International Journal of Algebra, Vol. 19, 2025, no. 3, 89 - 206
HIKARI Ltd, www.m-hikari.com
https://doi.org/10.12988/ija.2025.91961

Solution to 9 Notable Problems and Expansion of the Theory of Highly Nonlinear Functions

Roberto C. Reyes Carranza

Department of Mathematics
Long Island University, Brooklyn Campus
1 University Plaza
Brooklyn, NY 11201 USA

Mathematics Department
Manhattan University
4513 Manhattan College Parkway
Riverdale, NY 10471 USA

Abstract

We extend the Theory of Differentially δ-Uniform Functions in its various confines, now its influence is multiplied; we provide a special collection of K-Algebras. This solves hot challenges, e.g.: 1). We generalize for the second time Dillon's switching method in the (general) differentially uniform context. 2). With a singular style, we develop the analysis of Differential Equations exclusively for Galois fields (Section 9.4: an in-depth discussion, plus questions that require immediate action); on which there is hardly any research done and in a completely different sense, where the investigated functions have co-domain that is never the structure $\mathbb{F}_{p^n}$. Besides, we generalize the elegant BDC of Steinbach-Posthoff, and construct fascinating Chain Complexes. We introduce the $\mathbb{F}_{p^n}$-*Schrödinger equation* (and the newest *Black-Scholes*). 3). We obtain the novel Fundamental Theorem of Calculus associated with a derivative order type other than the famous Fractional. Further, we conduct the corresponding Algebraic Attack on the functions that currently offer the best resistance, and identify the survivors.

Mathematics Subject Classification: 11T71, 06E30, 26A33, 94A15, 06E20, 18G35, 47G30, 20C05

Keywords: nonlinearity, differential uniformity, differential cryptanalysis, chain complexes, differential equation, PDE, Reed-Muller codes, covering radius, finite field, Galois field, algebraic degree, permutation polynomial, number theory, combinatorics, block cipher, S-Box, vectorial Boolean function, Walsh transform, APN, cyclic code, statistical attack, cosets of subspaces covering, the polynomial method, Dembowski-Ostrom polynomial, Kloosterman sum, exceptional APN function, presemifield, algebraic cryptanalysis, dynamical system, Black-Scholes equation, AES, Rijndael, Serpent, polynomial ring, information security, code-breaker

1 Introduction

(Continued) 4). We solve the theoretical-concrete problem posed by Courtois and Pieprzyk about finding any non-linear S-box F not equivalent to the multiplicative inverse function, admitting a type of so many implicit equations $Q(x_1, \ldots, x_n, y_1, \ldots, y_n) = 0$, where Q has a low algebraic degree. 5-6). Regarding the prominent conjecture stated by Budaghyan, Carlet, and Leander concerning the CCZ-inequivalence between their exotic function F_n and power functions—which we show to be true for all known power APNs—we determine the form of the mappings applied by them and by us. This also allows us to ensure that the protagonist function we conceive, $J_{(n_i)_{i=0}^{\infty}}$, answers the problem of finding an APN family that is not CCZ-equivalent to the existing ones (where APN is being the *optimal* in terms of *differential attacks*, and is *optimal* in the sense that every derivative of it minimizes the sum of squares portion of the Walsh-Hadamard coefficients $\sum_{\lambda \in \mathbb{F}_{2^n}} W^2_{\Delta_a f}(0, \lambda)$); furthermore $J_{(n_i)_{i=0}^{\infty}}$ is *exceptional* APN. 7). We contribute to the powerful problem of Méaux and Roy of finding Boolean functions whose derivative also has a high algebraic degree. 8). Finding powerful S-boxes that are resistant to differential attacks has been a priority for the past 30 years, especially when the field degree is even (the case in most applications). We make a significant contribution to an open problem staten by Bracken and Leander, by constructing an infinite class of differentially 4-uniform functions (also covering the next cases, $\delta = 6, 8$). As for the criteria of choosing an S-box as a component for an iterated block cipher, Blondeau, Canteaut, and Charpin emphasize that it should be differentially 4-uniform whose differential spectrum contains a small $|\{b \in \mathbb{F}_{2^n}; \delta_f(a, b) = 4\}|$. Our permutations $\tilde{I}_{\tilde{x}_0,0}$ and $\tilde{I}_{\tilde{x}_0}$ satisfy this requirement. 9). We show that the pioneering infinite class of highly nonlinear functions of R. Carranza $\mathcal{C}^{\text{all}}_{2;n-1}$ owns all algebraic degrees including the optimum.

In the vast cosmos of applications based upon discrete objects, the field of even characteristic $\mathbb{F}_{2^n}$ is ubiquitous, and is the one to which we shall pay most attention. To provide randomness, major symmetric cryptosystems are using functions from $\mathbb{F}_{2^n}$ to itself, called S-boxes, which are required to show a low

differential uniformity (to provide protection against differential cryptanalysis and to its variants) and a high nonlinearity (to protect against linear cryptanalytic attacks) (see [104, 11, 109], and [52]). A secure S-box in a substitution-permutation network should be a permutation with a high algebraic degree to protect against higher order differential attacks and the Berlekamp-Massey attack (see [87, 88, 17, 33], and [31]). We must take a short break to point out that, in addition, we propose problems that will require a certain recognizable mental caliber, those **New Representative Open Problems** are: 3, 4B, 5, 8, 11, 13, 17, 19, 21, and 23 to 33.

The Advanced Encryption Standard (AES) uses the multiplicative inverse function, which is a differential 4-uniform function. Finding infinite classes of APN (even differential 4 or 6-uniform) permutations with high nonlinearity on even degree field extensions is a current challenge. In [18], Bracken and Leander listed this as an open problem. To know more about a class of sporadic binomials permutations with low differential uniformity ($\delta = 4, 6$), see the article of Charpin and Kyureghyan (2017) in [39]. Then Qu, Tan, How Tan, and Li [109] gives us a survey of differentially 4-uniform permutation families, even without the requirement of high nonlinearity (see Carlet [32], and Zha [138]).

Note that we can identify the field $\mathbb{F}_{2^n}$ with the vector space $\mathbb{F}_2^n$ over $\mathbb{F}_2$, depending on how much algebraic structure is needed. We construct new families of δ-uniform permutations in even degree field extensions (also for odd degree extensions), where δ can be 4, 6, and 8. Our functions are represented via an explicit formula in univariate polynomial representation, the more desired representation. In this process, we obtain new general and practical theorems that can be widely applied in any finite field, e.g., to construct new S-Boxes.

We had the privilege of discovering results of unusual advantage and applicability, on which the construction of our functions is based; we talk about several powerful results such as, for example, the Partition of Finite Fields by Affine Functions, Theorem 4.9. A sort of infinite classes of functions such as the subclass $K_{i,n-k}(x) = x^{2^{2i}-2^i+1} + (x^{2^{2i}-2^i} + x^{2^{2i}-(2)2^i+1} + x^{2^{2i}-(2)2^i} + x^{2^{2i}-(3)2^i+1} + x^{2^{2i}-(3)2^i} + \ldots + x^{2^i+1} + x^{2^i} + x + 1)Tr_n^1(a_1x)\ldots Tr_n^1(a_{n-k}x)$ is granted by bases of the underlying structure of vector space. For this reason we shall call this generatrix method as follows: *generatrix granted by the underlying space* $\mathbb{F}_2^n$. Suggested **Problem 1:** investigate this method for the complementary case, that is, for $\mathbb{F}_{p^n}$—identifying it with its corresponding underlying vector space $\mathbb{F}_p^n$—for odd characteristic p. The generatrix granted by the underlying space $\mathbb{F}_2^n$ is a powerful generator; for each function F, this method is able to generate a family of functions f, of the form $f = F\mathrm{o}(\mathrm{Id} + P_r)$, with cryptographic strengths very similar to those held by F; in the case where, for example, F is a power function, possible limitations in the implementation cost are circumvented by our f. The way how we change the affine subspace (a $k_{n,r}$-flat),

delineated mainly by the equation $|U_{a_1} \cap \cdots \cap U_{a_r}| = 2^{n-r}$, which in an special case can be made of a few points distributed by an internal symmetry, leads us to exceptional results (consult Subsection 4.1). We dedicate Section 5 to the analysis of the algebraic degree of this stellar family. The algebraic degree is a main aspect in the construction of any function classified as powerful, we develop this idea by pre-visualizing fascinating and diverse mathematical constructions; this will be the centerpiece that will allow, for example, to develop the analysis of *Differential Equations* properly for $\mathbb{F}_{p^n}$ in its most general context, refer to Section 9. We also cover the *Boundary Value Problem* on the Évariste Galois Field, the time-dependent $\mathbb{F}_{p^n}$*-Schrödinger-type equation* $-\mu\nabla^2(\Psi) + V(X,T)\Psi = \gamma\partial_{T=\bar{H}}(\Psi)$, and the newest *Black-Scholes model*.

Almost all of the diff. 4-uniform permutations that have been found are only of algebraic degree $n-1$, and functions with that quality are now abundant. Each of the current functions may be interesting in their formulation and present a certain degree of non-vulnerability to a particular type of attack. Furthermore, it is inevitable to carry out a comparison between them; it is worth noting that in Subsection 8.1 we present the advantages and weaknesses in the race to design the strongest S-box. Taking into account the set of cryptographic qualities of interest (in Section 8 we provide a list of these qualities), our functions achieve definitely remarkable and widely diverse outcomes, belonging to the almost empty select subset with top-tier quality within the existing families. In this competition, the well-known power functions (which are diff. 4-uniform when the degree of the field is even), which were the first to appear, have been taken into account. We carry out this comprehensive comparison in a side-by-side format in a tabular form (see Tables 3 to 7). Much of the research community presents their constructions of differentially 4-uniform permutations by modifying the image values in different ways. Almost all of them rely on the function used by AES, thus interconnecting the different points of view within this portion of the topic, which is known to be competitive, attracting people of proven brilliance. One can start with the desire to make a fairly general statement, but sometimes some properties are lost, asking ourselves: **specifically, regarding the final result, which family or families of S-Boxes are the most efficient?**. We list them in Sub-section 8.1. Our method produces in both fields (whose degree is even, but also includes those of odd degree), families in each of the top three categories, that is, permutations f for $\Delta(f) = 4$, $\Delta(f) = 6$, and $\Delta(f) = 8$, in addition, this class has all possible algebraic degrees. The functions built by the different authors present interesting architectures that can be used in more than one application.

World-scale leaders whose outlook is in common with ours are the following: Claude Shannon Institute, מכון ויצמן למדע (Weizmann Institute of Science), IBM, Eidgenössische Technische Hochschule Zürich (ETH Zurich),

Centre National de la Recherche Scientifique (CNRS), Universitetet i Bergen, Army Research Office, among a few other top institutions. In order to provide complete coverage of this deepening of the discipline, the author believes it convenient to retain part of his Ph.D. thesis [111]. Specifically, our fertile research has reached a priceless development by touching on hot topics of the highest applicability. The following is strongly related to ours, a *discrete dynamical system* is defined as the pair $(f, \mathbb{X})$ made up of a function $f : \mathbb{X} \longrightarrow \mathbb{X}$, where $\mathbb{X}$ is a finite set. An *artificial neural network* is a special case that, due to its applications, is worth mentioning. The dynamics of f is given by the sequence of compositions: (including the identity $\mathrm{id}_{\mathbb{X}}$ and f itself), fof, $fofof$, etc. This immediately produces the directed graph whose vertex set is $\mathbb{X}$ and the edge set is the set of $a \to b$ such that $b = f(a)$ (there may be edges of the form $a \to a$); it can be observed that from this graph all state transitions of f can be deduced, meaning that this graph (called the state space of f) is a way of representing the dynamics of f. Our functions are also discrete dynamical systems, and may be useful in that framework [121, 129].

A large constituent of the universe has a discrete configuration. It is a must to describe discrete objects, R, with some finite cardinality $|R|$, of course, this is done for infinite pairs $(R, |R|)$. We will focus on the abstraction of the widely applicable $\mathbb{Z}$, that is, we will consider rings $(R, +, \times)$ that are commutative with multiplicative identity, and where the cancellation property (Theorem 1.2; making R an *integral domain*) can be applied. Let us look at the situation of the ring of square matrices with n rows with entries in R. Overall, this matrix ring, $M_{n\times n}(R)$, is not commutative, consider $n > 1$ and $R(\neq \{0\})$ commutative; meanwhile, the matrix product in $M_{n\times n}(R)$ is defined following a row-column algorithm via the operations on the commutative ring R. In this sense $M_{n\times n}(R)$ is not so non-commutative, it works closely connected with the commutative. Then the same applies to the so-called general linear group, of $n \times n$ invertible matrices, $GL(n, R)$, also to its subgroup of all matrices with determinant 1, $SL(n, R) = \ker(\det : GL(n, R) \to R^*)$ (recall that if R is a field with multiplicative group R^*, then $GL(n, R)$ can be expressed in terms of its $SL(n, R)$, as the semidirect product $GL(n, R) = SL(n, R) \ltimes R^*$). Everything is going splendidly, since such an integral domain turns out to be a Field; at this point R acquires the old natural feature belonging to the physical world of having quite a bit of cyclicity, more precisely, R without a point (0) is cyclic. Theorem 1.3 is a pinnacle fact, putting our exclusive attention on *finite fields*. We want that when we manipulate the polynomial functions (channels that communicate-transform the elements of one ring into those of another; isomorphisms and any ring homomorphism are examples of this) on R we have the division algorithm (i.e. $R[X]$: a *Euclidean domain*). The structure $R[X]$ (see Theorem 1.6) is just an integral domain, and the struggle to understand how it works is not over. First, we introduce some notations.

Theorem 1.1 *[65]. The following facts apply to an ideal:*
1). Every ideal is the kernel of a ring homomorphism and vice versa.
2). Assume R is a commutative ring with identity. The ideal (in R) M is a maximal ideal if and only if the quotient ring R/M is a field.
3). If R is a field, the maximal ideals in $R[x]$ are the ideals $\langle f(x)\rangle$ generated by irreducible polynomials $f(x)$.

Theorem 1.2 *[65] (Cancellation Property). Let R be a commutative ring with identity. Then R is an integral domain if and only if for every b, c in R, and every nonzero element $a \in R$ such that $ab = ac$, we have $b = c$.*

Theorem 1.3 *[65]. Finite Fields are the only finite Integral Domains.*

Let p be a prime number. Let us define the *category* $\mathbf{Ga}_{(\mathrm{char}=p)}$ consisting of the collection of objects of the form $\mathrm{ob}(\mathbf{Ga}_{(\mathrm{char}=p)}) \stackrel{\mathrm{def}}{=} \{GF(p), GF(p^{l_1}), GF(p^{l_1 l_2}), GF(p^{l_1 l_2 l_3}), \ldots\}$ and whose collection of morphisms from A to B, for each $A, B \in \mathrm{ob}(\mathbf{Ga}_{(\mathrm{char}=p)})$ we delimit it through:

$$\mathrm{Hom}_{\mathbf{Ga}_{(\mathrm{char}=p)}}(A,B) \stackrel{\mathrm{def}}{=} \begin{cases} \mathrm{Hom}(A,B), \text{if } A \leqslant B, \\ \{0(x)\}, \text{if } A \nleqslant B \end{cases}$$

so that Theorem 1.5 is respected; $\mathrm{Hom}(A,B)$ denotes the collection of homomorphisms from A to B. It is noteworthy that $\mathrm{ob}(\mathbf{Ga}_{(\mathrm{char}=p)})$ consists of almost cyclic objects, see Theorem 1.4; in general, for $(R,+,\times)$ not isomorphic to the prime field $\mathbb{Z}_p$, the additive group $(R,+)$ $(\supseteq (R^*,+))$ cannot be cyclic (more generally, as an Abelian group, $(R,+)$ is isomorphic to the direct product of cyclic groups $\mathbb{Z}_{p^{\alpha_1}} \times \mathbb{Z}_{p^{\alpha_2}} \times \cdots \times \mathbb{Z}_{p^{\alpha_n}}$, where every $\alpha_i = 1$). Throughout the article, we shall deal with classes of functions beyond morphisms in $\mathrm{Hom}_{\mathbf{Ga}_{(\mathrm{char}=p)}}(A,B)$, i.e. a variety of non-homomorphisms in the *category* $\mathbf{Ca}_{(\mathrm{char}=p)}$ consisting of $\mathrm{ob}(\mathbf{Ca}_{(\mathrm{char}=p)}) \stackrel{\mathrm{def}}{=} \mathrm{ob}(\mathbf{Ga}_{(\mathrm{char}=p)})$ and $\mathrm{Hom}_{\mathbf{Ca}_{(\mathrm{char}=p)}}(A,B) = \widetilde{\mathrm{Hom}}_{\mathbf{Ga}_{(\mathrm{char}=p)}}(A,B) \stackrel{\mathrm{def}}{=} \mathrm{Hom}_{\mathbf{Set}}(A,B)$, where **Set**, written in bold, represents the *category of sets*. By the way, regarding category theory one can look at Tom Leinster's book [90].

Theorem 1.4 *Let R be a finite field. The nonzero elements in R form the group under multiplication $(R^*,\times)$, which is also isomorphic to the cyclic group $\mathbb{Z}_{p^n-1}$, where R has size equal to p^n.*

Theorem 1.5 *[65]. If R is a field then any nonzero ring homomorphism from R into another ring, R', can only be an injection.*

Theorem 1.6 *[65]. The following sequence of facts about the ring $R[x]$ holds:*

1). If R is a ring (if it is commutative), then $R[x]$ is a ring (commutative too). In such a case, if both $f(x), g(x) \in R[x]$, then $\deg(fg) \leq \deg(f)+\deg(g)$.

2). If R is an integral domain, then $R[x]$ is an integral domain. If both $f(x), g(x) \in R[x] \setminus \{0\}$, then $\deg(fg) = \deg(f) + \deg(g)$. The units of $R[x]$ are just the units of R.

(Note: there will be times when we denote a function F by its image $F(x)$).

3). If R is a field, then $R[x]$ is (still) an integral domain.

4). If R is a commutative ring such that $R[x]$ is a Euclidean Domain (i.e., an integral domain equipped with a Division Algorithm), then R is necessarily a field. Part (4) also works when $R[x]$ is a Principal Ideal Domain.

Theorem 1.7 *[65]. Let $\mathbb{K}$ a field. The polynomial ring $\mathbb{K}[x]$ is a Euclidean Domain. Specifically, if $\tau(x)$ and $\kappa(x)$ are polynomials in $\mathbb{K}[x]$ with $\kappa(x)$ nonzero, then there are unique $q(x)$ and $r(x)$ in $\mathbb{K}[x]$ such that $\tau(x) = q(x)\kappa(x) + r(x)$ with $r(x) = 0$ or $\deg(r(x)) < \deg(\kappa(x))$.*

Theorem 1.8 *[94] (Hermite-Dickson's Criterion (1897)) $f \in \mathbb{F}_{p^n}$ is a permutation polynomial of $\mathbb{F}_{p^n}$ if and only if the following conditions hold:*

1). f has exactly one root in $\mathbb{F}_{p^n}$;

2). for each integer t with $1 \leq t \leq p^n - 2$ and $t \neq 0 \mod (p)$, the reduction of $f^t(x) \mod (x^{p^n} - x)$ has degree $\leq p^n - 2$.

