \ldots M(\alpha_m) \cdot \overrightarrow{F}$;
2. *Matrices $M(\alpha_i)$'s commute, that is $\Delta_{\alpha_i,\alpha_j} F(x) = \Delta_{\alpha_j,\alpha_i} F(x)$, for any $1 \le i, j \le m$.*
3. *If α_m is $\mathbb{F}_2$-linearly dependent from $\alpha_1, \ldots, \alpha_{m-1}$, then $\Pi_{1 \le i \le m} M(\alpha_i) = 0$. In particular, $M(\alpha_i)$ is nilpotent of order 2, that is $M(\alpha_i)^2 = 0$ or $\Delta_{\alpha_i,\alpha_i} F(x) = 0$.*

Example 1. Let $n = 3$ and $\alpha \in \mathbb{F}_{2^n}^*$.

$$M(\alpha) = \begin{pmatrix} . & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 & \alpha^7 \\ . & . & . & \alpha^2 & . & \alpha^4 & . & \alpha^6 \\ . & . & . & \alpha & . & . & \alpha^4 & \alpha^5 \\ . & . & . & . & . & . & . & \alpha^4 \\ . & . & . & . & . & \alpha & \alpha^2 & \alpha^3 \\ . & . & . & . & . & . & . & \alpha^2 \\ . & . & . & . & . & . & . & \alpha \\ . & . & . & . & . & . & . & . \end{pmatrix}$$

Block construction of $M(\alpha)$. Let $\alpha \in \mathbb{F}_{2^n}^*$. It is possible to construct the matrix $M(\alpha)$ by following the recursive method:

$$M_1(\alpha) = \begin{pmatrix} 0 & \alpha \\ 0 & 0 \end{pmatrix}, \qquad M_i(\alpha) = \left(\begin{array}{c|c} M_{i-1}(\alpha) & \alpha^{2^{i-1}} \left(\mathrm{Id}_{i-1} + M_{i-1}(\alpha)\right) \\ \hline 0 & M_{i-1}(\alpha) \end{array}\right),$$

where Id_j is the identity matrix of size 2^j. Then $M(\alpha) := M_n(\alpha)$.

We can notice here that even thought the size of the matrix $M(\alpha)$ grows exponentially with n, it is very sparse. Furthermore, since it has a nice block structure as well as several symmetries, practical computation with matrices $M(\alpha)$, even if n is quite large, is possible.

3.2 Characterization of derivative functions

Theorem 1. *Let $\alpha \in \mathbb{F}_{2^n}^*$. The rank of the matrix $M(\alpha)$ is* $\mathrm{rank}(M(\alpha)) = 2^{n-1}$. *Moreover, the kernel of the linear application defined by $M(\alpha)$ has dimension 2^{n-1} and is generated by the matrix $K(\alpha)$:*

$$K(\alpha) = \begin{pmatrix} \mathrm{Id}_{n-1} \\ \hline \alpha^{2^{n-1}-1} M_{n-1}(\alpha) \end{pmatrix}.$$

Sketch of Proof. We can verify easily that $M(\alpha)K(\alpha) = 0$. It implies that the vector space generated by the matrix $K(\alpha)$ is included in $\ker(M(\alpha))$ and $\dim(\ker(M(\alpha))) \geq 2^{n-1}$. However, since $M(\alpha) = (m_{i,j})$ with $m_{i,j} = \alpha^{j-i}$ if $j \succ i$ and 0 otherwise, $M(\alpha)$ is an upper triangular matrix and $m_{i,i+1} = \alpha$ for every even integer i and 0 otherwise. That is, $M(\alpha)$ has exactly 2^{n-1} elements different from zero on the upper diagonal. Thus, $\mathrm{rank}(M(\alpha)) \geq 2^{n-1}$. We conclude by using the *rank-nullity*[1] theorem: $\dim(Ker(\alpha)) + \mathrm{rank}(M(\alpha)) = 2^n$. □

In order to ease the notations, we will use $Ker(\alpha)$ to denote the vector space $\ker(M(\alpha))$, its basis matrix is then $K(\alpha)$.

Corollary 1.

$$\mathrm{Im}(M(\alpha)) = Ker(\alpha).$$

Sketch of Proof. From Proposition 1 *(3.)*, we know that $\mathrm{Im}(M(\alpha)) \subset Ker(\alpha)$. We conclude with Theorem 1, since $\dim(\mathrm{Im}(M(\alpha))) = \dim(Ker(\alpha)) = 2^{n-1}$. □

This last corollary can be translated into the following:

Corollary 2. *Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ and $\alpha \in \mathbb{F}_{2^n}$. Then, it exists a function $G : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ such that $\Delta_\alpha G(x) = F(x)$* if and only if *$\alpha$ is a $0-$linear structure of F.*

Note that, this characterization of derivative functions was already given in another way in [16, Theorem 1]. Nevertheless, the structure of the matrix $K(\alpha)$, permits to find and compute them efficiently even if n is large.

Example 2. Let $n = 3$ and $\alpha \in \mathbb{F}_{2^n}$. The vector space $Ker(\alpha)$ is spanned by the columns of $K(\alpha)$:

$$K(\alpha)^\intercal = \begin{pmatrix} 1 & . & . & . & . & . & . \\ . & 1 & . & . & \alpha^8 & . & . \\ . & . & 1 & . & \alpha^9 & . & . \\ . & . & . & 1 & \alpha^{10} & \alpha^9 & \alpha^8 \end{pmatrix}$$

[1] See for instance [10, Section50].

3.3 Higher order derivatives

Before discussing the general case of higher order derivatives, we first start with second order derivatives. This helps to understand better the general result that follows.

Lemma 1. *Let $\alpha, \beta \in \mathbb{F}_{2^n}^*$ be distinct. Then,*

$$\mathrm{Im}\,(M(\alpha)M(\beta)) = Ker(\alpha) \cap Ker(\beta) \qquad \textit{and} \tag{1}$$
$$\ker\,(M(\alpha)M(\beta)) = Ker(\alpha) + Ker(\beta). \tag{2}$$

Proof. We have that

$$\mathrm{Im}(M(\alpha)M(\beta)) = \{M(\alpha) \cdot x \mid x \in \mathrm{Im}(M(\beta))\} = \mathrm{Im}(M(\alpha)_{|\mathrm{Im}(M(\beta))}).$$

Since $M(\alpha)$ and $M(\beta)$ commute, we have that $\mathrm{Im}(M(\beta))$ is invariant (see Definition 6 or [10, Section 39]) under the action of $M(\alpha)$. It means that we may ignore the fact that $M(\alpha)$ is defined outside $\mathrm{Im}(M(\beta))$ and may consider $M(\alpha)$ as a linear transformation of $\mathrm{Im}(\beta)$. Thus, from Corollary 1, we have that $\mathrm{Im}(M(\alpha)_{|\mathrm{Im}(M(\beta))}) = \ker(M(\alpha)_{|\mathrm{Im}(M(\beta))}) = Ker(\alpha) \cap \mathrm{Im}(M(\alpha)) = Ker(\alpha) \cap Ker(\beta)$.

We prove Eq. (2). We know from the rank-nullity theorem and Eq. (1) that

$$\dim(\ker(M(\alpha)M(\beta))) + \mathrm{rank}(M(\alpha)M(\beta)) = 2^n$$
$$\dim(\ker(M(\alpha)M(\beta))) + \dim(Ker(\alpha) \cap Ker(\beta)) = 2^n.$$

Moreover, $2^n = \dim(Ker(\alpha)) + \dim(Ker(\beta))$. In other words,

$$\begin{aligned}\dim(\ker(M(\alpha)M(\beta))) &= \dim(Ker(\alpha)) + \dim(Ker(\beta)) - \dim(Ker(\alpha) \cap Ker(\beta)) \\ &= \dim(Ker(\alpha) + Ker(\beta)).\end{aligned}$$

We conclude this proof by noticing the following natural inclusion:

$$Ker(\alpha) + Ker(\beta) \subseteq \ker(M(\alpha)M(\beta)).$$

□

We extend Lemma 1 to more than two distinct elements α, β in the next theorem.