Definition 1.9 *[31] $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ is linear if F is a linearized polynomial over $\mathbb{F}_{2^n}$, that is, $F(x) = \sum_{i=0}^{n-1} c_i x^{2^i}$, where $c_i \in \mathbb{F}_{2^n}$. For any $c \in \mathbb{F}_{2^n}$, $F + c$ is called affine (Definition 1.11 generalizes this classic definition). A core type is the mapping $Tr_n^m(x) = \sum_{i=0}^{n/m-1} x^{2^{im}}$, called the trace function from $\mathbb{F}_{2^n}$ onto its subfield $\mathbb{F}_{2^m}$ (note that some authors denote it by $Tr_m^n(x)$ instead).*

Definition 1.10 *([31, 26]). Let the functions $F, G, P_1, P_2, A_0 : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, where P_1, P_2 are affine permutations, and A_0 is affine, then:*

1). G and $P_1 o G o P_2$ are called affine equivalent (A-E also AE).

2). G and $P_1 o G o P_2 + A_0$ are called extended affine equivalent (EA-E also EAE).

3). F and G are called Carlet-Charpin-Zinoviev equivalent (CCZ-E) if their graphs $\mathcal{G}_F$ and $\mathcal{G}_G$ are affine equivalent.

Any permutation is CCZ-equivalent to its inverse. EA-equivalence implies CCZ-equivalence, but not vice versa [24].

Definition 1.11 *[27] Every function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ has a unique representation as a univariate polynomial over $\mathbb{F}_{2^n}$ of degree at most $2^n - 1$, i.e., $F(x) = \sum_{i=0}^{2^n-1} c_i x^i$, $c_i \in \mathbb{F}_{2^n}$. Every integer $i \in [0, 2^n - 1]$, has unique a binary expansion $i = \sum_{s=0}^{n-1} i_s 2^s$, $i_s \in \{0, 1\}$. The algebraic degree of F is*

denoted (as opposed to its degree which is denoted as $\deg(F)$*) and defined as* $d^0(F) = max\{\omega_2(i); i \text{ is the exponent of a term in } F, \text{ with nonzero coefficient}\}$, *where* $\omega_2(i) = \sum_{s=0}^{n-1} i_s$ *is the 2-adic weight of* i. *A function of algebraic degree* $d^0(F) \leq 1$, *resp.* $d^0(F) = 2$, *resp.* $d^0(F) = 3$ *is called affine, resp. quadratic, resp. cubic.*

The simple definition that follows extends the algebraic degree initially defined for the ring $\mathbb{F}_{2^n}[x]$, to the ring $\mathbb{F}_{p^n}[x]$, which will fit perfectly in the subsequent results.

Definition 1.12 *(Generalized Algebraic Degree) Every function* $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ *has a unique representation as a univariate polynomial over* $\mathbb{F}_{p^n}$ *of degree at most* $p^n - 1$, *i.e.,* $F(x) = \sum_{i=0}^{p^n-1} c_i x^i$, *where* $c_i \in \mathbb{F}_{p^n}$. *Every integer* $i \in [0, p^n - 1]$ *has unique a expansion in base* p, $i = \sum_{s=0}^{n-1} i_s p^s$, *where* $i_s \in \{0, 1, \cdots, p-1\}$. *The algebraic degree of* F *is denoted and defined as* $d^0(F) = max\{\omega_p(i); i \text{ is the exponent of a term in } F\}$, *where* $\omega_p(i) = \sum_{s=0}^{n-1} i_s$. *Of course, if* T *is a term in* F, *then it cannot have coefficient equal to zero.*

Definition 1.13 *Let* $r \geq 1$. *Let us call* $\mathbb{F}_{p^n}^{d^0=r}[X]$ *(respectively, by* $\mathbb{F}_{p^n}^{d^0\leq r}[X]$*) the set of functions (in the variable* X *running* $\mathbb{F}_{p^n}$*) whose formulas belong to* $\mathbb{F}_{p^n}[X] \mod (X^{p^n} - X)$ *whose terms have algebraic degree equal to* r *(respectively, they have algebraic degree at most* r, *but including the set of all constant functions over* $\mathbb{F}_{p^n}$*).*

Definition 1.14 *([31, 26]). Let* $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, $a, b \in \mathbb{F}_{2^n}$, *the Walsh-Hadamard Coefficient is given by:* $W_f(a, b) = \sum_{x\in\mathbb{F}_{2^n}} (-1)^{Tr_n^1(bf(x)+ax)}$, *where* $Tr_n^1(x) = \sum_{i=0}^{n-1} x^{2^i}$ *is the trace function from* $\mathbb{F}_{2^n}$ *into* $\mathbb{F}_2$. *The set* $\mathcal{W}_f = \{W_f(a, b); a, b \in \mathbb{F}_{2^n}, b \neq 0\}$ *is called the Walsh (Walsh-Hadamard) spectrum of* f. *The set* $\{|W_f(a, b)|; a, b \in \mathbb{F}_{2^n}, b \neq 0\}$ *is called the extended Walsh spectrum of* f.

Definition 1.15 ***(Reed-Muller Codes)*** *([97, 43, 42]). Let* $v = (v_1, v_2, \ldots, v_n)$ *denote a vector which ranges over* $\mathbb{F}_2^n$, *and* $\boldsymbol{f}$ *the vector of length* 2^n *obtained from a Boolean function* $f(v_1, v_2, \cdots, v_n)$ *over* $\mathbb{F}_2^m$. *The* r*-th order binary Reed-Muller code* $RM(r, n)$ *of length* $N = 2^n$, *for* $0 \leq r \leq n$, *is the set of all vectors* $\boldsymbol{f}$, *where* $f(v_1, v_2, \cdots, v_n)$ *is the corresponding Boolean function which is a polynomial of degree at most* r.

Theorem 1.16 *([97]). The weight distribution of the coset of* $RM(1, n)$ *which contains* f *is* $\frac{1}{2}\{2^n \pm \hat{F}(u)\}$ *for* $u \in \mathbb{F}_2^n$, *where* $\hat{F}$ *is the Hadamard transform of the real vector* F *of* $1's$ *and* $-1's$, *and the component of* F *in the place corresponding to* u *is* $F(u) = (-1)^{f(u)}$.

The weight distribution of the coset containing f is thus determined by the Hadamard transform of F.

Definition 1.17 (Nonlinearity) *([43, 60]). The nonlinearity of a Boolean function f, is defined to be $NL(f) = d(f, RM(1,n))$ (i.e. the distance of f from $RM(1,n)$). Therefore it is also the weight of the coset $f + RM(1,n)$. And it also equal to the value attained in Theorem 1.16.*

We say that f is highly nonlinear whenever the amount $NL(f)$ is high enough with respect to the required security level, and close enough to one of the known bounds.

Corollary 1.18 *The covering radius of the Reed-Muller code $RM(1,n)$, $\rho(RM(1,n)) = \max_f NL(f)$, where f varies over all Boolean function of order $\leq n$.*

If the algebraic degree is r, it means that the Boolean function belongs to the r-th Reed-Muller code $RM(r,n)$. The algebraic degree of functions $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ with $d^0(f) \geq 2$ is invariant under EA-equivalence, but not under CCZ-equivalence (see [35]). The nonlinearity can be expressed in terms of the Walsh spectrum: $NL(f) = 2^{n-1} - \frac{1}{2}\max_{(a,b)\in\mathbb{F}_{2^n}\times\mathbb{F}_{2^n}^*} |W_f(a,b)|$.

Therefore, the nonlinearity is bounded by the covering radius of the corresponding Reed-Muller code. This problem has been investigated by coding theorists for decades with important results ([43]).

Definition 1.19 *[104, 112, 58]. Let G_1 and G_2 be finite Abelian groups. A function $f : G_1 \to G_2$ is differentially δ-uniform if $\forall a \in G_1 - \{0\}$ and $b \in G_2$, the equation $\Delta_a f(x) = b$ admits at most δ solutions, where $\Delta_a f(x) := f(x+a) - f(x)$ (derivative of f at the point x in the direction a). For $\delta = 2$ (the optimal situation), the function f is called APN (almost perfect non-linear). We are mainly interested in the scenario $G_1 = G_2 = \mathbb{F}_{2^n}$. Four equivalent definitions for APN function (going to the context of finite groups, Abelian or not, Robert Coulter and Marie Henderson call it semi-planar function [46]) are:*

1). The function $x \longrightarrow f(x+a) - f(x)$ is 2-to-1 for all $a \neq 0$.

2). $f(a)+f(b)+f(c)+f(d) \neq 0$, $\forall$ distinct $a, b, c, d \in \mathbb{F}_{2^n}$ with $a+b+c+d = 0$.

3). (Kaisa Nyberg; Thierry Pierre Berger, Anne Canteaut, Pascale Charpin, and Yann Laigle-Chapuy [105, 20]) For all $a \neq 0$, $\sum_{\lambda\in\mathbb{F}_{2^n}} W^2_{\Delta_a f}(0,\lambda) = 2^{2n+1}$.

4). (Refer to the French article by François Rodier [115]) A polynomial map f is APN iff the affine surface $f(x_0) + f(x_1) + f(x_2) + f(x_0+x_1+x_2) = 0$ has all of its rational points contained in the surface $(x_0+x_1)(x_1+x_2)(x_0+x_2) = 0$.

The set $\{\delta_f(a,b); a \in G_1 - \{0\}, b \in G_2\}$ *is called the differential spectrum of* f*, where* $\delta_f(a,b)$ *denotes the size* $|\{x \in G_1; \Delta_a f(x) = b\}|$*. In addition,* $\Delta(f) = \Delta_f := \delta = \max_{a \in G_1 - \{0\}, b \in G_2} \delta_f(a,b)$*. If* f *is APN on infinitely many extensions of* $\mathbb{F}_{2^n}$*, it is called exceptional APN.*

Lemma 1.20 *([23, 24, 34]). The differential spectrum and extended Walsh spectrum are CCZ-invariants. Consequently, the differential uniformity and nonlinearity of functions,* $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$*, are preserved.*

1.1 Towards the Derivative in the $\mathbb{F}_{p^n}$ Context

The (point-wise) derivative is one of the tools par excellence in the analysis of a function, f, whose fundamental notion is that it informs about the change that f undergoes around a point, this change being determined by the points neighboring the point. The Fréchet derivative considers functions from one normed vector space (over $\mathbb{R}$ or $\mathbb{C}$) to another, $f : V \to W$. All V, W, and their norm functions are tied to $\mathbb{R}$; given any $v \neq 0$ in V, there always exists ϵv in V for ϵ as close (under the usual topology of $\mathbb{R}$) to 0 as desired. Then, when the derivative exists (at a point x) it becomes natural to associate to it a (bounded) linear transformation $L_x : V \to W$, where it makes sense to approximate f locally by L_x on some open ball $B_{\|.\|_V}(x;\epsilon)$, such that L_x is the derivative of f at x; similarly it happens with the Gâteaux differentiability (weaker than Fréchet differentiability), but the following well-known fact also takes place: if the Fréchet derivative exists, then the Gâteaux derivative also exists, and both coincide. In the beautiful terrain of a function $f : M \to N$, where M (and N) are differentiable manifolds with dimensions m (and n), taking advantage of charts $(\varphi_{M,\alpha} : U_\alpha \to \mathbb{R}^m, U_\alpha)$ of M around x and $(\varphi_{N,\beta} : \widetilde{U}_\beta \to \mathbb{R}^n, \widetilde{U}_\beta)$ of N around $f(x)$, we can translate the derivative of f at x (if it exists) as the derivative at $\varphi_{M,\alpha}(x)$ of the induced function $\varphi_{N,\beta} \circ f \circ \varphi^{-1}_{M,\alpha} : \mathbb{R}^m \to \mathbb{R}^n$ (M is defined so that there is independence with respect to the chart around x that is applied). The derivative of f at x is the linear transformation between tangent spaces $df_x : T_xM \to T_{f(x)}N$ such that $df_x(v) = (f \circ \lambda)'(0)$, where v is the equivalence class $\cong$ of some curve λ on M (Two curves are equivalent according to $\cong$, $\lambda_1 \cong \lambda_2$: if they pass through x, i.e. $x = \lambda_1(0) = \lambda_2(0)$, and the quantity $\frac{d}{dt}(\varphi_{M,\alpha} \circ \lambda_1)(\text{at } t = 0)$ is the same for both), we shall denote v as $\lambda'(0)$; Similarly, $(f \circ \lambda)'(0)$ symbolizes the equivalence class corresponding to the curve $f \circ \lambda$ in N. If M is not a Euclidean space, then clearly sums like $x + v$ are meaningless, where $v \in T_xM$; however, given $y \in U_\alpha$ such that $\varphi_{M,\alpha}(y)$ belongs to some open ball $B_{\|.\|_{\mathbb{R}^m}}(\varphi_{M,\alpha}(x);\epsilon)$, df_x can be applied to the equivalence class $\tau'(0)$ of the curve τ over M, such that $\tau(0) = x$, $\frac{d}{dt}(\varphi_{M,\alpha} \circ \tau)(t = 0) = \varphi_{M,\alpha}(y) - \varphi_{M,\alpha}(x)$, to obtain an element in N (i.e. $\widetilde{f(y)} := \varphi^{-1}_{N,\beta}(\varphi_{N,\beta}(f(x)) + \frac{d}{dt}(\varphi_{N,\beta} \circ \mu)(t = 0))$) that in this sense

the charts allow $\|.\|_{\mathbb{R}^n}$-approximate to $f(y)$, where $\mu'(0) = df_x(\tau'(0))$. Again a linear map. Re-thinking abstractly, when we deal with a finite set of points as is the pure case of the structure $\mathbb{F}_{p^n}$, it is not possible to generalize the derivative in such senses (tied to $\mathbb{R}$, where the derivative at a point is a linear map) with any of the 2 definitions of derivative that this school of researchers uses to analyze the problems in our area (for example, Differential δ-Uniformity of S-Boxes). The so-called formal derivative (that is, $\frac{d}{dx}(a_0 + \sum_{i=1}^{k} a_i x^i) := a_1 + \sum_{i=2}^{k} i a_i x^{i-1}$) is not convenient, since the derivative of abundant functions leads to a trivial function in which valuable information about f is lost; in this respect, making use of such a formal derivative would be forcing one to continue using the derivative that was adequate for the non-discrete case. The derivative of f at a point according to Definition I, seen as a function of h ($\in \mathbb{F}_{p^n}$), is in general a non-linear map. Given such scarcity, the most strategic definition (universally used in the literature) of the derivative is given by comparisons in the dependent variable of the function f for a given point and direction. In the continuous case endowed with its usual topology (say, $f : \mathbb{C} \to \mathbb{C}$), if the derivative exists (equal to some $L \in \mathbb{C}$), L is obtained precisely from the set of comparisons, analogously, we will obtain it from a set of comparisons performed in our universe $\mathbb{F}_{p^n}$. The limit when h goes to 0 is taken to capture information about f at x. But this information comes from the set $\{\frac{f(x+h)-f(x)}{h}; \text{ as } h \neq 0\}$. The rate of change $\frac{f(x+h)-f(x)}{h}$ is approximated by L, that is, $f(x+h) - f(x)$ is approximated by the linear function (of $h \in \mathbb{C}$) Lh. Beyond this linear part, we can consider the complete expression of $f(x+h) - f(x)$. That is, we investigate the set $\{f(x+h) - f(x); \text{ where } h \neq 0\}$, note that here we do not need to take any limit. Let $x \in \mathbb{F}_{p^n}$, if we vary $h \in \mathbb{F}_{p^n} \setminus \{0\}$ in some way, then exactly the quantity **governed by** f, $\partial_h(f)(x) := f(x+h) - f(x)$ (**Definition I** of the derivative of f, also denoted by $\Delta_h(f)$ and $D_h(f)$), represents the natural device to measure the behavior of function f around $f(x)$. We introduce the second definition, $\widetilde{\partial_h}(f)(x) := \frac{f(x+h)-f(x)}{h}$ (**Definition II** of the derivative of f), here the numerator stores the information governed by f. As a consequence, the derivative in the degenerate case such that $h = 0$ (in $\mathbb{F}_{p^n}$) exists: $\partial_0(f) = 0$; also $\widetilde{\partial_0}(f) = 0$, subject to using the following convention with respect to the multiplicative inverse function, $\mathfrak{Y}(0) = 0$ (used in the literature for the field $\mathbb{F}_{2^n}$; similarly, we can identify $\mathfrak{Y}(x)$ with the bijection x^{p^n-2} onto $\mathbb{F}_{p^n}$). In the sense that equivalent goals are reached, using Definition II is equivalent to using Definition I (any direction h will be chosen other than 0); for example, Theorem 9.14, also Theorem 9.16, holds for both definitions. In the continuous case, it is common to find important functions such that their lateral or partial derivatives coincide in all directions, making it convenient to speak of a derivative with uniqueness (independent of all directions); but there is no problem if one considers the derivative over specific directions h (more generally, for each h this derivative

is unique, fortunately), as is also done in the continuous case when exploring subspaces of functions. In our context, the derivative is defined given some direction h, which allows us to analyze functions. We define the first-order derivative via $\partial^{(1)}_{h_1}(f) := \partial_{h_1}(f)$. The derivatives of order m for $m \geq 2$ are defined iteratively, $\partial^{(m)}_{h_1 \cdots h_m}(f) := \partial_{h_m}\big(\partial^{(m-1)}_{h_1 \cdots h_{m-1}}(f)\big)$, where $h_1, \cdots, h_m \in \mathbb{F}^*_{p^n}$, analogously for the other type of derivative.

Remark for Sec. 9.3. We will call the general type of derivation, $\frac{c\partial_a}{1-c}$, a *genuine derivation* (or sufficiently invertible) to indicate that there is an integral operator associated with it. Considering that the integral is the device that allows us to access the measurement of Area, through the 2nd `FTC`, the R. Carranza-Ellingsen-Felke-Riera-Stănică-Tkachenko-Borisov-Chew-Johnson-Wagner mod (p)-*c-integral operator* in the direction a makes it a reality to conceive the quantity *area under the curve* (`a.u.c.`) for a function $f : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$, from a point x_1 to a point x_2 in $\mathbb{F}_{p^n}$, that is, `a.u.c.` of $f = \mathcal{I}_{p-1,a,1-c;\,[x_1,x_2]}\ f := (\mathcal{I}_{p-1,a,1-c}\ f)|_{\text{at } x=x_2} - (\mathcal{I}_{p-1,a,1-c}\ f)|_{\text{at } x=x_1}$. So the `a.u.c.` of f is independent of the path between x_1 and x_2, but it still depends on the function $\mathcal{I}_{p-1,a,1-c}\ f$. Let us give the following conceptual aspect. The quantity $\mathcal{I}_{p-1,a,1-c;\,[x_1,x_2]}\ f$ is the input that leads us to access the measurement (Area) of the abstract-2-dimensional object for a function whose domain and codomain are both discrete sets built with a field structure. By the way, one can explore some variant (which is not necessarily carried out over the complete domain of integration) of the *convolution* $f * g$, suitable enough for ***signal processing***, this time for quality signals like $f, g : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$.

Table 1: Nonlinearities of Monomial APN (*semi-planar* [46]) Functions on $\mathbb{F}_{2^n}$.

In [84] Gohar Kyureghyan established a new version (extended) of the definition of *crooked* map (Thomas D. Bending and Dmitry Fon-Der-Flaass [8]) so that crooked maps are also available when n is even. J. F. Dillon and Hans Dobbertin performed the Walsh-Hadamard spectrum calculations for the Kasami-Welch and Gold families, showing that they coincide when $gcd(r, n) = 1$ [55, 56]. S. Yoshiara and U. Dempwolff showed that two APN power functions are CCZ-equivalent if and only if they are cyclotomic equivalent [135, 54]. R.C.R. Carranza [112] demonstrated the inequivalence according to Carlet-Charpin-Zinoviev between the Kasami-Welch function—as well as Welch, Niho, and applicable to Dobbertin—and the unusual Budaghyan-Carlet-Leander Gold based function. André Weil [131] obtained bounds for the Kloosterman sums. Later, Gilles Lachaud and Jacques Wolfmann [86], based on the fact that a not supersingular elliptic curve is isomorphic to a Kloosterman curve, and on results of Taira Honda, William C. Waterhouse, and René Schoof, found the form of the Kloosterman sums. The names Leonard Carlitz and Saburo Uchiyama [36] sound familiar when it comes to the nonlinearity of the multiplicative inverse function.

$f(x) = x^d$	Exponent d	Constraints	Nonlinearity	Ref.
Gold (AE to a *crooked* map)	$2^r + 1$	$gcd(r, n) = 1$	$2^{n-1} - 2^{\frac{n-1}{2}}$, n odd $2^{n-1} - 2^{\frac{n}{2}}$, n even	[72] [104] [84]
Kasami-Welch	$2^{2r} - 2^r + 1$	$gcd(r, n) = 1$	$2^{n-1} - 2^{\frac{n-1}{2}}$, n odd $2^{n-1} - 2^{\frac{n}{2}}$, n even	[81] [78] [112]
Welch	$2^r + 3$	$n = 2r + 1$	$2^{n-1} - 2^{\frac{n-1}{2}}$	[60] [76] [29]
Niho	$2^r + 2^{r/2} - 1$ $2^r + 2^{(3r+1)/2} - 1$	$n = 2r + 1$, r even $n = 2r + 1$, r odd	$2^{n-1} - 2^{\frac{n-1}{2}}$ (n odd)	[61]
Inverse	$2^{2r} - 1$	$n = 2r + 1$ (Not APN for n even)	If n is odd: $\lfloor 2^{n-1} - 2^{\frac{n}{2}} \rfloor \epsilon_{2, \gcd(\lfloor 2^{n-1} - 2^{\frac{n}{2}} \rfloor, 2)} +$ $(\lfloor 2^{n-1} - 2^{\frac{n}{2}} \rfloor - 1) \epsilon_{2, \gcd(\lfloor 2^{n-1} - 2^{\frac{n}{2}} \rfloor - 1, 2)}$ where $\lfloor x \rfloor := \ell \in \mathbb{Z}$, with $\ell \leq x < \ell + 1$, $\epsilon_{i,j}$: Kronecker's delta. If n is even: $2^{n-1} - 2^{\frac{n}{2}}$.	[104] [31] [36]
Dobbertin	$2^{4r} + 2^{3r} + 2^{2r} + 2^r - 1$	$n = 5r$		[62] [27]

Auxiliary Nomenclature:

`id`, or Id: identity function.

$\mathbb{F}_{p^n}$ also $GF(p^n)$: the finite field of characteristic p (a prime number) and degree n.

$\mathbb{F}_{p^n} \setminus A$ also $\mathbb{F}_{p^n} - A$ means the set complement of set A.

$\mathcal{G}_F$: the graph of the function F

$d^0(F)$: algebraic degree of F. Note that some authors use $\deg(F)$ to refer to $d^0(F)$, while others prefer to use $d^0(F)$.

$\deg(\varphi)$: degree of the polynomial φ.

$d^0_X(F)$: algebraic degree of F with respect to the variable X.

$\deg_X(\varphi)$: degree of the polynomial φ with respect to the variable X.

$|A|$ denotes the size (cardinality) of set A.

$\gcd(a, b)$: the greatest common divisor of a and b.

$\mathbb{Z}^+$ (and $\mathbb{Z}_0^+$): the set of positive integers (and non-negative integers), respectively.

$A \leqslant B$: A is subfield (respectively, is subring) of B, if A and B are fields (respectively, rings).

$\stackrel{\text{def}}{=}$, $:=$ both classical symbols are reserved to define a function, for example.

$\ker(f)$: the kernel, also known as the null space, of a linear transformation f is the part of the domain that f maps to the zero of the co-domain.

$\mathcal{F}\big(\mathbb{S}, \mathbb{K}\big)$: indicates the vector space (over $\mathbb{K}$) of functions ($f : \mathbb{S} \to \mathbb{K}$) between (a set) $\mathbb{S} \neq \varnothing$ and (a field) $\mathbb{K}$. More generally, if $\mathbb{K}$ is replaced by a (commutative) ring R, then $\mathcal{F}\big(\mathbb{S}, R\big)$ is an R-module.

$\mathcal{F}\big(\mathbb{S}\big)$: indicates $\mathcal{F}\big(\mathbb{S}, \mathbb{S}\big)$.

$\mathbb{F}^*_{p^n}$: stands for $\mathbb{F}_{p^n} \setminus \{0\}$. As for a ring R, $R^* = R \setminus \{0\}$.

$f(a)$, $f(A)$: we use parentheses to evaluate the function f over points as well as over sets, say a and A, respectively.

$NL(f)$: as $nl(f)$ is also used in the literature to denote the non-linearity of the function f.

$\overline{\mathbb{F}_{p^n}}$: is the algebraic closure of $\mathbb{F}_{p^n}$.

$R[x]$: polynomial ring in the variable x over R (with coefficients in R).

p: is a prime number throughout the article; while, for instance, P and $\mathcal{P}$, can denote something as specified where they are used.

$a|b$: a divides b.

Warning: when the occasion warrants it, we will denote a function f by its value $f(x)$ (on sporadic occasions); it will always be clear to distinguish when it is f itself and when it is its image.

2 Dillon-Edel-Pott Approach

The technique of *switching* an APN function ([67, 58, 57]) uses group ring (a free module) notation, to obtain functions with low differential uniformity by changing a component function of a known such function, a process that was first identified by John Dillon.

Definition 2.1 *Let $\mathbb{F}$ be an arbitrary field (the elements of this ring are the scalars) and $(G,+)$ a group (we shall consider G to be Abelian and not necessarily finite; its elements are the basis). Let the set $\mathbb{F}[G]$, wich consists of all elements of the form $a = \sum_{g\in G} a_g g$, where $a_g \in \mathbb{F}$ and the sum runs over some finite subset of G (called the support of a), together with the addition in a component-wise fashion, multiplication and the scalar multiplication, which are defined respectively as*

$$\begin{array}{c} \sum_{g\in G} a_g g \; + \sum_{g\in G} b_g g := \sum_{g\in G}(a_g + b_g)g, \\ \sum_{g\in G} a_g g \; \cdot \sum_{g\in G} b_g g := \sum_{g\in G}(\sum_{h\in G} a_h b_{g-h})g, \text{ and} \\ \alpha . \sum_{g\in G} a_g g := \sum_{g\in G}(\alpha a_g)g. \end{array}$$

$(\mathbb{F}[G], +, \, . \, , \, . \,)$ becomes an interesting algebra, the so called group algebra of G over $\mathbb{F}$.

Given a (n,n) function $(F : \mathbb{F}_2^n \to \mathbb{F}_2^n)$, consider the group algebra $\mathbb{F}[\mathbb{F}_2^n \times \mathbb{F}_2^n]$, where the formal sums $\sum_{v\in\mathbb{F}_2^n} c(v)(v, F(v))$, for $c(v) \in \mathbb{F}$, denote its elements. We focus on the case $c(v) \in \mathbb{F}_2 \subseteq \mathbb{F}$. We associate a group algebra element corresponding to the graph of the function F, $G_F := \sum_{v\in\mathbb{F}_2^n} 1(v, F(v))$. Let U a subgroup of G, consider the canonical group homomorphism: $\phi_U : G \longrightarrow \frac{G}{U}$, where $\phi_U(g) = g+U$. This group homomorphism can be extended by linearity to the homomorphism:

$$\begin{array}{rccc} \phi_U : & \mathbb{F}[G] & \longrightarrow & \mathbb{F}[\frac{G}{U}] \\ & D = \sum_{g\in G} a_g g & & \phi_U(D) := \sum_{g\in G} a_g(g+U) \end{array}$$

$\phi_U(D) = \sum_{g\in G} a_g(g+U) = \sum_{g+U\in\frac{G}{U}}(\sum_{h\in g+U} a_h)(g+U)$, the last sum is in terms of the cosets $g+U$, where we take the sum of all coefficients a_h such that $h+U = g+U$. If D has only coefficients (a_g) 1 or 0, so that $D = \sum_{g\in G,\ a_g=1} 1g$ corresponds to a set $D_\sharp = \{g; a_g = 1\} \subseteq G$, then the coefficient of $g+U$ in $\phi_U(D)$ is the following sum in $\mathbb{F}$:

$$\sum_{h\in g+U} a_h (\in \{0,1\}) = \sum_{h\in g+U,\ a_h=1} 1 = |D_\sharp \cap (g+U)|.$$

In particular, if each coset of U meets $D_\sharp$ in at most one element, i.e. $|(g+U)\cap D_\sharp| \in \{0,1\}$, $\forall g \in G$, then:

$$\phi_U(D) = \sum_{g+U\in\frac{G}{U}} |(g+U)\cap D_\sharp|(g+U) = \sum_{g+U\in\frac{G}{U},\ |(g+U)\cap D_\sharp|=1} g+U$$

and it has only coefficients 0 and 1. This is the case if U is a subgroup of ($\leqslant$) $\{0\}\times\mathbb{F}_2^n$.

Definition 2.2 *[67] Let U be a subgroup of $\mathbb{F}_2^n\times\mathbb{F}_2^n$. We say that the functions F and $H:\mathbb{F}_2^n\to\mathbb{F}_2^n$ are switching neighbours with respect to U if $\phi_U(G_F)=\phi_U(G_H)$. We say that F and H are switching neighbours in the narrow sense if $U\leqslant\{0\}\times\mathbb{F}_2^n$ and when U is viewed as a $\mathbb{F}_2$-vector space,* $\dim(U)=1$.

If F and H are switching neighbors with respect to U, we may obtain H from F by first projecting G_F onto $\phi_U(G_F)$, and then lifting this element to G_H, which give us the images of H. The subgroup $U\leqslant\{0\}\times\mathbb{F}_2^n$ has the advantage that the coefficients of $\phi_U(G_F)$ are 0 and 1 only, since the cosets of $\{0\}\times\mathbb{F}_2^n$ (and therefore also the cosets of U) meet G_F no more than once. G_F can be seen as our $D_\sharp$ above. In this case, $\phi_U(G_F)$ corresponds to a mapping $F_U:\mathbb{F}_2^n\to\frac{\mathbb{F}_2^n}{U'}$ with $F_U(v):=F(v)+U'$ and $U'=\{u;(0,u)\in U\}$, where U' is basically the same as U.

Now we study the equation $\phi_U(G_F)=\phi_U(G_H)$ in more detail, first consider $\phi_U(G_F)$:

$$\sum_{x\in\mathbb{F}_2^n} 1((x,F(x))+U) = \sum_{(x,F(x))+U\in\frac{\mathbb{F}_2^n\times\mathbb{F}_2^n}{U}} \Big(\sum_{h\in(x,F(x))+U} 1_h\Big)((x,F(x))+U)$$

as a formal sum in $\mathbb{F}[\frac{\mathbb{F}_{2^n}\times\mathbb{F}_{2^n}}{U}]$. Then $\phi_U(G_F)=\phi_U(G_H)$ as group ring elements if and only if $\phi_U(G_F)-\phi_U(G_H)=\sum_{x\in\mathbb{F}_2^n}0((x,F(x))+U)=\sum_{x\in\mathbb{F}_2^n}0\{(x,F(x)+u);u\in U'\}$. Then $\{(x,F(x)+u);u\in U'\}=\{(x,H(x)+u);u\in U'\}$, $\forall x\in\mathbb{F}_2^n$, i.e. $\{F(x)+u;u\in U'\}=\{H(x)+u;u\in U'\}$, $\forall x\in\mathbb{F}_2^n\Leftrightarrow H(x)\in F(x)+U'$, $\forall x\in\mathbb{F}_2^n$.

Lemma 2.3 *Let F, $H:\mathbb{F}_2^n\to\mathbb{F}_2^n$, and let $U\leqslant\{0\}\times\mathbb{F}_2^n$. Then $F_U=H_U$ iff $(0,F(v)-H(v))\in U$, $\forall\ v\in\mathbb{F}_2^n$. If $U=\{(0,0),(0,u)\}$, then $F_U=H_U$ iff there is a Boolean function $f:\mathbb{F}_2^n\to\mathbb{F}_2$ such that $H(v)=F(v)+f(v).u$.*

Lemma 2.3 shows that one may obtain all switching neighbors of F in the narrow sense (with respect to a one-dimensional subspace) by adding a Boolean function f times a vector $u\neq 0$. Let F be an APN function, the following theorem of Yves Edel and Alexander Pott [67] gives a necessary and sufficient

condition for f to produce another (not necessarily equivalent) APN function by the application of the switching method:

Theorem 2.4 *[67]*
Assume that $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ is an APN function. Let $u \in \mathbb{F}_2^n$, $u \neq 0$, $f : \mathbb{F}_2^n \to \mathbb{F}_2$ be a Boolean function, and $H(v) := F(v) + f(v).u$. Then: H is an APN function $\iff$ (For all x, y, $a \in \mathbb{F}_2^n$, $(F(x) + F(x+a) + F(y) + F(y+a) = u \implies f(x) + f(x+a) + f(y) + f(y+a) = 0)$).

The following theorem set up a general method for constructing new quadratic APN functions from known ones.

Theorem 2.5 *[26] Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be a quadratic APN function, let $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$ be a quadratic function where m is a divisor of n, $\varphi_F(x,a) = F(x) + F(x+a) + F(a) + F(0)$, and $\varphi_f(x,a) = f(x) + f(x+a) + f(a) + f(0)$. If for every $a \in \mathbb{F}_{2^n}^*$ there exists a linear function $l_a : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$ such that:*
1). $\varphi_f(x,a) = l_a(\varphi_F(x,a))$ on $\mathbb{F}_{2^n} \times \{a\}$,
2). For every $u \in \mathbb{F}_{2^m}^*$, if $\varphi_F(x,a) = u$ for some $x \in \mathbb{F}_{2^n}$ then $l_a(u) \neq u$.
Then $F + f$ is an APN function.

By application of Theorem 2.5 Budaghyan et al. founded an APN function (see Theorem 7.3) which possesses a simple and closed polynomial formula.

3 An Ultimate Generalization of Dillon Switching Method Towards δ-Uniform Classes

Both theorems 2.4 and 2.5 are major results in the theory of APN Functions; we can show that Theorem 2.4 implies Theorem 2.5 when f is a quadratic and Boolean function ($m = 1$). For the non-Boolean case ($m > 1$) neither implies the other. We complete this historical development—our Theorem 3.1 generalizes Theorem 2.5. On the other hand, it also generalizes Theorem 2.4. Moreover, Theorem 3.1 generalizes a previous generalization of Theorem 2.4, catapulting it to the *differentially δ-uniform* scenario, proved in the Ph.D. dissertation (2020) [111]. In this respect, our next theorem answers the question, given a function F of class differentially δ-uniform, how should the function G be so that the sum $F + G$ is of the same class as F. The diagram below shows the historical development of the Switching Method; for a collection of new switching neighbors we proved, see [111]. As for *differentially (c,δ)-uniform functions*, $c = 1$ corresponds to the usual derivative, given in Definition I in Subsection 1.1. While $c \neq 1$ corresponds to a convenient modification of the derivative called c-derivative, which also has the property of being linear.

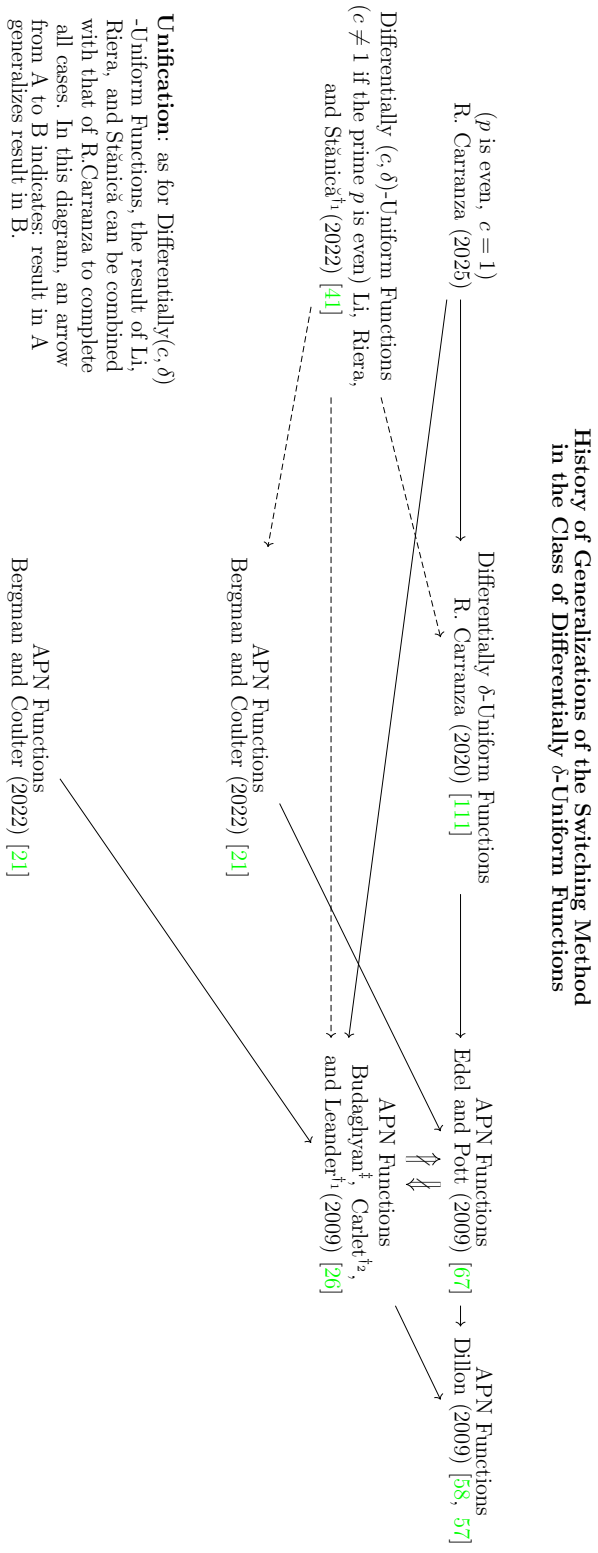

Figure 1: $\dagger_1$: George Boole International Prize, $\dagger_2$: Mathematics in France Leader Award, ‡: Emil Artin Junior Prize in Mathematics.