Theorem 2. *Let $\alpha_1, \ldots, \alpha_m \in \mathbb{F}_{2^n}^*$ be $\mathbb{F}_2$-linearly. Then,*

1. *the set of all m-order derivatives with respect to $\{\alpha_i\}_{1 \le i \le m}$ is*

$$\mathrm{Im}(\overrightarrow{\Delta_{\alpha_1, \ldots, \alpha_m}}) = \mathrm{Im}(\prod_{1 \le i \le m} M(\alpha_i)) = \bigcap_{1 \le i \le m} Ker(\alpha_i). \tag{3}$$

Furthermore, $\dim\left(\bigcap_{1 \le i \le m} Ker(\alpha_i)\right) = 2^{n-m}$.

2. *the set of all functions such that their m-order derivative, with respect to $\{\alpha_i\}_{1\leq i\leq m}$, cancel is*

$$\ker(\overrightarrow{\Delta_{\alpha_1,\dots,\alpha_m}}) = \ker(\prod_{1\leq i\leq m} M(\alpha_i)) = \sum_{1\leq i\leq m} Ker(\alpha_i). \tag{4}$$

Furthermore, $\dim\left(\sum_{1\leq i\leq m} Ker(\alpha_i)\right) = 2^n - 2^{n-m}$.

Sketch of Proof.

1. Eq. (3) can be proven by induction on m with Eq. 1 as initialization and by noticing that matrices $M(\alpha_i)$ commute. We can prove the dimension by induction on m with the rank-nullity theorem and the fact that, for all distinct $1 \leq i, j \leq m$:

$$\dim(\ker(M(\alpha_i)M(\alpha_j))) = \dim(Ker(\alpha_j)) + \dim(Ker(\alpha_i) \cap \mathrm{Im}(M(\alpha_j))).$$

2. Let $\overrightarrow{v} = \sum_{i=1}^m \overrightarrow{v_i}$ with $\overrightarrow{v_i} \in Ker(\alpha_i)$, that is $\overrightarrow{v} \in \sum_{i=1}^m Ker(\alpha_i)$. Then, $(\prod_{i=1}^m M(\alpha_i)) \cdot \overrightarrow{v} = 0$, and thus $\sum_{i=1}^m Ker(\alpha_i) \subseteq \ker(\prod_{i=1}^m M(\alpha_i))$.
From Eq. (3), we know that

$$\dim(\ker(\prod_{i\leq i\leq m} M(\alpha_i))) = 2^n - \dim(\mathrm{Im}(\prod_{1\leq i\leq m} M(\alpha_i))) = 2^n - 2^{n-m}.$$

Now, we notice that with the vector spaces $Ker(\alpha_i)$, the intersection is distributive over the sum. Indeed, since $\mathrm{Im}(M(\alpha_i)) = Ker(\alpha_i)$, from Eq. (1) and the fact that $M(\alpha_i)$'s commute, we have naturally, for $\beta \in \mathbb{F}_{2^n}^*$,

$$M(\beta)\left(\sum_{1\leq i\leq m} M(\alpha_i)\right) = \sum_{1\leq i\leq m} (M(\alpha_i)M(\beta))$$

$$\Rightarrow \qquad Ker(\beta) \cap \left(\sum_{1\leq i\leq m} Ker(\alpha_i)\right) = \sum_{1\leq i\leq m} (Ker(\alpha_i) \cap Ker(\beta)).$$

Thus, we can apply the *inclusion-exclusion principle* (see [1, Chapter 4]) to these particular vector spaces. Hence we obtain that

$$\dim\left(\sum_{1\leq i\leq m} Ker(\alpha_i)\right) = \sum_{1\leq k\leq m} (-1)^{k+1}\binom{m}{k}2^{n-k}.$$

The proof is completed by showing that the last equality is equal to $2^n - 2^{n-m}$, with the help of an induction on m.

□

Theorem 2 brings necessary and sufficient conditions to formalize higher order derivatives as in Corollary 2 for order 1. Most notably, we can now extract the following results:

Corollary 3. *Let* $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$,

1. *if* $\Delta_{\alpha_1,\ldots,\alpha_m} F(x) = 0$ *then there are functions* $F_1, \ldots, F_m : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, *with* $\Delta_{\alpha_i} F_i(x) = 0$, *such that* $F(x) = F_1(x) + \cdots + F_m(x)$ *(the converse is obviously true).*
2. *if* F *possess some* $0-$*linear structure in* $\alpha_1, \ldots, \alpha_m$ $\mathbb{F}_2-$*linearly independent,* $m < n$, *that is* $\Delta_{\alpha_i} F(x) = 0$, $1 \leq i \leq m$, *then, there exists a function* $G : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ *such that* $\Delta_{\alpha_1,\ldots,\alpha_m} G(x) = F(x)$ *(the converse is obviously true).*

4 Antidifferentiation

In this section, we introduce necessary and sufficient conditions as well as an algorithm to recover the antiderivative functions. From the sections above, we can first deduce the following proposition.