Theorem 3.1 (Differentially Uniform Version-II) *Assume that* $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ *is a differentially* δ*-uniform function. Let* m *a divisor of* n, $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$, $\Delta_a f$ *a derivative of* f, $A_{\Delta_a f(z)} = \{x \in \mathbb{F}_{2^n}; \Delta_a f(x) = \Delta_a f(z)\}$, $\check{A}_{\Delta_a f(z)} = \mathbb{F}_{2^n} - A_{\Delta_a f(z)}$, *and* $H(x) = F(x) + f(x)$ *on* $\mathbb{F}_{2^n}$. *Then:* H *is a differentially* δ*-uniform function* $\iff$ *For all* $a \neq 0$ *and* $\delta + 2$ *mutually distinct values distributed in two non-empty sets* x_i*'s* $\in A_{\Delta_a f(x_{i_0})}$, *for some* $x_{i_0} \in \mathbb{F}_{2^n}$, *and* x'_j*'s* $\in \check{A}_{\Delta_a f(x_{i_0})}$, $\big(\Delta_a F(x_i) + \Delta_a F(x'_j) = \omega_{x'_j}(x_{i_0})$, *where* $\omega_{x'_j}(x_{i_0}) \in \mathbb{F}^*_{2^m}$, *implies* $\Delta_a f(x_i) + \Delta_a f(x'_j) \neq \omega_{x'_j}(x_{i_0})\big)$.

Proof. We shall prove the contrapositive of both statements.
Case 1: H is not *differentially* δ*-uniform* $\Longrightarrow\big(\exists\ a \neq 0$ and $\delta + 2$ mutually distinct values distributed in two non-empty sets x_i's $\in A_{\Delta_a f(x_{i_0})}$, for some x_{i_0} in $\mathbb{F}_{2^n}$, and x'_j's $\in \check{A}_{\Delta_a f(x_{i_0})}$, such that $\big(\Delta_a F(x_i) + \Delta_a F(x'_j) = \omega_{x'_j}(x_{i_0})$ and $\Delta_a f(x_i) + \Delta_a f(x'_j) = \omega_{x'_j}(x_{i_0})$, where $\omega_{x'_j}(x_{i_0}) \in \mathbb{F}^*_{2^m}\big)\big)$. *Proof.* H is not *differentially* δ*-uniform*, then $\exists\ a \neq 0$, $b \in \mathbb{F}_{2^n}$ such that the equation $\Delta_a H(x) = b$ has a solution set S_H with $|S_H| \geq \delta + 2$. If we assume that all solutions belong to the nonempty set $A_{\Delta_a f(\tilde{x})}$, for some $\tilde{x} \in \mathbb{F}_{2^n}$. Then, for any $x \in S_H$, $\Delta_a H(x) = \Delta_a F(x) + \Delta_a f(x) = \Delta_a F(x) + \Delta_a f(\tilde{x}) = b$. Given $b - \Delta_a f(\tilde{x})$, we have that $S_H \subseteq S_F$, where S_F is the solution set of the equation for the uniform differentiability of function F, $b - \Delta_a f(\tilde{x}) = \Delta_a F(x)$. Thence $|S_F| \geq \delta + 2$ solutions, which contradicts the fact that F is *differentially* δ*-uniform*. That is, S_H cannot be contained in only one set like $A_{\Delta_a f(\tilde{x})}$. Thus, $\exists\ x_{i_0} \in S_H - A_{\Delta_a f(\tilde{x})}$ such that $S_H \cap A_{\Delta_a f(x_{i_0})} \neq \emptyset$ and $S_H \cap \check{A}_{\Delta_a f(x_{i_0})} \neq \emptyset$. Then, $\forall x_i \in S_H \cap A_{\Delta_a f(x_{i_0})}$, $\forall x'_j \in S_H \cap \check{A}_{\Delta_a f(x_{i_0})}$:

$$\Delta_a F(x_i) = b - \Delta_a f(x_{i_0}) \text{ and } \Delta_a f(x_i) = \Delta_a f(x_{i_0}), \text{ and} \qquad (1)$$

$$\Delta_a F(x'_j) = b - \lambda_{x'_j} \text{ and } \Delta_a f(x'_j) = \lambda_{x'_j}, \text{ where } \lambda_{x'_j} \neq \Delta_a f(x_{i_0}). \qquad (2)$$

Adding the systems of equations (1) and (2), there are $a \neq 0$ and $\delta + 2$ mutually distinct values (belonging to S_H) x_i's $\in A_{\Delta_a f(x_{i_0})} \neq \emptyset$ and x'_j's $\in \check{A}_{\Delta_a f(x_{i_0})} \neq \emptyset$, for some x_{i_0} in $\mathbb{F}_{2^n}$, with: $\Delta_a F(x_i) + \Delta_a F(x'_j) + \omega_{x'_j}(x_{i_0}) = 0$ and $\Delta_a f(x_i) + \Delta_a f(x'_j) - \omega_{x'_j}(x_{i_0}) = 0$, where $\omega_{x'_j}(x_{i_0}) = \Delta_a f(x_{i_0}) + \Delta_a f(x'_j) \in \mathbb{F}^*_{2^m}$.
Case 2: Conversely, $\big($there exists $a \neq 0$ and $\delta + 2$ mutually distinct values distributed in two non-empty sets x_i's $\in A_{\Delta_a f(x_{i_0})}$, for some x_{i_0} in $\mathbb{F}_{2^n}$, and x'_j's $\in \check{A}_{\Delta_a f(x_{i_0})}$, such that $\big(\Delta_a F(x_i) + \Delta_a F(x'_j) = \omega_{x'_j}(x_{i_0})$ and $\Delta_a f(x_i) + \Delta_a f(x'_j) = \omega_{x'_j}(x_{i_0})$, where $\omega_{x'_j}(x_{i_0}) \in \mathbb{F}^*_{2^m}\big)\big) \Longrightarrow$ H is not *differentially* δ*-uniform. Proof.* Let $\Delta_a F(x_{i_0})$ be equal to b, for some $b \in \mathbb{F}_{2^n}$. Substituting this into the equation for all the $\delta + 2$ values x_i, x'_j from the hypothesis, $\Delta_a F(x_i) + \Delta_a F(x'_j) = \omega_{x'_j}(x_{i_0})$, we have: $\Delta_a F(x'_j) = -b + \omega_{x'_j}(x_{i_0})$, $\forall x'_j \in \check{A}_{\Delta_a f(x_{i_0})}$. Thus, $\Delta_a F(x_i) + \Delta_a F(x'_j) = \Delta_a F(x_i) - b + \omega_{x'_j}(x_{i_0}) = \omega_{x'_j}(x_{i_0})$, $\forall x_i \in A_{\Delta_a f(x_{i_0})}$.

Then, $\Delta_a F(x_i) = b$, $\forall x_i \in A_{\Delta_a f(x_{i_0})}$. Then: $\Delta_a H(x_i) = \Delta_a F(x_i) + \Delta_a f(x_i) = b + \Delta_a f(x_{i_0})$, $\forall x_i \in A_{\Delta_a f(x_{i_0})}$ and $\Delta_a H(x'_j) = \Delta_a F(x'_j) + \Delta_a f(x'_j) = \Delta_a F(x'_j) + \omega_{x'_j}(x_{i_0}) - \Delta_a f(x_i) = -(b + \Delta_a f(x_{i_0}))$, $\forall x'_j \in \check{A}_{\Delta_a f(x_{i_0})}$. Thus the $\delta + 2$ values x_i's, x'_j's solve the equation $\Delta_a H(x) = b + \Delta_a f(x_{i_0})$ (in characteristic 2), and H as such can not be *differentially δ-uniform.* □

For $n \geq 2$ (the non-trivial case), Theorem 2.5 is a corollary of Theorem 3.1.

Corollary 3.2 *Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be a quadratic APN function, let $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$ be a quadratic function where m is a divisor of n, $n \geq 2$, $\varphi_F(x, a) = F(x) + F(x + a) + F(a) + F(0)$, and $\varphi_f(x, a) = f(x) + f(x + a) + f(a) + f(0)$. If for every $a \in \mathbb{F}_{2^n}^*$ there exists a linear function $l_a : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$ such that:*

1). $\varphi_f(x, a) = l_a(\varphi_F(x, a))$ on $\mathbb{F}_{2^n} \times \{a\}$,

2). For every $u \in \mathbb{F}_{2^m}^*$, if $\varphi_F(x, a) = u$ for some $x \in \mathbb{F}_{2^n}$ then $l_a(u) \neq u$.

Then $F + f$ is an APN function.

Proof. The prove is given by application of Theorem 3.1. Suppose that $\Delta_a F(x_i) + \Delta_a F(x'_j) = w$ for some $w \in \mathbb{F}_{2^m}^*$. Adding $\Delta_a F(0)$, two times, we have that $\varphi_F(x_i, a) + \varphi_F(x'_j, a) = w$. Since F is quadratic, $\varphi_F(x_i, a)$ is linear in its first variable. Thus, $\varphi_F(x_i + x'_j, a) = w$. By the condition (2) of the linear function l_a in the hypothesis, we have that $l_a(w) \neq w$. By application of the function l_a and its linearity, and by the condition (1) in the hypothesis, we have: $\varphi_f(x_i, a) + \varphi_f(x'_j, a) = l_a(\varphi_F(x_i, a) + \varphi_F(x'_j, a)) = l_a(w)$. Thus, adding $\Delta_a f(0)$, two times into the previous equation, we have that $\Delta_a f(x_i) + \Delta_a f(x'_j) = l_a(w)$. Then $\Delta_a f(x_i) + \Delta_a f(x'_j) = l_a(w) \neq w$, we done. □

4 Novel Approach of Differentially $\{4, 6, 8\}$-Uniform Permutations

Now we present one of our main results using a different method that we introduce in this article. Our approach is distinct from the switching method of Dillon. The method of Dillon applies the switching method to find switching neighbors—only the case when U is a subgroup of a particular form has been developed—in the narrow sense conform to the Definition 2.2 (we too have made a contribution with new switching neighbors in that direction, see pages 38 to 46 in [111]). Whereas our way can be understood as us applying a perturbation along the independent variable.

We give new differentially 4-uniform polynomial permutations in even degree field extension. Furthermore, we provide whole families of such functions which also have closed forms. Thus, we make a significant contribution to an

open problem of Bracken and Leander. **Note.** It is worth noting that to offer good resistance to differential cryptanalysis, it is not a weakness to have a differential delta-uniformity of $\Delta(f) = 4$ (the best candidates are $\Delta(f) = 4, 6, 8$, i.e. $\delta = \Delta(f) = \Delta_f$ very small) without reaching $\delta = 2$, since history has shown that components (with an extreme algebraic structure) in a cipher have introduced vulnerability [12]. We must consider the following two features about the function f: have a very small $\Delta(f)$, and for each input difference $a \neq 0$, it must have the number of output differences b that occur Δ_f times, $|\{(\text{an output difference}) \ b \in \mathbb{F}_{2^n}; \delta_f(a, b) = \Delta_f\}| = \omega_{\Delta_f}$, also small, in this sense, to have a behavior more similar to an APN function. That is, for each fixed $a \neq 0$, the probability of obtaining a pair (a, b) such that $\delta_f(a, b) = \Delta_f$ is small. And to prevent the block cipher from *algebraic attacks*, the algebraic degree should be not too small and not too large (so it should not be $n - 1$). Our functions are as required but we also have an optimal algebraic degree, and furthermore, we obtain families with all algebraic degrees (see Section 5).

Permutations, F, with low differential uniformity ($\Delta(F) \leq 8$) can be used as S-boxes of symmetric cryptosystems as they have good resistance to differential attacks. The AES (advanced encryption standard) uses the multiplicative inverse function, which is a differential 4-uniform function. To improve AES or to find new standards, we need differential 4-uniform functions. Finding differential 4-uniform permutation functions with high nonlinearity on even degree fields is a challenge. In view of these reasons, in [18], Bracken and Leander listed an open problem:

Open Problem 2. Find more highly nonlinear permutations of even degree fields with differential uniformity of 4.

Definition 4.1 *[138] It is known that if f a permutation on $\mathbb{F}_{2^n}$, then its algebraic degree satisfies that $d^0(f) \leq n-1$. If $d^0(f) = n-1$, the permutation f is said to have optimal algebraic degree (o.a.d.).*

Charpin and Kyureghyan (2017) in [39] discovered a class of sporadic binomials permutations with low differential uniformity ($\delta = 4$, 6). Yu and Wang built differential 6 and 4-uniform permutations from the inverse function [136]. Then Qu et al. [109] gives us a survey of differentially 4-uniform permutations families, even without the requirement of high nonlinearity, see also Carlet [32] and Zha [138].

4.1 The Granted by the Underlying Space $\mathbb{F}_2^n$ Method

We construct new families of differentially 4-uniform permutations in this article in even degree field extensions. Our functions are given through an explicit formula in polynomial representation having quite desirable shapes. The other strategic feature of our polynomials is that their coefficients are precisely in the

prime field $\mathbb{F}_2$, on account of Tr_n^1. This requirement increased the difficulty for us in the search for these functions, and this, endows them suitable in terms of computational implementation. **Remark.** As if it were a gift, these novel functions are provided exclusively by the field itself, determined by bases of the host field, for these reasons we name this method as *generatrix granted by the underlying space* $\mathbb{F}_2^n$, consult Theorems 4.6, 4.12, and 5.2.

Theorem 4.2 (Differentially $\{4, 6, 8\}$-Uniform Permutations) *There is a linearly independent set of $\mathbb{F}_2^n$, $(a_i)_{i=1}^{n-1}$, whith $Tr_n^1(a_1) = \cdots = Tr_n^1(a_{n-1}) = 0$, such that:*
1) If n odd and $\gcd(n,k) = 1$, then the family of functions:

$$f(x) = f_{k,g}(x) := x^{2^k+1} + (x^{2^k} + x + 1)Tr_n^1(a_1x)\cdots Tr_n^1(a_gx),$$

is differentially 4-uniform permutation on $\mathbb{F}_{2^n}$. Moreover:
If $g = n-1$, then $d^0(f)$ is optimal and $nl(f) \geq nl(x^{2^k+1}) - 2 = 2^{n-1} - 2^{\frac{n-1}{2}} - 2$.
If $g = n-2$, then $d^0(f)$ is optimal too and $nl(f) \geq 2^{n-1} - 2^{\frac{n-1}{2}} - 4$.
2) If $n = 2m$, where m is odd and $\gcd(n,k') = 2$, then the family of functions:

$$G_{k',g}(x) := x^{2^{k'}+1} + (x^{2^{k'}} + x + 1)Tr_n^1(a_1x)\cdots Tr_n^1(a_gx),$$

is differentially γ-uniform permutation on $\mathbb{F}_{2^n}$, where $\gamma \in \{4, 6, 8\}$, $g \in \{n-2, n-1\}$. Moreover:
If $g = n-1$, then $d^0(G_{k',g})$ is optimal and $nl(G_{k',g}) \geq nl(x^{2^{k'}+1}) - 2$.
If $g = n-2$, then $d^0(G_{k',g})$ is optimal and $nl(G_{k',g}) \geq nl(x^{2^{k'}+1}) - 4$.
3) If n odd and $\gcd(n,i) = 1$, then the family of functions:

$$\begin{aligned} K_{i,g}(x) := x^{2^{2i}-2^i+1} + (x^{2^{2i}-2^i} + x^{2^{2i}-(2)2^i+1} + x^{2^{2i}-(2)2^i} + x^{2^{2i}-(3)2^i+1} + \\ x^{2^{2i}-(3)2^i} + \cdots + x^{2^i+1} + x^{2^i} + x + 1)Tr_n^1(a_1x)\cdots Tr_n^1(a_gx), \end{aligned}$$

is differentially 4-uniform permutation on $\mathbb{F}_{2^n}$. Furthermore:
If $g = n-1$, then $nl(K_{i,g}) \geq nl(F) - 2 = 2^{n-1} - 2^{\frac{n-1}{2}} - 2$ with $F(x) = x^{2^{2i}-2^i+1}$, and $d^0(K_{i,g})$ is optimal.
If $g = n-2$, then $d^0(K_{i,g})$ is optimal and $nl(K_{i,g}) \geq 2^{n-1} - 2^{\frac{n-1}{2}} - 4$.
4) If n even, then the families of functions $\tilde{I}_{\tilde{x}_0,0}$ and $\tilde{I}_{\tilde{x}_0}$ are differentially 4-uniform permutations on $\mathbb{F}_{2^n}$, $nl(\tilde{I}_{\tilde{x}_0}) \geq nl(\mathfrak{Y}) - 2 = 2^{n-1} - 2^{\frac{n}{2}} - 2$ (it can also be seen that there is a subclass for which the quantity $2^{n-1} - 2^{\frac{n}{2}}$ is reached), and both $d^0(\tilde{I}_{\tilde{x}_0,0})$ and $d^0(\tilde{I}_{\tilde{x}_0})$ are optimal.

Proof. We will first demonstrate more general results. Then we will obtain our results as consequences as particular cases. Following the sequence of propositions in this section followed by those of sections 5 and 6.

Lemma 4.3 *There exists a linearly independent set of* $\mathbb{F}_2^n$, $(a_i)_{i=1}^{n-1}$, *such that* $Tr_n^1(a_1) = \cdots = Tr_n^1(a_{n-1}) = 0$.

Proof. Let $\mathcal{B}^{(n)} = \{1, \alpha, \alpha^2, \cdots, \alpha^{n-1}\}$ be a *basis* over $\mathbb{F}_{2^n}$ with α a *primitive element* of the field. If we select $\mathcal{B}^{(n)}$ such that it contains elements whose trace is 1 then we can consider the maximal subsets of $\mathcal{B}^{(n)}$: $\{\alpha^{e_1}, \cdots, \alpha^{e_p}\}$ and $\{\alpha^{e_{p+1}}, \cdots, \alpha^{e_n}\}$, such that $Tr_n^1(\alpha^{e_i}) = 1$, for $i \leq p$, and $Tr_n^1(\alpha^{e_i}) = 0$, for $p < i$, for some p. Thus the set of $n-1$ vectors $\{\alpha^{e_1} + \alpha^{e_2}, \cdots, \alpha^{e_1} + \alpha^{e_p}, \alpha^{e_{p+1}}, \cdots, \alpha^{e_n}\}$ are *linearly independent* (because of definition of linear independence) and have trace 0. □

Lemma 4.4 *There exist a basis in* $\mathbb{F}_2^n$, $(a_i)_{i=1}^n$, *where its basis vectors have trace 1.*

Proof. Half of the elements in the vector space $\mathbb{F}_2^n$ have trace equal to 1. Any vector v of trace 1 can be spanned by a linear combination of basis vectors because taking the trace of v is the same as taking the trace of the basis vectors. As such, there must exist at least one vector $\alpha^{e_1} \in \mathcal{B}^{(n)}$ such that $Tr_n^1(\alpha^{e_1}) = 1$.

Consider the maximal subsets of $\mathcal{B}^{(n)}$: $\{\alpha^{e_1}, \cdots, \alpha^{e_p}\}$ and $\{\alpha^{e_{p+1}}, \cdots, \alpha^{e_n}\}$, such that $Tr_n^1(\alpha^{e_i}) = 1$, for $i \leq p$, and $Tr_n^1(\alpha^{e_i}) = 0$, for $p < i$, for some p. Then the set of n vectors $\{\alpha^{e_1}, \alpha^{e_2}, \cdots, \alpha^{e_p}, \alpha^{e_1} + \alpha^{e_{p+1}}, \cdots, \alpha^{e_1} + \alpha^{e_n}\}$ is also a *basis* in $\mathbb{F}_2^n$ where its elements have trace 1. □

Lemma 4.5 *Let* $c \in \mathbb{F}_{2^n}$, $i_1, i_2, \cdots, i_l \in \mathbb{N}$, $\mathcal{P} \in \mathbb{F}_2[x_{i_1}, x_{i_2}, \cdots, x_{i_{j+l}}]$ *a polynomial with coefficients in* $\mathbb{F}_2$, *and* $Tr_n^1(a_1) = \cdots = Tr_n^1(a_j) = 0$. *Then, the equation*

$$x + \mathcal{P}(tr(a_1 x), \cdots, Tr_n^1(a_j x), Tr_n^1(x^{2^{i_1}+1} + x\, tr(1)), \cdots, Tr_n^1(x^{2^{i_l}+1} + x\, Tr_n^1(1))) = c,$$

has only one solution,

$$x = c + \mathcal{P}(tr(a_1 c), \cdots, Tr_n^1(a_j c), Tr_n^1(c^{2^{i_1}+1} + c\, Tr_n^1(1)), \cdots, Tr_n^1(c^{2^{i_l}+1} + c\, Tr_n^1(1))).$$

Proof. **Uniqueness:** Let $\phi(x) := x + P(x)$, where $P(x) := \mathcal{P}(Tr_n^1(a_1 x), \cdots, Tr_n^1(a_j x), Tr_n^1(x^{2^{i_1}+1} + x\, Tr_n^1(1)), \cdots, Tr_n^1(x^{2^{i_l}+1} + x\, Tr_n^1(1)))$. The equation for x, $\phi(x) = c$, implies $x = c + P(x)$, where the algebraic expression $P(x)$ is Boolean, i.e. $P(x) \in \{0, 1\}, \forall x \in \mathbb{F}_{2^n}$. Then, the equation $\phi(x) = c$, has only two possible solutions, c and $c+1$. If x_0 is a solution for that equation, then x_0+1 is not a solution: $\phi(x_0+1) = x_0+1+P(x_0+1) = x_0+P(x_0)+1 = \phi(x_0)+1 \neq \phi(x_0) = c$, because of the identity $P(x+1) = P(x)$ on $\mathbb{F}_{2^n}$, in the next paragraph. Then the solution for this equation is unique. Identity $P(x+1) = P(x)$

on $\mathbb{F}_{2^n}$: $P(x+1) = \mathcal{P}(Tr_n^1(a_1x), \cdots, Tr_n^1(a_jx), Tr_n^1(x^{2^{i_1}+1} + 1 + xTr_n^1(1) + Tr_n^1(1)), \cdots, Tr_n^1(x^{2^{i_l}+1}+1+xTr_n^1(1)+Tr_n^1(1))) = \mathcal{P}(Tr_n^1(a_1x), \cdots, Tr_n^1(a_jx), Tr_n^1(x^{2^{i_1}+1} + x\,Tr_n^1(1)), \cdots, Tr_n^1(x^{2^{i_l}+1} + x\,Tr_n^1(1))) = P(x)$, on $\mathbb{F}_{2^n}$, because of $Tr_n^1(a_1) = \cdots = Tr_n^1(a_j) = 0$, and $Tr_n^1(x+1)^{2^k+1} = Tr_n^1(x^{2^k+1}+1)$ on $\mathbb{F}_{2^n}$, $\forall k \in \mathbb{N}$.

Form of the Solution: We consider the following form of the solution, $x = c + P(c)$. If $P(c) = 0$, then $\phi(c+P(c)) = \phi(c) = c+P(c) = c+0 = c$. On the other hand, if $P(c) = 1$, then $\phi(c+P(c)) = \phi(c+1) = \phi(c)+1 = c+P(c)+1 = c+1+1 = c$, as in a previous calculations, where $\phi(x_0+1) = \phi(x_0)+1$. Therefore in both cases $x = c + P(c)$ is the solution for the given equation, $\phi(x) = c$. □

A Closure Property: Lemma 4.5 provides us a new-specific class of involutions (A function h is a *involution* if it is equal to its compositional inverse (its inverse function), $h^{-1} = h$). Theorem 4.6 is true for the case of the sum of traces into the formula to construct f (e.g. when f is of the form $f(x) = F(x + Tr_n^1(a_1x) + Tr_n^1(x^{2^{i_1}+1} + x\,Tr_n^1(1))))$, but it is also true for the product case (f of the form $f(x) = F(x + Tr_n^1(a_1x)Tr_n^1(x^{2^{i_1}+1} + x\,Tr_n^1(1))))$, achieving a *closure property* with respect to both operations, an exciting thing in Algebra. Furthermore, Theorem 4.6 does not depend on the δ-parameter, being an influential result in the *Theory of Differentially δ-Uniform Functions*.

Theorem 4.6 (Classes of Differentially γ-Uniform Functions) *Let F be a differentially δ-uniform function, $\mathcal{P}$ belongs to the polynomial ring $\mathbb{F}_2[x_{i_1}, x_{i_2}, \cdots, x_{i_{j+l}}]$, and $Tr_n^1(a_1) = \cdots = Tr_n^1(a_j) = 0$ over $\mathbb{F}_{2^n}$. Then, the family of functions $f(x) = F(x + \mathcal{P}(Tr_n^1(a_1x), \cdots, Tr_n^1(a_jx), Tr_n^1(x^{2^{i_1}+1} + x\,Tr_n^1(1)), \cdots, Tr_n^1(x^{2^{i_l}+1} + x\,Tr_n^1(1))))$ is differentially γ-uniform, where $\delta \leq \gamma \leq 2\delta$, $j+l \geq 1$, and each $i_k \in \mathbb{N}$.*

Proof. Given $a \neq 0$, b, both in $\mathbb{F}_{2^n}$, considering the corresponding equation for f to be studied: $\Delta_a f(x) = F(x + P(x) + P(x+a) - P(x) + a) - F(x + P(x)) = b$, where $P(x) := \mathcal{P}(Tr_n^1(a_1x), \cdots, Tr_n^1(a_jx), Tr_n^1(x^{2^{i_1}+1} + x\,Tr_n^1(1)), \cdots, Tr_n^1(x^{2^{i_l}+1} + x\,Tr_n^1(1)))$, the same notation as in the previous Lemma. Since $P(x+a) - P(x)$ is a Boolean function, for $a = 1$, it is possible that the term $P(x+a) - P(x) + a$ becomes zero, then the equation for $b = 0$ is reduced to the following equation, $\Delta_1 f(x) = F(x+P(x)) - F(x+P(x)) = 0$, on $\mathbb{F}_{2^n} \cap \{x \in \mathbb{F}_{2^n};\ P(x+1)+1 = P(x)\}$. **Case** $a \neq 1$. **Subcase** $P(x+a)-P(x) = 0$: The equation $\Delta_a f(x) = b$ becomes: $F(x + P(x) + a) - F(x + P(x)) = b$. Because F is *differentially δ-uniform* over $\mathbb{F}_{2^n}$, this equation has at most δ solutions for the variable $y = x + P(x)$, which will be denoted by $y = y_t$ and $y = y_t + a$, for $1 \leq t \leq \frac{\delta}{2}$. In the following steps we solve the equations in x, $x + P(x) = y$, for each value of y. The equation $x + P(x) = y_t$, by Lemma 4.5, has the unique solution $x = y_t + P(y_t)$, for $1 \leq t \leq \frac{\delta}{2}$.

The equation $x + P(x) = y_t + a$, by Lemma 4.5, has the unique solution $x = y_t + a + P(y_t + a)$, for $1 \leq t \leq \frac{\delta}{2}$. Then, there are at most δ solutions. **Subcase** $P(x + a) - P(x) = 1$: The equation $\Delta_a f(x) = b$ becomes: $F(x+P(x)+a+1)-F(x+P(x)) = b$. Because of F is *differentially δ-uniform* over $\mathbb{F}_{2^n}$, this equation has at most δ solutions for the variable $y = x + P(x)$, which will be denoted by $y = z_t$ and $y = z_t + a + 1$, for $1 \leq t \leq \frac{\delta}{2}$. In the following we will try to solve the equations in x, $x + P(x) = y$, for each value of y. The equation $x + P(x) = z_t$, by Lemma 4.5, has the unique solution $x = z_t + P(z_t)$, for $1 \leq t \leq \frac{\delta}{2}$. The equation $x + P(x) = z_t + a + 1$, by Lemma 4.5, has the unique solution $x = z_t+a+1+P(z_t+a+1) = z_t+a+1+P(z_t+a)$, because of the identity, $P(x+1) = P(x)$, on $\mathbb{F}_{2^n}$, for $1 \leq t \leq \frac{\delta}{2}$. Then, there are at most δ solutions. **Case** $a = 1$. $\Delta_1 f(x) = F(x+P(x)+1)-F(x+P(x)) = b$, because of the identity, $P(x+1) = P(x)$ on $\mathbb{F}_{2^n}$, this equation can be treated as the equations that appear in the case for $a \neq 1$. So the equation $\Delta_1 f(x) = b$ has at most δ solutions. In conclusion, for any $a \neq 0$, b, both in $\mathbb{F}_{2^n}$, the equation $\Delta_a f(x) = b$ attains a total of at most 2δ solutions in $\mathbb{F}_{2^n}$. □

For any $a \in \mathbb{F}_{2^n}$, let $S_a = \{x \in \mathbb{F}_{2^n};\, Tr_n^1(ax) = 0\}$ its corresponding $\mathbb{F}_2$-vector subspace of $\mathbb{F}_{2^n}$, and the set $H_a = \{x \in \mathbb{F}_{2^n};\, Tr_n^1(ax) = 1\}$ its hyperplane, respectively. For $a \neq 0$, $\dim S_a = n - 1$. We can show the following lemma:

Lemma 4.7 *Let $a_1 \neq a_2$ two nonzero elements in $\mathbb{F}_{2^n}$. Then the intersections $S_{a_1} \cap S_{a_2}$, $S_{a_1} \cap H_{a_2}$, $H_{a_1} \cap S_{a_2}$, and $H_{a_1} \cap H_{a_2}$ form a partition of $\mathbb{F}_{2^n}$, such that: $|S_{a_1} \cap S_{a_2}| = |S_{a_1} \cap H_{a_2}| = |H_{a_1} \cap S_{a_2}| = |H_{a_1} \cap H_{a_2}| = 2^{n-2}$.*

Lemma 4.8 *Let $\{a_i \in \mathbb{F}_{2^n};\, i = 1, 2, 3\}$ be a $\mathbb{F}_2$-linearly independent set of $\mathbb{F}_2^n$, such that $|S_{a_i} \cap S_{a_j}| = |\{x \in \mathbb{F}_{2^n};\, Tr_n^1(a_i x) = Tr_n^1(a_j x) = 0\}| = 2^{n-2}$, for all $i \neq j$. Then, the intersections $S_{a_1} \cap S_{a_2} \cap S_{a_3}$, $S_{a_i} \cap S_{a_j} \cap H_{a_k}$, $S_{a_i} \cap H_{a_j} \cap H_{a_k}$, and $H_{a_1} \cap H_{a_2} \cap H_{a_3}$ form a partition of $\mathbb{F}_{2^n}$, such that: $|S_{a_1} \cap S_{a_2} \cap S_{a_3}| = |S_{a_i} \cap S_{a_j} \cap H_{a_k}| = |S_{a_i} \cap H_{a_j} \cap H_{a_k}| = |H_{a_1} \cap H_{a_2} \cap H_{a_3}| = 2^{n-3}$, for all i, j, k different from each other.*

Proof. We denote by $\tilde{t}_{i,j,k} = \{x \in \mathbb{F}_{2^n};\, Tr_n^1(a_1 x) = i,\, Tr_n^1(a_2 x) = j, Tr_n^1(a_3 x) = k\}$, and $t_{i,j,k} = |\tilde{t}_{i,j,k}|$, for any $(i,\, j,\, k) \in \mathbb{F}_2^3$. From $\{a_i\}_{i=1}^3$ linearly independent, $a_1 + a_2 + a_3 \neq 0$, $|S_{a_1+a_2+a_3} = \{x \in \mathbb{F}_{2^n};\, Tr_n^1(a_1 x) + Tr_n^1(a_2 x) = Tr_n^1(a_3 x)\}| = 2^{n-1}$. The set $\{\tilde{t}_{0,0,0},\, \tilde{t}_{0,1,1},\, \tilde{t}_{1,0,1},\, \tilde{t}_{1,1,0}\}$ defines a partition of $S_{a_1+a_2+a_3}$, then $t_{0,0,0} + t_{0,1,1} + t_{1,0,1} + t_{1,1,0} = |S_{a_1+a_2+a_3}| = 2^{n-1}$.
Besides, the set $\{\tilde{t}_{0,0,1},\, \tilde{t}_{0,1,0},\, \tilde{t}_{1,0,0},\, \tilde{t}_{1,1,1}\}$ defines a partition of $H_{a_1+a_2+a_3} = \{x \in \mathbb{F}_{2^n};\, Tr_n^1(a_1 x)+Tr_n^1(a_2 x) = Tr_n^1(a_3 x)+1\}$, then $t_{0,0,1}+t_{0,1,0}+t_{1,0,0}+t_{1,1,1} = |H_{a_1+a_2+a_3}| = 2^n - |S_{a_1+a_2+a_3}| = 2^{n-1}$.

From the hypothesis $|S_{a_i} \cap S_{a_j}| = 2^{n-2}$ we have a common cardinality: $|S_{a_i} \cap H_{a_j}| = |H_{a_i} \cap S_{a_j}| = |H_{a_i} \cap H_{a_j}| = 2^{n-2}$, for all $i \neq j$ in {1, 2, 3}. Then, taking into account the partitions, we have the following system of 14 linear equations (in order from left to right) in the 8 variables, $t_{i,j,k}$:

$t_{0,0,0} + t_{0,0,1} = |S_{a_1} \cap S_{a_2}| = 2^{n-2}$, $t_{0,0,0} + t_{1,0,0} = |S_{a_2} \cap S_{a_3}| = 2^{n-2}$,
$t_{0,0,0} + t_{0,1,0} = |S_{a_1} \cap S_{a_3}| = 2^{n-2}$, $t_{0,1,1} + t_{0,1,0} = |S_{a_1} \cap H_{a_2}| = 2^{n-2}$,
$t_{0,1,1} + t_{1,1,1} = |H_{a_2} \cap H_{a_3}| = 2^{n-2}$, $t_{0,1,1} + t_{0,0,1} = |S_{a_1} \cap H_{a_3}| = 2^{n-2}$,
$t_{1,0,1} + t_{1,0,0} = |H_{a_1} \cap S_{a_2}| = 2^{n-2}$, $t_{1,0,1} + t_{0,0,1} = |S_{a_2} \cap H_{a_3}| = 2^{n-2}$,
$t_{1,0,1} + t_{1,1,1} = |H_{a_1} \cap H_{a_3}| = 2^{n-2}$, $t_{1,1,0} + t_{1,1,1} = |H_{a_1} \cap H_{a_2}| = 2^{n-2}$,
$t_{1,1,0} + t_{0,1,0} = |H_{a_2} \cap S_{a_3}| = 2^{n-2}$, $t_{1,1,0} + t_{1,0,0} = |H_{a_1} \cap S_{a_3}| = 2^{n-2}$,
$t_{0,0,0} + t_{0,1,1} + t_{1,0,1} + t_{1,1,0} = |S_{a_1+a_2+a_3}| = 2^{n-1}$,
$t_{0,0,1} + t_{0,1,0} + t_{1,0,0} + t_{1,1,1} = |H_{a_1+a_2+a_3}| = 2^{n-1}$.
$S_{a_1} \cap S_{a_2} \cap S_{a_3}$ is an $\mathbb{F}_2$-vector subspace of $S_{a_i} \cap S_{a_j}$, for any $i \neq j$, of one less or same dimension, namely $|S_{a_1} \cap S_{a_2} \cap S_{a_3}| = 2^{n-2}$ (or 2^{n-3}). Then, from the first three equations, $t_{0,0,1} = t_{1,0,0} = t_{0,1,0} = 0$ or 2^{n-3}, respectively. Substituting in the equation (14): $t_{1,1,1} = 2^{n-1}$ or 2^{n-3}, respectively. Now, substituting $t_{1,1,1} = 2^{n-1}$ in the equation (5): $t_{0,1,1} = 2^{n-2} - 2^{n-1}$ (contradiction with $t_{0,1,1} \in \mathbb{N} \cup \{0\}$). Then $t_{1,1,1} = 2^{n-3}$ and $t_{0,1,1} = 2^{n-2} - 2^{n-3} = 2^{n-3}$. Besides, from the equation (14), $3\,t_{0,0,1} + 2^{n-3} = 2^{n-1}$, i.e. $t_{0,0,1} = t_{1,0,0} = t_{0,1,0} = 2^{n-3}$. Doing back substitution. From the first equation, $t_{0,0,0} = 2^{n-3}$. From equations (7), (12): $t_{1,0,1} = |H_{a_1} \cap S_{a_2}| - t_{1,0,0} = 2^{n-3}$, $t_{1,1,0} = |H_{a_1} \cap S_{a_3}| - t_{1,0,0} = 2^{n-3}$. All the equations are satisfied. In summary $t_{i,j,k} = 2^{n-3}$. □

Our next top-tier theorem is a cornerstone whose scope encompasses all of finite field theory working for fields of even as well as odd degree.