Proposition 2. *Let* $F, G : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$. *They share the same derivatives in directions given by a subspace* V *of* $\mathbb{F}_{2^n}$ if and only if *every elements of* V *is a* $0-$*linear structure of* $F + G$.

Indeed, we have previously seen[2] that:

$$\Delta_v F(x) = \Delta_v G(x), \quad \forall v \in V \Leftrightarrow \overrightarrow{F} + \overrightarrow{G} \in \bigcap_{v \in V} Ker(v). \tag{5}$$

This results in a new function equivalence over $\mathbb{F}_{2^n}$:

Definition 8 (Differential equivalence). *Let* $F, G : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$. *The functions* F *and* G *are said* differentially equivalent *with respect to a subspace* $V \subseteq \mathbb{F}_{2^n}$, *denoted by* $F \sim_V G$, *if*

$$\Delta_v F(x) = \Delta_v G(x), \qquad \textit{for all } v \in V.$$

From Eq. (5), we have that the equivalence class, we call *differential coset*, of the function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ with respect to the subspace $V \subseteq \mathbb{F}_{2^n}$ is the affine space $\cap_{v \in V} Ker(v) + \overrightarrow{F}$. In other words, a function $G : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ shares the same derivatives as F in directions given by V if and only if it consists in the sum of some higher order derivative function over V (see Eq. (3)) and F itself: $F \sim_V G \Leftrightarrow \overrightarrow{G} \in \cap_{v \in V} Ker(v) + \overrightarrow{F}$.

Furthermore, we know that the (algebraic) degree of a function $h : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ such that $\overrightarrow{h} \in \cap_{v \in V} Ker(v)$ could not exceed $n - \dim(V)$. Indeed, we know that the algebraic degree of a function strictly decrease with its differentiation [12, Proposition 2]. Then, there is $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ such that $\Delta_V F(x) = h(x)$ and we have:

$$n \geq \deg(F) > \deg(\Delta_v F(x)) > \cdots > \deg(\Delta_V F(x)) \Rightarrow n - \dim(V) \geq \deg(h(x)).$$

[2] Remark that $Ker(\alpha) \cap Ker(\beta) \subset Ker(\alpha + \beta) \Leftarrow \Delta_{\alpha+\beta}(\Delta_{\alpha,\beta} F)(x) = 0$ from Eq. (1).

In other words, the lower the dimension of the subspace, the lower the algebraic degree of the functions we can add in order to stay in the same differential coset. It is also clear that, in general, the differential equivalence does not preserve differential uniformity and is thus distinct from CCZ-equivalence [6]. We can thus deduce the following proposition:

Proposition 3. *Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be a function and let $V \subset \mathbb{F}_{2^n}$. Then,*

- *if $\deg(F) \geq \dim(V)$, for all $G : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ such that $F \sim_V G$, we have $\deg(G) = \deg(F)$.*
- *if $\dim(V) \geq n - 1$, for all $G : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ such that $F \sim_V G$, we have $\delta(F) = \delta(G)$.*

We are now able to introduce the consistency theorem as well as an algorithm which computes the coefficients of antiderivative functions from consistent derivatives. By consistent, we mean derivatives that satisfy conditions in order to be *integrated* together, that is which are the derivative of a same function.

Theorem 3. *Let $\alpha_1, \ldots, \alpha_m \in \mathbb{F}_{2^n}^*$ be $\mathbb{F}_2-$linearly independent elements and let $f_1, \ldots, f_m : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be such that $\overrightarrow{f_i} \in Ker(\alpha_i)$, $1 \leq i \leq m$. Then, there is at least one function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ satisfying*

$$\Delta_{\alpha_i} F(x) = f_i(x), \quad \text{for all } 1 \leq i \leq m, \tag{6}$$

if and only if

$$\Delta_{\alpha_j} f_i(x) = \Delta_{\alpha_i} f_j(x), \quad \text{for all } 1 \leq i, j \leq m. \tag{7}$$

Proof. Assume $\Delta_{\alpha_i} F(x) = f_i(x)$, $1 \leq i \leq m$, then $\Delta_{\alpha_j} f_i(x) = \Delta_{\alpha_i, \alpha_j} F(x) = \Delta_{\alpha_i} f_j(x)$.

Reciprocally, for all i, since $\overrightarrow{f_i} \in Ker(\alpha_i)$, there is $F_i : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ such that $\Delta_{\alpha_i} F_i(x) = f_i(x)$. Thus, from Eq. (7) and Theorem 2: $\Delta_{\alpha_i, \alpha_j} F_j(x) = \Delta_{\alpha_j, \alpha_i} F_i(x) \Leftrightarrow \Delta_{\alpha_i, \alpha_j}(F_i + F_j)(x) = 0 \Leftrightarrow \overrightarrow{F_i + F_j} \in Ker(\alpha_i) + Ker(\alpha_j)$.

Hence, there are $\overrightarrow{G_i} \in Ker(\alpha_i)$ and $\overrightarrow{G_j} \in Ker(\alpha_j)$ such that $\overrightarrow{F_i + F_j} = \overrightarrow{G_i + G_j}$. Moreover, for all $1 \leq i \leq m$, we can choose G_i to be the same each time F_i is involved in a function. Thus, all the functions $F_i + G_i$, $1 \leq i \leq m$, are equal and we can so denote by $F = F_i + G_i$. Finally, we have $\Delta_{\alpha_i} F(x) = \Delta_{\alpha_i}(F_i + G_i)(x) = \Delta_{\alpha_i} F_i(x) = f_i$ for all $1 \leq i \leq m$. □

From Theorem 3, and due to the fact that both matrices $M(\alpha)$ and $K(\alpha)$, $\alpha \in \mathbb{F}_{2^n}^*$ are easy to implement efficiently, we end up with Algorithm 1. Notice that this algorithm only uses tools from linear algebra to compute solutions x of linear systems $Mx = y$ (we denote $x = M \backslash y$). Moreover, the involved matrices are easy to handle. Note also that from Proposition 2, we know that the function in output is not unique, but the last matrix M, at the end of the computation, generates the subspace $\cap_i Ker(\alpha_i)$, so we can recover any differential equivalent functions.

Algorithm 1 Antidifferentiation over $\mathbb{F}_{2^n}$.

function ANTIDERIVATIVE($\{(f_i, \alpha_i) \mid 1 \leq i \leq m\}$ verifying conditions in Th. 3)

1: $M \leftarrow K(\alpha_1)$; $\quad \overrightarrow{sol} \leftarrow 0_{\mathbb{F}_{2^n}^{2^n}}$; $\quad \overrightarrow{F_1} \leftarrow M(\alpha_1)\backslash\overrightarrow{f_1}$;
2: **for** $i = 2$ to $i \leq m$ **do**
3: $\quad \overrightarrow{F_i} \leftarrow M(\alpha_i)\backslash\overrightarrow{f_i}$;
4: $\quad \overrightarrow{sol} \leftarrow \overrightarrow{sol} + M \cdot \Big((M(\alpha_i)M) \setminus \Big(M(\alpha_i) \cdot \overrightarrow{F_1 + F_i + sol}\Big)\Big)$;
5: $\quad M \leftarrow M\kappa$; $\quad \triangleright\ \kappa$: generating matrix of $\ker(M(\alpha_i)M)$
6: **return** $sol + F_0$

5 Applications

In this section, we discuss the first natural application which consists in recovering quadratic APN functions from 2-*to*-1 affine functions. We briefly discuss the main idea of this method and show its equivalence to the previous works [15, 17]. We believe also that our point of view permits a better understanding of these works.