Theorem 4.9 (Global Property of Partition of Finite Fields by Affine Functions) *Let $(a_i)_{i=1}^{n-1}$ a linearly independent set of $\mathbb{F}_2^n$, the sets $S_{a_i} = \text{Kernel}(tr(a_i x)) = \{x \in \mathbb{F}_{2^n};\, Tr_n^1(a_i x) = 0\}$ their corresponding $\mathbb{F}_2$-vector subspaces of $\mathbb{F}_{2^n}$, and $H_{a_i} = \{x \in \mathbb{F}_{2^n};\, Tr_n^1(a_i x) = 1\}$ their affine subspaces. Then, the intersections of the form $S_{a_{i_1}} \cap \cdots \cap S_{a_{i_{n-1}}}$, $H_{a_{i_1}} \cap S_{a_{i_2}} \cap \cdots \cap S_{a_{i_{n-1}}}$, $H_{a_{i_1}} \cap H_{a_{i_2}} \cap S_{a_{i_3}} \cap \cdots \cap S_{a_{i_{n-1}}}, \cdots$, and $H_{a_{i_1}} \cap \cdots \cap H_{a_{i_{n-1}}}$ form a partition of $\mathbb{F}_{2^n}$. Besides, $|U_{a_{i_1}} \cap \cdots \cap U_{a_{i_{n-1}}}| = 2^{n-(n-1)} = 2^1$, where $U_{a_{i_1}} \cap \cdots \cap U_{a_{i_{n-1}}}$ denotes any partition element of $\mathbb{F}_{2^n}$.*

Proof. It is sufficient to demonstrate that $|U_{a_{i_1}} \cap \cdots \cap U_{a_{i_k}}| = 2^{n-k}$, for all $U_{a_{i_1}}, \cdots U_{a_{i_k}}$, for all $1 \leq k \leq n-1$. In particular the theorem. We proceed by *induction*. We use the Lemmas 4.7 and 4.8 for some beginning values for n:
For $n = 2$: $|U_{a_{i_1}}| = 2^{n-1} = 2^1$.
For $n = 3$: $|U_{a_{i_1}}| = 2^{n-1} = 2^2$; $|U_{a_{i_1}} \cap U_{a_{i_2}}| = 2^{n-2} = 2^1$.
For $n = 4$: $|U_{a_{i_1}}| = 2^{n-1} = 2^3$; $|U_{a_{i_1}} \cap U_{a_{i_2}}| = 2^{n-2} = 2^2$; $|U_{a_{i_1}} \cap U_{a_{i_2}} \cap U_{a_{i_3}}| = 2^{n-3} = 2^1$.
The induction hypothesis: Supposing true up to $K = n-2$, i.e. let $\{a_{i_1}, \cdots, a_{i_{n-2}}\}$ a *linearly independent set*, such that $|U_{a_{i_1}} \cap \cdots \cap U_{a_{i_k}}| = 2^{n-k}$, for all $1 \leq k \leq n-2$.
Induction Step: To demonstrate for $K+1 = n-1$, $|U_{a_{i_1}} \cap \cdots \cap U_{a_{i_{n-1}}}| = 2^{n-(n-1)} = 2^1$, for all $U_{a_{i_1}} \cap \cdots \cap U_{a_{i_{n-1}}}$:

Let $\tilde{t}_{l_{i_1},\cdots,l_{i_k}} := \{x \in \mathbb{F}_{2^n};\, Tr_n^1(a_{i_1}x) = l_{i_1}, \cdots,\, Tr_n^1(a_{i_k}x) = l_{i_k}\}$, and $t_{l_{i_1},\cdots,l_{i_k}} = |\tilde{t}_{l_{i_1},\cdots,l_{i_k}}|$, $\forall\ (l_{i_1},\cdots,l_{i_k}) \in \mathbb{F}_2^k$, where $1 \leq k \leq n-1$. Systems of equations:
Case-I: Trace Values That Sum to Zero: By the induction hypothesis $\{a_i\}_{i=1}^{n-1}$ are linearly independent, $a_1+\cdots+a_{n-1} \neq 0$. Then $2^{n-1} = |S_{a_1+\cdots+a_{n-1}} = \{x \in \mathbb{F}_{2^n};\, Tr_n^1((a_1+\cdots+a_{n-1})x) = Tr_n^1(a_1x)+\cdots+Tr_n^1(a_{n-1}x) = l_1+\cdots+l_{n-1} = 0\}| = t_{0_{i_1},\cdots,0_{i_{n-1}}} + \sum_{(l_{i_1},\cdots,l_{i_{n-1}})\in\mathbb{F}_2^{n-1}\ has\ even\ 1's} t_{l_{i_1},\cdots,l_{i_{n-1}}}$.
Case-II: Trace Values That Sum to One: Also, $2^{n-1} = 2^n - |S_{a_1+\cdots+a_{n-1}}| = |H_{a_1+\cdots+a_{n-1}} = \{x \in \mathbb{F}_{2^n};\, Tr_n^1((a_1+\cdots+a_{n-1})x) = l_1+\cdots+l_{n-1} = 1\}| = \sum_{(l_{i_1},\cdots,l_{i_{n-1}})\in\mathbb{F}_2^{n-1}\ has\ odd\ 1's} t_{l_{i_1},\cdots,l_{i_{n-1}}}$.
To define by $\bar{t}_{l_{i_{k+1}},\cdots,l_{i_{n-1}}} := t_{l_{i_1},\cdots,l_{i_k},l_{i_{k+1}},\cdots,l_{i_{n-1}}}$, where $l_{i_1},\cdots,l_{i_k}$ are the fixed values, $l_{i_{k+1}},\cdots,l_{i_{n-1}}$ are the free values. Then we have the identity $\sum_{(l_{i_{k+1}},\cdots,l_{i_{n-1}})\in\mathbb{F}_2^{n-1-k}} \bar{t}_{l_{i_{k+1}},\cdots,l_{i_{n-1}}} = t_{l_{i_1},\cdots,l_{i_k}}$. The induction hypothesis yields the following systems of equations (a Diophantine problem (that will have a unique solution)):
From $n-1$ factors $(U_{a_{i_j}})$, $n-2$ are fixed values, and 1 is a free value:

$$\bar{t}_{0_{i_{n-1}}} + \bar{t}_{1_{i_{n-1}}} = |U_{a_{i_1}} \cap \cdots \cap U_{a_{i_{n-2}}}| = 2^{n-(n-2)} = 2^2.$$

From $n-1$ factors $(U_{a_{i_j}})$, $n-3$ are fixed values, and 2 are free values:

$$\bar{t}_{0_{i_{n-2}}0_{i_{n-1}}} + \bar{t}_{0_{i_{n-2}}1_{i_{n-1}}} + \bar{t}_{1_{i_{n-2}}0_{i_{n-1}}} + \bar{t}_{1_{i_{n-2}}1_{i_{n-1}}} = 2^{n-(n-3)} = 2^3.$$

From $n-1$ factors $(U_{a_{i_j}})$, $n-4$ are fixed values, and 3 are free values:

$$\bar{t}_{0_{i_{n-3}}0_{i_{n-2}}0_{i_{n-1}}} + \sum_{(l_{i_{n-3}},l_{i_{n-2}},l_{i_{n-1}})\in\mathbb{F}_2^3\ has\ one\ entry\ 1} \bar{t}_{l_{i_{n-3}}l_{i_{n-2}}l_{i_{n-1}}} + \sum_{(l_{i_{n-3}},l_{i_{n-2}},l_{i_{n-1}})\in\mathbb{F}_2^3\ has\ two\ entry\ 1's} \bar{t}_{l_{i_{n-3}}l_{i_{n-2}}l_{i_{n-1}}} + \bar{t}_{1_{i_{n-3}}1_{i_{n-2}}1_{i_{n-1}}} = 2^{n-(n-4)} = 2^4.$$

...
From $n-1$ factors $(U_{a_{i_j}})$, $n-(\mu+1)$ are fixed values, and μ are free values:

$$\bar{t}_{0_{i_{n-\mu}}\cdots 0_{i_{n-1}}} + \sum_{(l_{i_{n-\mu}}\cdots l_{i_{n-1}})\in\mathbb{F}_2^{\mu}\ has\ one\ entry\ 1} \bar{t}_{l_{i_{n-\mu}}\cdots l_{i_{n-1}}} + \sum_{(l_{i_{n-\mu}}\cdots l_{i_{n-1}})\in\mathbb{F}_2^{\mu}\ has\ two\ entry\ 1's} \bar{t}_{l_{i_{n-\mu}}\cdots l_{i_{n-1}}} + \cdots + \sum_{(l_{i_{n-\mu}}\cdots l_{i_{n-1}})\in\mathbb{F}_2^{\mu}\ has\ \mu-1\ entry\ 1's} \bar{t}_{l_{i_{n-\mu}}\cdots l_{i_{n-1}}} + \bar{t}_{1_{i_{n-\mu}}\cdots 1_{i_{n-1}}} = 2^{n-(n-(\mu+1))} = 2^{\mu+1}.$$

...
From $n-1$ factors $(U_{a_{i_j}})$, 1 is a fixed value, and $n-2$ are free values:

$$\bar{t}_{0_{i_2}\cdots 0_{i_{n-1}}} + \sum_{(l_{i_2}\cdots l_{i_{n-1}})\in \mathbb{F}_2^{n-2}\, has\, one\, entry\, 1} \bar{t}_{l_{i_2}\cdots l_{i_{n-1}}} + \sum_{(l_{i_2}\cdots l_{i_{n-1}})\in \mathbb{F}_2^{n-2}\, has\, two\, entry\, 1's} \bar{t}_{l_{i_2}\cdots l_{i_{n-1}}} + \cdots + \sum_{(l_{i_2}\cdots l_{i_{n-1}})\in \mathbb{F}_2^{n-2}\, has\, n-3\, entry\, 1's} \bar{t}_{l_{i_2}\cdots l_{i_{n-1}}} + \bar{t}_{1_{i_2}\cdots 1_{i_{n-1}}} = 2^{n-1}.$$

The intersection $(S_{a_{i_1}} \cap \cdots \cap S_{a_{i_{n-2}}}) \cap S_{a_{i_{n-1}}}$ is a $\mathbb{F}_2$-vector subspace of $S_{a_{i_1}} \cap \cdots \cap S_{a_{i_{n-2}}}$, then it has one less or the same dimension that of the space $S_{a_{i_1}} \cap \cdots \cap S_{a_{i_{n-2}}}$. Then:

$$t_{0_{i_1}\cdots 0_{i_{n-1}}} = \Big|\bigcap_{j=1}^{n-1} S_{a_{i_j}}\Big| = \begin{cases} \Big|\bigcap_{j=1}^{n-2} S_{a_{i_j}}\Big| = 2^{n-(n-2)} = 2^2, \text{ if } \dim(\bigcap_{j=1}^{n-1} S_{a_{i_j}}) = \\ \dim(\bigcap_{j=1}^{n-2} S_{a_{i_j}}). \\ 2^{-1}\Big|\bigcap_{j=1}^{n-2} S_{a_{i_j}}\Big| = 2^1, \text{ if } \dim(\bigcap_{j=1}^{n-1} S_{a_{i_j}}) = \dim(\bigcap_{j=1}^{n-2} S_{a_{i_j}}) - 1. \end{cases}$$

Case when $t_{0_{i_1}\cdots 0_{i_{n-1}}} = 2^1$: Substituting in the last system of equations:
From $n-1$ factors, $n-2$ are fixed values, in particular to be 0, and 1 free value:

$$\bar{t}_{0_{i_{n-1}}} + \bar{t}_{1_{i_{n-1}}} = 2^2,\ \bar{t}_{0_{i_{n-1}}} = t_{0_{i_1}\cdots 0_{i_{n-1}}},\ \text{then } \bar{t}_{1_{i_{n-1}}} = 2^2 - 2^1 = 2^1.$$

From $n-1$ factors, $n-3$ are fixed values, in particular to be 0, and 2 free values:

$$\bar{t}_{0_{i_{n-2}}0_{i_{n-1}}} + \bar{t}_{0_{i_{n-2}}1_{i_{n-1}}} + \bar{t}_{1_{i_{n-2}}0_{i_{n-1}}} + \bar{t}_{1_{i_{n-2}}1_{i_{n-1}}} = 2^3,$$
$$\bar{t}_{0_{i_{n-2}}0_{i_{n-1}}} = t_{0_{i_1}\cdots 0_{i_{n-1}}},\quad \bar{t}_{0_{i_{n-2}}1_{i_{n-1}}} = \bar{t}_{1_{i_{n-1}}},\quad \bar{t}_{1_{i_{n-2}}0_{i_{n-1}}} = \bar{t}_{1_{i_{n-1}}},$$
$$\text{then:}\quad \bar{t}_{1_{i_{n-2}}1_{i_{n-1}}} = 2^3 - 3(2^1) = 2^1.$$

...

From $n-1$ factors, $n-\mu-1$ are fixed values, in particular to be 0, and μ free values, for $1 \le \mu \le n-2$ (from the induction hypothesis):

$$\sum_{j=0}^{\mu} \binom{\mu}{j} \bar{t}_{\substack{l_{i_{n-\mu}}\cdots l_{i_{n-1}} \\ ((l_{i_{n-\mu}},\cdots l_{i_{n-1}}) \\ \text{has } j \text{ entries } 1's)}} = 2^{\mu+1}.$$

We obtain the constant sequence: $\bar{t}_{1_{i_{n-1}}} = \bar{t}_{1_{i_{n-2}}1_{i_{n-1}}} = \cdots = \bar{t}_{1_{i_2}\cdots 1_{i_{n-1}}} = 2^1$.
Case If $t_{0_{i_1}\cdots 0_{i_{n-1}}} = 2^2$: Again substituting in the system of equations:
From $n-1$ factors, $n-2$ are fixed values, in particular to be 0, and 1 free value:

$\bar{t}_{0_{i_{n-1}}} + \bar{t}_{1_{i_{n-1}}} = 2^2$, $\bar{t}_{0_{i_{n-1}}} = t_{0_{i_1}\cdots 0_{i_{n-1}}}$, then $\bar{t}_{1_{i_{n-1}}} = 2^2 - 2^2 = 0$, for arbitrary $\bar{t}_{1_{i_{n-1}}}$.

From $n-1$ factors, $n-3$ are fixed values, in particular to be 0, and 2 free values:

$$\bar{t}_{0_{i_{n-2}}0_{i_{n-1}}} + \bar{t}_{0_{i_{n-2}}1_{i_{n-1}}} + \bar{t}_{1_{i_{n-2}}0_{i_{n-1}}} + \bar{t}_{1_{i_{n-2}}1_{i_{n-1}}} = 2^3,$$
$$\bar{t}_{0_{i_{n-2}}0_{i_{n-1}}} = t_{0_{i_1}\cdots 0_{i_{n-1}}},\quad \bar{t}_{0_{i_{n-2}}1_{i_{n-1}}} = \bar{t}_{1_{i_{n-2}}0_{i_{n-1}}} = \bar{t}_{1_{i_{n-1}}} = 0, \text{ substituting the previous identity}$$
$$\text{then:}\quad \bar{t}_{1_{i_{n-2}}1_{i_{n-1}}} = 2^3 - 2^2 = 2^2, \text{ for arbitrary } \bar{t}_{1_{i_{n-2}}1_{i_{n-1}}}.$$

From $n-1$ factors, $n-4$ are fixed values, in particular to be 0, and 3 free values:

$$2^2 + 3(0) + 3(2^2) + \bar{t}_{1_{i_{n-3}}1_{i_{n-2}}1_{i_{n-1}}} = 2^4,$$
$$\text{then:}\quad \bar{t}_{1_{i_{n-3}}1_{i_{n-2}}1_{i_{n-1}}} = 0, \text{ for arbitrary } \bar{t}_{1_{i_{n-3}}1_{i_{n-2}}1_{i_{n-1}}}.$$

We obtain the alternating sequence:

$$\bar{t}_{\substack{l_{i_{n-\mu}}\cdots l_{i_{n-1}} \\ ((l_{i_{n-\mu}},\cdots l_{i_{n-1}}) \\ \text{has } \mu \text{ free values})}} = \begin{cases} 0, & \text{if } (l_{i_{n-\mu}},\cdots l_{i_{n-1}}) \text{ contains an odd number of 1's} \\ 4, & \text{if } (l_{i_{n-\mu}},\cdots l_{i_{n-1}}) \text{ contains an even number of 1's,} \end{cases} \tag{1}$$

$\forall\, 1 \le \mu \le n-2$.
Substituting in the equation:

$$2^{n-1} = |H_{a_1+\cdots+a_{n-1}}| = \sum_{(l_{i_1},\cdots,l_{i_{n-1}})\in\mathbb{F}_2^{n-1}\, has\, odd\, 1's} t_{l_{i_1},\cdots,l_{i_{n-1}}} =$$
$$\sum_{(l_{i_1},\cdots,l_{i_{n-1}})\in\mathbb{F}_2^{n-1}\, has\, one\, entry\, 1} \bar{t}_{1_{i_{n-1}}} +$$
$$\sum_{(l_{i_1},\cdots,l_{i_{n-1}})\in\mathbb{F}_2^{n-1}\, has\, three\, entry\, 1's} \bar{t}_{1_{i_{n-3}}1_{i_{n-2}}1_{i_{n-1}}} + \cdots +$$
$$\sum_{(l_{i_1},\cdots,l_{i_{n-1}})\in\mathbb{F}_2^{n-1}\, has\, n-3\, entry\, 1's} \bar{t}_{1_{i_3}\cdots 1_{i_{n-1}}} \text{ or}$$
$$\sum_{(l_{i_1},\cdots,l_{i_{n-1}})\in\mathbb{F}_2^{n-1}\, has\, n-2\, entry\, 1's} \bar{t}_{1_{i_2}\cdots 1_{i_{n-1}}} + \epsilon\ t_{\substack{1_{i_1}\cdots 1_{i_{n-1}} \\ (\text{all } n-1 \text{ places} \\ \text{are } 1's)}} = 2^{n-1},$$
$$\text{for some } \epsilon \in \{0,1\}.$$

Namely:

$$0 + \cdots + 0 + \epsilon\, t_{\substack{1_{i_1}\cdots 1_{i_{n-1}} \\ (\text{all } n-1 \text{ places} \\ \text{are } 1's)}} = 2^{n-1}, \text{ for some } \epsilon \in \{0, 1\}.$$

Then the term $t_{1_{i_1}\cdots 1_{i_{n-1}}}$ needs to be present and can't be 0; it is $t_{1_{i_1}\cdots 1_{i_{n-1}}} = 2^{n-1}$.
From the induction hypothesis we have:

$$t_{l_{i_1}\cdots l_{i_{n-2}}} = |U_{a_{i_1}} \cap \cdots \cap U_{a_{i_{n-2}}}| = 2^{n-(n-2)} = 2^2$$

In particular:

$$t_{1_{i_1}\cdots 1_{i_{n-2}}} = |H_{a_{i_1}} \cap \cdots \cap H_{a_{i_{n-2}}}| = 2^2.$$

By definition:

$$t_{1_{i_1}\cdots 1_{i_{n-2}}0_{i_{n-1}}} + t_{1_{i_1}\cdots 1_{i_{n-2}}1_{i_{n-1}}} = t_{1_{i_1}\cdots 1_{i_{n-2}}}$$

From the previous four equations:

$$2^{n-1} = t_{1_{i_1}\cdots 1_{i_{n-1}}} = 2^2 - t_{1_{i_1}\cdots 1_{i_{n-2}}0_{i_{n-1}}} \leq 2^2, \text{ where } t_{1_{i_1}\cdots 1_{i_{n-2}}0_{i_{n-1}}} \geq 0, \quad \forall n \geq 4.$$

For $n \leq 3$ the theorem is true, from the previous lemmas, Lemma 4.7 and 4.8. Then $t_{0_{i_1}\cdots 0_{i_{n-1}}} = 2^2$ is not true. Then, $t_{0_{i_1}\cdots 0_{i_{n-1}}} = 2^1$, then for this case we have the corresponding *constant sequence*:

$$\bar{t}_{1_{i_{n-1}}} = \bar{t}_{1_{i_{n-2}}1_{i_{n-1}}} = \cdots = \bar{t}_{\substack{1_{i_{n-\mu}}\cdots 1_{i_{n-1}} \\ ((l_{i_1},\cdots,l_{i_{n-1}}) \text{ has } \mu \text{ entry } 1's)}} = \cdots = \bar{t}_{1_{i_2}\cdots 1_{i_{n-1}}} = 2^1.$$

Equivalently:

$$t_{0_{i_1}\cdots 0_{i_{n-2}}1_{i_{n-1}}} = t_{0_{i_1}\cdots 0_{i_{n-3}}1_{i_{n-2}}1_{i_{n-1}}} = \cdots = t_{0_{i_1}\cdots 0_{i_{n-\mu-1}}1_{i_{n-\mu}}\cdots 1_{i_{n-1}}} = \cdots = t_{0_{i_1}1_{i_2}\cdots 1_{i_{n-1}}} = 2^1,$$

for all $1 \leq i_1, \cdots, i_{n-1} \leq n-1$, $1 \leq \mu \leq n-2$.

It remains to see what happens in the case of $n-1$ ones, $t_{1_{i_1}\cdots 1_{i_{n-1}}}$. By back substitution, beginning with the last equation (which has $n-2$ ones and 1 zero) of the constant sequence, $t_{0_{i_1}1_{i_2}\cdots 1_{i_{n-1}}} = 2^1$, for all $1 \leq i_1, \cdots, i_{n-1} \leq n-1$ (then also $t_{1_{i_1}\cdots 1_{i_{n-2}}0_{i_{n-1}}} = 2^1$) into the equation:

$$t_{1_{i_1}\cdots 1_{i_{n-2}}0_{i_{n-1}}} + t_{1_{i_1}\cdots 1_{i_{n-2}}1_{i_{n-1}}} = t_{1_{i_1}\cdots 1_{i_{n-2}}}$$

$$t_{1_{i_1}\cdots 1_{i_{n-2}}1_{i_{n-1}}} = 2^2 - 2^1 = 2^1.$$

Then, with the last equation $t_{1_{i_1}\cdots 1_{i_{n-1}}} = 2^1$, and $t_{0_{i_1}\cdots 0_{i_{n-1}}} = 2^1$, we obtain the following constant sequence:

$$t_{0_{i_1}\cdots 0_{i_{n-1}}} = t_{0_{i_1}\cdots 0_{i_{n-2}}1_{i_{n-1}}} = t_{0_{i_1}\cdots 0_{i_{n-3}}1_{i_{n-2}}1_{i_{n-1}}} = \cdots =$$
$$t_{0_{i_1}\cdots 0_{i_{n-\mu-1}}1_{i_{n-\mu}}\cdots 1_{i_{n-1}}} = \cdots = t_{0_{i_1}1_{i_2}\cdots 1_{i_{n-1}}} = t_{1_{i_1}\cdots 1_{i_{n-1}}} = 2^1,$$

for all $1 \leq i_1, \cdots, i_{n-1} \leq n-1$, $1 \leq \mu \leq n-2$.
Which means that $|U_{a_{i_1}} \cap \cdots \cap U_{a_{i_{n-1}}}| = t_{l_{i_1}\cdots l_{i_{n-1}}} = 2^1$, $\forall\ l_{i_1}\cdots l_{i_{n-1}}$, $(l_{i_1}, \cdots, l_{i_{n-1}})$ contains any number of ones, from 0 up to $n-1$. Then $|U_{a_1}\cap\cdots\cap U_{a_{n-1}}| = 2^1$, for all $U_{a_1}, \cdots, U_{a_{n-1}}$. □

Corollary 4.10 *Let $(a_i)_{i=1}^{n-1}$ a linearly independent set of $\mathbb{F}_2^n$, and ϕ a function on $\mathbb{F}_{2^n}$, define the sets $\widetilde{H}_{a_i} := \{x \in \mathbb{F}_{2^n};\ Tr_n^1(a_i\phi(x)) = 1\}$. Then*

$$|\widetilde{H}_{a_{i_1}} \cap \cdots \cap \widetilde{H}_{a_{i_{n-1}}}| = |\phi^{-1}[\{v_0, v_1\}]|, \text{ where } H_{a_1} \cap \cdots \cap H_{a_{n-1}} = \{v_0, v_1\}.$$

In particular, if ϕ is a permutation, then $|\widetilde{H}_{a_{i_1}} \cap \cdots \cap \widetilde{H}_{a_{i_{n-1}}}| = 2$.

Corollary 4.11 *Let $(a_i)_{i=1}^{n-1}$ a linearly independent set, and let $0 \notin (h_i)_{i=1}^{l}$ a sequence of different elements, on $\mathbb{F}_{2^n}$. Defining $a_i^{(j)} := a_i h_j$, where each $h_j \neq 1$, then $\{x \in \mathbb{F}_{2^n};\ Tr_n^1(a_1x), \cdots Tr_n^1(a_{n-1}x) + Tr_n^1(a_1^{(1)}x)\cdots Tr_n^1(a_{n-1}^{(1)}x) + Tr_n^1(a_1^{(l)}x)\cdots Tr_n^1(a_{n-1}^{(l)}x) = 1\} \subset (H_{a_1} \cap \cdots \cap H_{a_{n-1}}) \cup \ \cdots\ \cup (H_{a_1^{(l)}} \cap \cdots \cap H_{a_{n-1}^{(l)}})$, and $|(H_{a_1} \cap \cdots \cap H_{a_{n-1}}) \cup \cdots \cup (H_{a_1^{(l)}} \cap \cdots \cap H_{a_{n-1}^{(l)}})| \leq 2(l+1)$.*

Besides, one can use the affine transformation $a_i^{(j)} := a_i + h_j$ in the proof of the Corollary. Moreover, if $H_{a_1} \cap \cdots \cap H_{a_{n-1}}, \cdots, H_{a_1^{(l)}} \cap \cdots \cap H_{a_{n-1}^{(l)}}$ are disjoints, then $|\{x \in \mathbb{F}_{2^n};\ Tr_n^1(a_1x)\cdots Tr_n^1(a_{n-1}x) + Tr_n^1(a_1^{(1)}x)\cdots Tr_n^1(a_{n-1}^{(1)}x) + Tr_n^1(a_1^{(l)}x)\cdots Tr_n^1(a_{n-1}^{(l)}x) = 1\} = (H_{a_1}\cap\cdots\cap H_{a_{n-1}}) \cup \cdots \cup (H_{a_1^{(l)}}\cap\cdots\cap H_{a_{n-1}^{(l)}})| = 2(l+1)$.

Example. Let $(a_i)_{i=1}^{n-1}$ a *linearly independent set* on $\mathbb{F}_{2^n}$, define $a_i^{(1)} := a_i h_1$, where $h_1 \neq 0, 1$, moreover $(H_{a_1} \cap \cdots \cap H_{a_{n-1}}) \cap (h_1 H_{a_1} \cap \cdots \cap H_{a_{n-1}}) = \emptyset$. Then $|\{x \in \mathbb{F}_{2^n};\ Tr_n^1(a_1x)\cdots Tr_n^1(a_{n-1}x) + Tr_n^1(a_1^{(1)}x)\cdots Tr_n^1(a_{n-1}^{(1)}x) = 1\} = (H_{a_1} \cap \cdots \cap H_{a_{n-1}}) \cup (H_{a_1^{(1)}} \cap \cdots \cap H_{a_{n-1}^{(1)}})| = 4$.

Theorem 4.9 implies that $|H_{a_1} \cap \cdots \cap H_{a_{n-1}}| = 2^1$, i.e., only two pre images will change, from x to $x+1$, that means: $H_{a_1} \cap \cdots \cap H_{a_{n-1}} = \{x_0, x_1\}$, for some $x_i \in \mathbb{F}_{2^n}^*$, $i : 0, 1$. The given families in the hypothesis of the main theorem (Theorem 4.2) belong to the more general family $f(x) = F(x + Tr_n^1(a_1x)\cdots Tr_n^1(a_{n-1}x))$. For f we shall make an approximation of its non-linearity through the nonlinearity for F (which is known):

$W_f(a,b) = (-1)^{Tr_n^1(b\,F(x_0+1)+a\,x_0)} + (-1)^{Tr_n^1(b\,F(x_1+1)+a\,x_1)} + \sum_{x\in\mathbb{F}_{2^n}-\{x_0,x_1\}} (-1)^{Tr_n^1(b\,F(x)+a\,x)}$
$= (-1)^{Tr_n^1(b\,F(x_0+1)+a\,x_0)} - (-1)^{Tr_n^1(b\,F(x_0)+a\,x_0)} + (-1)^{Tr_n^1(b\,F(x_1+1)+a\,x_1)}$
$-(-1)^{Tr_n^1(b\,F(x_1)+a\,x_1)} + \sum_{x\in\mathbb{F}_{2^n}} (-1)^{Tr_n^1(b\,F(x)+a\,x)}$
$= (-1)^{Tr_n^1(b\,F(x_0+1)+a\,x_0)} - (-1)^{Tr_n^1(b\,F(x_0)+a\,x_0)} + (-1)^{Tr_n^1(b\,F(x_1+1)+a\,x_1)}$
$-(-1)^{Tr_n^1(b\,F(x_1)+a\,x_1)} + W_F(a,b)$. Then:
$W_f(a,b) - W_F(a,b) = (-1)^{Tr_n^1(a\,x_0)}\left((-1)^{Tr_n^1(b\,F(x_0+1))} - (-1)^{Tr_n^1(b\,F(x_0))}\right) +$
$(-1)^{Tr_n^1(a\,x_1)}\left((-1)^{Tr_n^1(b\,F(x_1+1))} - (-1)^{Tr_n^1(b\,F(x_1))}\right)$. Then:

$W_f(a,b) - W_F(a,b) = \theta \in \{0, \pm 2, \pm 4\}$ (If it is ξ $(= |H_{a_1} \cap \cdots \cap H_{a_r}|)$ points, where $1 \leq r \leq n-1$, using this same procedure, where $\theta \in [-4\xi/2, 4\xi/2]$, we obtain Theorem 4.14). Then we have the following *bounds* for the nonlinearity of f:
$nl(f) = 2^{n-1} - \frac{1}{2}\max_{a\in\mathbb{F}_2^n,\ b\in\mathbb{F}_2^{n*}} |W_f(a,b)| = 2^{n-1} - \frac{1}{2}\max_{a\in\mathbb{F}_2^n,\ b\in\mathbb{F}_2^{n*}} |W_F(a,b)+\theta|$. Thus
$nl(F) - \frac{|\theta|}{2} = 2^{n-1} - \frac{1}{2}(|\theta| + \max_{a\in\mathbb{F}_2^n,\ b\in\mathbb{F}_2^{n*}} |W_F(a,b)|) \leq nl(f) \leq 2^{n-1} - \frac{1}{2}(-|\theta| + \max_{a\in\mathbb{F}_2^n,\ b\in\mathbb{F}_2^{n*}} |W_F(a,b)|) = nl(F) + \frac{|\theta|}{2}$. I.e. $nl(f) - nl(F) = \frac{\theta}{2} \in \{0, \pm 1, \pm 2\}$. Therefore,

Theorem 4.12 *Let $(a_i)_{i=1}^{n-1}$ be a linearly independent set of $\mathbb{F}_2^n$, $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$, and $f(x) = F(x + Tr_n^1(a_1x)\cdots Tr_n^1(a_{n-1}x))$. Then, $|nl(f) - nl(F)| \leq 2$.*

In particular, $nl(f) \geq nl(F) - 2$. Therefore, we obtain near-optimal nonlinearity if we choose $nl(F)$ optimal. **We emphasize that:** although other f can be constructed satisfying this same inequality, the challenge focuses on the extent to which other highly relevant cryptographic aspects are taken into account, which can only be fitted within the formula for f itself. Likewise, the success of another f will depend on each piece and where it is placed within the formulation of f. Some candidates for function F are those shown in Table 1 along with their nonlinearities.

The following result can be obtained analogously to Theorem 4.9.

Corollary 4.13 *Let $(a_i)_{i=1}^{n-1}$ a linearly independent set of $\mathbb{F}_2^n$, the sets $S_{a_i} = \text{Kernel}(Tr_n^1(a_ix)) = \{x \in \mathbb{F}_{2^n};\ Tr_n^1(a_ix) = 0\}$ their corresponding $\mathbb{F}_2$-vector subspaces of $\mathbb{F}_{2^n}$, under the trace function, $H_{a_i} = \{x \in \mathbb{F}_{2^n};\ Tr_n^1(a_ix) = 1\}$ their affine subspaces, and $1 \leq r \leq n-1$. Then, the intersections of the form $S_{a_1} \cap \cdots \cap S_{a_r}$, $H_{a_1} \cap S_{a_2} \cap \cdots \cap S_{a_r}$, $H_{a_1} \cap H_{a_2} \cap S_{a_3} \cap \cdots \cap S_{a_r}, \cdots$, and $H_{a_1} \cap \cdots \cap H_{a_r}$ form a partition of $\mathbb{F}_{2^n}$. Besides, $|U_{a_1} \cap \cdots \cap U_{a_r}| = 2^{n-r}$, where $U_{a_1} \cap \cdots \cap U_{a_r}$ denotes any partition element of $\mathbb{F}_{2^n}$.*

Theorem 4.14 *Let* $(a_i)_{i=1}^{n-1}$ *a linearly independent set of* $\mathbb{F}_2^n$, $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$, $1 \leq r \leq n-1$, *and* $f(x) = F(x + Tr_n^1(a_1 x) \cdots Tr_n^1(a_r x))$. *Then,* $|nl(f) - nl(F)| \leq 2^{n-r}$.

Open Problem 3. It would be a considerable advance to analyze when precisely the function of Theorem 4.14 ($f(x) = F(x + Tr_n^1(a_1 x) \cdots Tr_n^1(a_{n-1} x))$) is CCZ-inequivalent to F, for F as general as possible.

5 Discussions on the Class of Highly Nonlinear Functions Possessing All Algebraic Degrees Up to the Optimum

A novel property of the class of functions in (1)-(2) of Theorem 4.2 (later denoted by $\mathcal{C}_{2;n-1}^{\text{all}}$) is that for every algebraic degree from 2 to the optimum (i.e. $n-1$) there exists a member in the class $\mathcal{C}_{2;n-1}^{\text{all}}$ with such a degree. Moreover, $\mathcal{C}_{2;n-1}^{\text{all}}$ can be considered without the restrictions on $\gcd(n,k)$ and $\gcd(n,k')$, and whether n is divisible by 2 or not. Besides, the algebraic degree is the backbone of essential results. To date, no other class of *differentially* δ*-uniform functions* (including APN functions) with this quality of completeness is known. As for the class in Theorem 4.2-(3), it would be interesting to investigate whether it possesses this or a similar property. For each member of $\mathcal{C}_{2;n-1}^{\text{all}}$ we compute its algebraic degree by means of a rather general proof.

Theorem 5.1 *Let* $P_r : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ *be the function defined by the rule* $P_r(x) := Tr_n^1(a_1 x) \cdots Tr_n^1(a_r x)$, *such that* $(a_i)_{i=1}^{n-1}$ *is a linearly independent set of* $\mathbb{F}_2^n$, *and* $1 \leq r \leq n-1$. *Then* $d^0(P_r) = r$.