From the previous sections (or [16, Proposition 1]), we know that every affine function, $L(x) = \ell + \sum_i c_i x^{2^i} \in \mathbb{F}_{2^n}[x]$, is a derivative function if and only if L is not bijective. We can adapt Theorem 3 to fit affine functions and to find an easier condition since the differential of an affine function is constant:

Corollary 4. *Let $\alpha_1, \ldots, \alpha_m \in \mathbb{F}_{2^n}^*$ be $\mathbb{F}_2-$linearly independent elements and let $L_1, \ldots, L_m : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be affine functions such that $L_i(\alpha_i) = 0$, $1 \leq i \leq m$. Then there is at least one (quadratic) function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ such that $\Delta_{\alpha_i} F(x) = L_i(x)$, for all $1 \leq i \leq m$,* if and only if *$L_i(\alpha_j) + L_i(0) = L_j(\alpha_i) + L_j(0)$, for all $1 \leq i, j \leq m$.*

Note that a function is quadratic if and only if all of its derivatives are at most affines [2].

Let $\alpha_1, \ldots, \alpha_n \in \mathbb{F}_{2^n}^*$ be a base of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$ and consider the following matrix:

$$B = (\beta_{i,j})_{1 \leq i,j \leq n} = \begin{pmatrix} \beta_{1,1} & \beta_{1,2} & \beta_{1,3} & \cdots & \beta_{1,n} \\ \beta_{2,1} & \beta_{2,2} & & \cdots & \\ \vdots & & \ddots & & \vdots \\ \beta_{n,1} & & \cdots & & \beta_{n,n} \end{pmatrix}. \tag{8}$$

If we assume that each row of this matrix is a base of a subspace of $\mathbb{F}_{2^n}$, then there exist non-bijective affine functions $L_i : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ satisfying (without loss of generality)

$$\beta_{i,j} = L_i(\alpha_j) + L_i(0), \qquad \text{for all } 1 \leq i, j \leq m.$$

Remark that in this case, each $\beta_{i,i}$ should be zero. Then, from each row of the matrix B in (8), we can recover the coefficients of the affine functions L_i's by a simple linear operation. Moreover, if we choose our $\beta_{i,j}$ wisely such that

they satisfy the condition of Eq. (7) (*i.e.* the matrix B is symmetric), then there is a unique (quadratic) function (up to a constant, due to the differential equivalence) $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, which we can easily recover with Algorithm 1, such that $\Delta_{\alpha_i} F(x) = L_i(x)$, for all $1 \leq i \leq n$.

Finally, if all non-zero elements of each row of B are $\mathbb{F}_2$-linearly independent, it induces that the image set of each affine function L_i is an hyperplane (subspace of dimension 2^{n-1}), that is each L_i is 2-*to*-1. Furthermore, if any linear combination of the rows of matrix B spans again an hyperplane, the antiderivative F must be APN.

This kind of matrices B we just described, are exactly the kind of matrices used in [15] and [17] and have permitted to discover hundreds of new quadratic APN functions. However, the method to justify them and to recover the function F is slightly different. Indeed, our algorithm to recover the antiderivative F is more general, since it would work theoretically with non-affine 2-*to*-1 compatible derivatives. We would thus end up with non-quadratic APN functions.

As another application of the tools presented in the sections above, we can look for functions differentially equivalent to APN functions with respect to a subspace of dimension $\leq n-3$ (so that the functions to add in order to remain in the differential coset are quadratic). We performed a quick search on small fields ($5 \leq n \leq 9$) trying to find new APN functions from non-quadratic APN power functions with respect to a subspace of dimension $n-3$. Although exhaustive search in this differential cosets is expensive, after hours of computation, we did not find yet other APN functions in this differential coset. This leads us to express the following conjecture:

Conjecture 1. By fixing 2^{n-3} derivatives, in directions given by a subspace of $\mathbb{F}_{2^n}$, of a non-quadratic APN power functions, there is no other APN functions in its differential coset.

6 Conclusion

In this paper, we provided a different point of view on derivatives and higher order derivatives over $\mathbb{F}_{2^n}$. In the light of the above, concerning the possibility to recover APN functions, we shown that researchers should keep the focus on finding and studying class of 2-*to*-1 functions. Indeed, prior to this work, not much was known about what we could have done with 2-*to*-1 derivatives. The more we will know about these functions, the easier it will be to combine them (with respect to conditions of Theorem 3) and thus to recover APN functions using antidifferentiation over $\mathbb{F}_{2^n}$.

On another hand, the differential equivalence permits a new classification of functions over $\mathbb{F}_{2^n}$ that will very probably lead to new constructions of functions with prescribed differential properties over $\mathbb{F}_{2^n}$. Moreover, the matrix representation of derivatives we introduced in this paper should ease the future experiments.

References

[1] R.B.J.T Allenby and Alan Slomson. *How To Count: An Introduction To Combinatorics*. Discrete Mathematics and Its Application. CRC Press, 2010.

[2] Thierry Berger. Priveate communication, 2014.

[3] Eli Biham, Alex Biryukov, and Adi Shamir. Cryptanalysis of skipjack reduced to 31 rounds using impossible differentials. In Jacques Stern, editor, *Advances in Cryptology - EUROCRYPT '99, International Conference on the Theory and Application of Cryptographic Techniques, Prague, Czech Republic, May 2-6, 1999, Proceeding*, volume 1592 of *Lecture Notes in Computer Science*, pages 12–23. Springer, 1999.

[4] Eli Biham and Adi Shamir. Differential Cryptanalysis of DES-like Cryptosystems. *J. Cryptology*, 4(1):3–72, 1991.

[5] Christina Boura and Anne Canteaut. Zero-Sum Distinguishers for Iterated Permutations and Application to Keccak-f and Hamsi-256. In Alex Biryukov, Guang Gong, and Douglas R. Stinson, editors, *Selected Areas in Cryptography*, volume 6544 of *Lecture Notes in Computer Science*, pages 1–17. Springer, 2010.

[6] Claude Carlet, Pascale Charpin, and Victor Zinoviev. Codes, Bent Functions and Permutations Suitable For DES-like Cryptosystems. *Des. Codes Cryptography*, 15(2):125–156, 1998.

[7] Itai Dinur and Adi Shamir. Cube attacks on tweakable black box polynomials. In Antoine Joux, editor, *Advances in Cryptology - EUROCRYPT 2009, 28th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Cologne, Germany, April 26-30, 2009. Proceedings*, volume 5479 of *Lecture Notes in Computer Science*, pages 278–299. Springer, 2009.

[8] Yves Edel. On quadratic APN functions and dimensional dual hyperovals. *Des. Codes Cryptography*, 57(1):35–44, 2010.

[9] Yves Edel and Alexander Pott. A new almost perfect nonlinear function which is not quadratic. *Advances in Mathematics of Communications*, 3(1):59–81, 2009.

[10] Paul R. Halmos. *Finite-Dimensional Vector Spaces*. The Unversity Series in Undergraduate Mathematics. D. Van Nostrand Company, 1958.

[11] Lars R. Knudsen. Truncated and Higher Order Differentials. In Bart Preneel, editor, *FSE*, volume 1008 of *Lecture Notes in Computer Science*, pages 196–211. Springer, 1994.

[12] Xuejia Lai. Higher Order Derivatives and Differential Cryptanalysis. In *Symposium on Communication, Coding and Cryptography, in honor of James L. Massey on the occasion of his 60'th birthday*, Monte-Verita, Ascona, Switzerland, February 10-13 1994.

[13] Kaisa Nyberg. Differentially uniform mappings for cryptography. In Tor Helleseth, editor, *Advances in Cryptology - EUROCRYPT '93, Workshop on the Theory and Application of of Cryptographic Techniques, Lofthus, Norway, May 23-27, 1993, Proceedings*, volume 765 of *Lecture Notes in Computer Science*, pages 55–64. Springer, 1993.

[14] David Wagner. The boomerang attack. In Lars R. Knudsen, editor, *Fast Software Encryption, 6th International Workshop, FSE '99, Rome, Italy, March 24-26, 1999, Proceedings*, volume 1636 of *Lecture Notes in Computer Science*, pages 156–170. Springer, 1999.

[15] Guobiao Weng, Yin Tan, and Guang Gong. On Quadratic Almost Perfect Nonlinear Functions and Their Related Algebraic Object. In *Workshop on Coding and Cryptography, WCC 2013*, April 2006. Bergen, Norway.

[16] Hai Xiong, Longjiang Qu, Chao Li, and Ying Li. Some results on the differential functions over finite fields. *Appl. Algebra Eng. Commun. Comput.*, 25(3):189–195, 2014.

[17] Yuyin Yu, Mingsheng Wang, and Yongqiang Li. A matrix approach for constructing quadratic APN functions. In *Workshop on Coding and Cryptography, WCC 2013*, April 2006. Bergen, Norway.