Proof. Corollary 4.13 implies that $|H_{a_1} \cap \cdots \cap H_{a_r}| = 2^{n-r}$, i.e., there are $|\mathbb{F}_{2^n}| - 2^{n-r}$ different roots on $\mathbb{F}_{2^n}$ that satisfy the nonlinear equation $P_r(x) = 0$. Thus, after performing the algebraic operations and combine like terms of the polynomial $D_r(x) := \prod_{\alpha_i \text{ is one of these mentioned roots of } P_r} x - \alpha_i$, it can be rewritten as a polynomial of degree $\deg(D_r) = |\mathbb{F}_{2^n}| - 2^{n-r}$, i.e. $D_r(x) = x^{2^n - 2^{n-r}} +$ terms of less degree. Due to the form of the formula $P_r(x)$, any of its terms is of the form $\varkappa x^{2^{\theta_1} + \cdots + 2^{\theta_r}}$, for some $(\varkappa, \theta_1, \cdots, \theta_r) \in \mathbb{F}_{2^n} \times \left(\mathbb{Z}/n\mathbb{Z}\right)^r$ with $\varkappa \neq 0$. This leads to $d^0(P_r) \leq r$... (Eq. 1), and additionally, since every function $F \in \mathcal{F}(\mathbb{F}_{2^n}, \mathbb{F}_{2^n})$ has a sole representation as a univariate polynomial of degree at most $2^n - 1$, then $\deg(P_r(x) \mod (x^{2^n} - x)) \leq \max(\deg(\varkappa x^{2^{\theta_1} + \cdots + 2^{\theta_r}} \mod (x^{2^n} - x))) \leq \max_{\theta_i \neq \theta_j \text{ if } 1 \leq i \neq j \leq r} (\deg(\varkappa x^{2^{\theta_1} + \cdots + 2^{\theta_r}} \mod (x^{2^n} - x))) = \deg(\varkappa_1 x^{2^{n-1} + \cdots + 2^{n-r}}) = 2^n - 2^{n-r}$... (Eq. 2), if the coefficient $\varkappa_1 \neq 0$ (but if $\varkappa_1 = 0$, this same upper bound on $\deg(P_r(x) \mod (x^{2^n} - x))$

is still preserved). Since the roots of $P_r(x)$ are roots of $P_r(x) \mod (x^{2^n} - x)$ (this remainder results from applying the division algorithm to the pair $P_r(x)$, $x^{2^n} - x$. Besides, $x^{2^n} - x$ induces the zero function $0 : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, furthermore, is a non-zero element in the integral domain $\mathbb{F}_{2^n}[X]$), then we bound its degree, $\deg(P_r(x) \mod (x^{2^n} - x)) \geq \deg(D_r) = 2^n - 2^{n-r}$... (Eq. 3). From (Eq. 2)-(Eq. 3), $\deg(P_r(x) \mod (x^{2^n} - x)) = 2^n - 2^{n-r}$. Guaranteeing that $\varkappa_1 \neq 0$ in the term $\varkappa_1 x^{\deg(P_r(x) \mod (x^{2^n}-x))}$ of $P_r(x) \mod (x^{2^n} - x)$, and then, $d^0(P_r) \geq d^0(\varkappa_1 x^{\deg(P_r(x) \mod (x^{2^n}-x))})$. The integer representation of the exponent $\deg(P_r(x) \mod (x^{2^n} - x))$ is $2^{n-1} + \cdots + 2^{n-r}$, which is also unique. According to the definition of algebraic degree, $d^0(P_r) \geq r$... (Eq. 4). From (Eq. 1)-(Eq. 4), $d^0(P_r) = r$. □

In the remainder of this section, we delve deeper into the algebraic degree; below, we will shed light on a small part that we have previously investigated at the end and without much depth in this aspect. With respect to Theorem 4.2-(2), two subcases are presented; for the rich subfamily such that $g = n-2$, we clarify that the algebraic degree beyond being no less than $n-2$ (almost optimal algebraic degree), this is optimal. While for the other subfamily, where $g = n-1$, this is optimal as well. Without further ado, we provide the computation of the algebraic degree of this stellar class of functions in the beautiful theorem given below.

Theorem 5.2 *Let $(a_i)_{i=1}^{n-1}$ be a linearly independent set of $\mathbb{F}_2^n$, $u \geq 1$. Then, the following assertions holds.*

$d^0((x^{(2^u \text{ or } 2^{u\pm1})} + x + 1)P_m(x)) = m + 1$, $\forall\ n - 3 \geq m \geq 2$;

$d^0((x^{(2^u \text{ or } 2^{u\pm1})} + x + 1)P_{n-2}(x)) = n - 1$; *and*

$d^0((x^{(2^u \text{ or } 2^{2u})} + x + 1)P_{n-1}(x)) = n - 1$, *where* $P_m(x) = \prod_{i=1}^{m} Tr_n^1(a_i x)$, $\forall$ $m \geq 2$.

Proof. By Theorem 5.1, $P_m(x) = \mathfrak{A}x^{2^{n-1}+\cdots+2^{n-m}}+$ other terms of less degree, where $\mathfrak{A} \in \mathbb{F}_{2^n}^*$ (guarantees the existence of the leading term), $m \geq 2$, and $u \geq 1$. The terms of maximum algebraic degree ($= m$) in P_m exist and are determined, for instance, as 2^ωth powers (where $\omega \in \mathbb{Z}/n\mathbb{Z}$) of its leading term —because the algebraic degree is invariant under these powers, and P_m is idempotent under the field multiplication—given in the following polynomial:

$$\sum_{\omega \in \mathbb{Z}/n\mathbb{Z}} \mathfrak{A}^{2^\omega} x^{\sum_{\theta \in \{\omega, \omega+1, \cdots, \omega+n-m-1\}} -2^\theta}$$

Regarding this case, let us additionally consider that $n - 2 \geq m$. Possible terms with the maximum possible algebraic degree ($= m + 1$) in $xP_m(x)$ can only come from terms with algebraic degree m in $P_m(x)$, as presented below:

$$\sum_{\substack{\omega\in\mathbb{Z}/n\mathbb{Z},\\ 0\in\{\omega,\omega+1,\cdots,\omega+n-m-1\}}} x\mathfrak{A}^{2^\omega} x^{\sum\limits_{\theta\in\{\omega,\omega+1,\cdots,\omega+n-m-1\}}{}^{-2^\theta}} +$$

$$\sum_{\substack{\{0,\omega_1,\cdots,\omega_{n-m-1}\}\subseteq\left(\mathbb{Z}/n\mathbb{Z}\right)^{n-m}\\ \text{is a set of non-consecutive}\\ \text{different one each other values.}}} x\mathfrak{U}_{0,\omega_1,\cdots,\omega_{n-m-1}} x^{\sum\limits_{\theta\in\{0,\omega_1,\cdots,\omega_{n-m-1}\}}{}^{-2^\theta}}$$

$$= \sum_{\substack{\omega\in\mathbb{Z}/n\mathbb{Z},\\ 0\in\{\omega,\omega+1,\cdots,\omega+n-m-1\}}} \mathfrak{A}^{2^\omega} x^{\sum\limits_{\theta\in\{\omega,\omega+1,\cdots,\omega+n-m-1\}-\{0\}}{}^{-2^\theta}} +$$

$$\sum_{\substack{\{0,\omega_1,\cdots,\omega_{n-m-1}\}\subseteq\left(\mathbb{Z}/n\mathbb{Z}\right)^{n-m}\\ \text{is a set of non-consecutive}\\ \text{different one each other values.}}} \mathfrak{U}_{0,\omega_1,\cdots,\omega_{n-m-1}} x^{\sum\limits_{\theta\in\{\omega_1,\cdots,\omega_{n-m-1}\}}{}^{-2^\theta}}$$

Note that the expressions in this theorem have the following form (hereafter we omit the parentheses in the exponent, since there will be no ambiguity in reading it as usual):

$$\sum_{\text{conditions set \# 1}} \text{coefficient } x^{\left(\sum\limits_{\text{conditions set \# 2}} \text{some argument}\right)}$$

where, coefficient $\in \mathbb{F}_{2^n}$. Terms of algebraic degree $m+1$ in $x^u P_m(x)$:

$$\sum_{\substack{\omega\in\mathbb{Z}/n\mathbb{Z},\\ u\in\{\omega,\,\omega+1,\cdots,\,\omega+n-m-1\}}} x^{2^u}\mathfrak{A}^{2^\omega}x^{\theta\in\{\omega,\,\omega+1,\cdots,\,\omega+n-m-1\}}+$$

$$\sum_{\substack{\{u,\,\omega_1,\cdots,\,\omega_{n-m-1}\}\subseteq\left(\mathbb{Z}/n\mathbb{Z}\right)^{n-m}\\ \text{is a set of non-consecutive}\\ \text{different one each other values.}}} x^{2^u}\mathfrak{U}^{2^u}_{0,\,\omega_1-u,\cdots,\,\omega_{n-m-1}-u}x^{\theta\in\{u,\,\omega_1,\cdots,\,\omega_{n-m-1}\}}$$

$$=\sum_{\substack{\omega\in\mathbb{Z}/n\mathbb{Z},\\ u\in\{\omega,\,\omega+1,\cdots,\,\omega+n-m-1\}}} \mathfrak{A}^{2^\omega}x^{\theta\in\{\omega,\,\omega+1,\cdots,\,\omega+n-m-1\}-\{u\}}+$$

$$\sum_{\substack{\{u,\,\omega_1,\cdots,\,\omega_{n-m-1}\}\subseteq\left(\mathbb{Z}/n\mathbb{Z}\right)^{n-m}\\ \text{is a set of non-consecutive}\\ \text{different one each other values.}}} \mathfrak{U}^{2^u}_{0,\,\omega_1-u,\cdots,\,\omega_{n-m-1}-u}x^{\theta\in\{\omega_1,\cdots,\,\omega_{n-m-1}\}}$$

Don't forget that $\sum_{\omega\in\mathbb{Z}/n\mathbb{Z}} 2^\omega = 0$, for $n \geq 2$. Assuming that $d^0((x^{2^u}+x+1)P_m(x)) \leq m$:

$$\sum_{\substack{\{0,\,u,\,\omega_2,\cdots,\,\omega_{n-m-1}\}\subseteq\left(\mathbb{Z}/n\mathbb{Z}\right)^{n-m}\\ \text{is a set of non-consecutive}\\ \text{different one each other values.}}} \mathfrak{U}_{0,\,u,\,\omega_2,\cdots,\,\omega_{n-m-1}}x^{\theta\in\{u,\,\omega_2,\cdots,\,\omega_{n-m-1}\}}+$$

$$\sum_{\substack{\omega\in\mathbb{Z}/n\mathbb{Z},\\ u\in\{\omega,\,\omega+1,\cdots,\,\omega+n-m-1\},\\ \left(\{\omega,\,\omega+1,\cdots,\,\omega+n-m-1\}-\{u\}\right)\cup\{0\}\subseteq\left(\mathbb{Z}/n\mathbb{Z}\right)^{n-m}\\ \text{is a set of non-consecutive different}\\ \text{one each other values.}}} x^{\theta\in\{\omega,\,\omega+1,\cdots,\,\omega+n-m-1\}-\{u\}}\left(\mathfrak{A}^{2^\omega}+\underset{\text{(removing } u)}{\mathfrak{U}_{0,\,\omega,\,\omega+1,\cdots,\,\omega+n-m-1}}\right)$$

$$+\text{ terms of other types } = \sum_{\substack{\{\omega_1,\cdots,\,\omega_{n-m-1}\}\subseteq\left(\mathbb{Z}/n\mathbb{Z}\right)^{n-m-1}\\ \text{is a set of different}\\ \text{one each other values.}}} (0)x^{\theta\in\{\omega_1,\cdots,\,\omega_{n-m-1}\}} \quad \text{(Eq. 1)}$$

Assuming that also $d^0((x^{2^{u\pm1}}+x+1)P_m(x)) \leq m$. The above equation corresponds to u. The first summation in the equation corresponding to $u\pm1$ is given by the following expression:

$$\sum_{\substack{\{0,\, u\pm1,\, \omega_2,\cdots,\, \omega_{n-m-1}\}\subseteq\left(\mathbb{Z}/n\mathbb{Z}\right)^{n-m}\\ \text{is a set of non-consecutive}\\ \text{different one each other values.}}} \mathfrak{U}_{0,\, u\pm1,\, \omega_2,\cdots,\, \omega_{n-m-1}} x^{\sum\limits_{\theta\in\{u\pm1,\, \omega_2,\cdots,\, \omega_{n-m-1}\}}{}^{-2^\theta}}$$

A portion of this summation is separated and written as the summation at the beginning of the equation corresponding to $u \pm 1$, below:

$$\sum_{\substack{\omega\in\mathbb{Z}/n\mathbb{Z},\\ \{u\pm1,\, \omega_2,\cdots,\, \omega_{n-m-1}\}\\ \text{is chosen such that it coincides with}\\ \{\omega,\, \omega+1,\cdots,\, \omega+n-m-1\}-\{u\}.\\ \text{Where } u\in\{\omega,\, \omega+1,\cdots,\, \omega+n-m-1\},\\ \left(\{\omega,\, \omega+1,\cdots,\, \omega+n-m-1\}-\{u\}\right)\cup\{0\}\subseteq\left(\mathbb{Z}/n\mathbb{Z}\right)^{n-m}\\ \text{is a set of non-consecutive different}\\ \text{one each other values.}}} \underset{\text{(removing } u\text{)}}{\mathfrak{U}_{0,\, \omega,\, \omega+1,\cdots,\, \omega+n-m-1}} x^{\sum\limits_{\theta\in\{\omega,\, \omega+1,\cdots,\, \omega+n-m-1\}-\{u\}}{}^{-2^\theta}}$$

$$+ \text{ terms of other types } = \sum_{\substack{\{\omega_1,\cdots,\, \omega_{n-m-1}\}\subseteq\left(\mathbb{Z}/n\mathbb{Z}\right)^{n-m-1}\\ \text{is a set of different}\\ \text{one each other values.}}} (0) x^{\sum\limits_{\theta\in\{\omega_1,\cdots,\, \omega_{n-m-1}\}}{}^{-2^\theta}} \quad \text{(Eq. 2)}$$

Eq. (1) implies:

$\mathfrak{U}_{0,\, u,\, \omega_2,\cdots,\, \omega_{n-m-1}} = 0$, and $\mathfrak{A}^{2^\omega} + \underset{\text{(removing } u\text{)}}{\mathfrak{U}_{0,\, \omega,\, \omega+1,\cdots,\, \omega+n-m-1}} = 0$.

Eq. (2) implies:

$\underset{\text{(removing } u\text{)}}{\mathfrak{U}_{0,\, \omega,\, \omega+1,\cdots,\, \omega+n-m-1}} = 0$, where $u\pm1 \in \{\omega,\, \omega+1,\cdots,\, \omega+n-m-1\}-\{u\}$.

Then: $0 = \underset{\text{(removing } u\text{)}}{\mathfrak{U}_{0,\, \omega,\, \omega+1,\cdots,\, \omega+n-m-1}} \neq 0$, where $u\pm1 \in \{\omega,\, \omega+1,\cdots,\, \omega+n-m-1\}-\{u\}$, which means a contradiction. Therefore, $d^0((x^{2^u}+x+1)P_m(x)) \leq m$ and $d^0((x^{2^{u\pm1}}+x+1)P_m(x)) \leq m$ cannot occur simultaneously, or rather, $d^0((x^{2^u}+x+1)P_m(x)) = m+1$ or $d^0((x^{2^{u\pm1}}+x+1)P_m(x)) = m+1$. In particular, we reach an optimal case: $d^0((x^{2^u}+x+1)P_{n-2}(x)) = n-1$ or $d^0((x^{2^{u\pm1}}+x+1)P_{n-2}(x)) = n-1$. Note that, while if it is $u=1$, it is enough to use $u+1$.

Case $d^0((x^{2^u}+x+1)P_{n-1}(x)) = n-1$:

$P_{n-1}(x) = \prod\limits_{i=1}^{n-1} Tr_n^1(a_i x) = \varkappa x^{2^{n-1}+\cdots+2^1}$ + other terms of less degree, where $\varkappa \neq 0$ (ensures the existence of the leading term). The maximum algebraic degree ($= n-1$) terms in P_{n-1} exist and are determined as 2^ω powers of their leading term (of maximum degree), and constitute the polynomial below:

$$\sum_{\omega\in\mathbb{Z}/n\mathbb{Z}} \varkappa^{2^\omega} x^{\sum\limits_{\theta\in\mathbb{Z}/n\mathbb{Z}-\{\omega\}}{}^{+2^\theta}}$$

The only terms with algebraic degree $n-1$ in $xP_{n-1}(x)$ are produced from only one of the terms with algebraic degree $n-1$ and possibly from the terms with algebraic degree $n-2$ in $P_{n-1}(x)$, as shown below:

$$x\varkappa^2 x^{\sum\limits_{\theta\in\mathbb{Z}/n\mathbb{Z}-\{1\}}2^\theta}+\sum_{\omega\in\mathbb{Z}/n\mathbb{Z}-\{0\}} x\zeta_{0,\,\omega}x^{\sum\limits_{\theta\in\mathbb{Z}/n\mathbb{Z}-\{0,\,\omega\}}2^\theta}$$
$$=\varkappa^2 x^{\sum\limits_{\theta\in\mathbb{Z}/n\mathbb{Z}-\{0\}}2^\theta}+\sum_{\omega\in\mathbb{Z}/n\mathbb{Z}-\{0\}} \zeta_{0,\,\omega}x^{\sum\limits_{\theta\in\mathbb{Z}/n\mathbb{Z}-\{\omega\}}2^\theta}$$

Terms of algebraic degree $n-1$ in $x^uP_{n-1}(x)$:

$$x^{2^u}\varkappa^{2^{u+1}} x^{\sum\limits_{\theta\in\mathbb{Z}/n\mathbb{Z}-\{u+1\}}2^\theta}+\sum_{\omega\in\mathbb{Z}/n\mathbb{Z}-\{u\}} x^{2^u}\zeta_{0,\,\omega-u}^{2^u}x^{\sum\limits_{\theta\in\mathbb{Z}/n\mathbb{Z}-\{u,\,\omega\}}2^\theta}$$
$$=\varkappa^{2^{u+1}} x^{\sum\limits_{\theta\in\mathbb{Z}/n\mathbb{Z}-\{u\}}2^\theta}+\sum_{\omega\in\mathbb{Z}/n\mathbb{Z}-\{u\}} \zeta_{0,\,\omega-u}^{2^u}x^{\sum\limits_{\theta\in\mathbb{Z}/n\mathbb{Z}-\{\omega\}}2^\theta}$$

Assuming (regarding u) that $d^0((x^{2^u}+x+1)P_{n-1}(x))\leq n-2$:

$$\big(\varkappa^2+\zeta_{0,\,n-u}^{2^u}\big)x^{\sum\limits_{\theta\in\mathbb{Z}/n\mathbb{Z}-\{0\}}2^\theta}+\big(\varkappa^{2^{u+1}}+\zeta_{0,\,u}\big)x^{\sum\limits_{\theta\in\mathbb{Z}/n\mathbb{Z}-\{u\}}2^\theta}+$$
$$\sum_{\omega\in\mathbb{Z}/n\mathbb{Z}-\{0,\,u\}}\big(\zeta_{0,\,\omega}+\zeta_{0,\,\omega-u}^{2^u}\big)x^{\sum\limits_{\theta\in\mathbb{Z}/n\mathbb{Z}-\{\omega\}}2^\theta}=-\sum_{\omega\in\mathbb{Z}/n\mathbb{Z}}\varkappa^{2^\omega}x^{\sum\limits_{\theta\in\mathbb{Z}/n\mathbb{Z}-\{\omega\}}2^\theta}\quad\text{(Eq. 3)}$$

Eq. (3) implies:

$$\begin{cases}\varkappa^2+\zeta_{0,\,n-u}^{2^u}+\varkappa=0\\ \varkappa^{2^{u+1}}+\zeta_{0,\,u}+\varkappa^{2^u}=0\\ \zeta_{0,\,\omega}+\zeta_{0,\,\omega-u}^{2^u}+\varkappa^{2^\omega}=0\text{ for any }\omega\neq 0,u.\end{cases}$$

Item (3) in this system works for $\omega=2u$: $\zeta_{0,\,2u}+\zeta_{0,\,u}^{2^u}+\varkappa^{2^{2u}}=0$ (Eq. 4).

Assuming (regarding $2u$) also that $d^0((x^{2^{2u}}+x+1)P_{n-1}(x))\leq n-2$ one of its equations is:

$$-\zeta_{0,\,2u}=\varkappa^{2^{2u}}\big(1+\varkappa^{2^{2u}}\big)=\big(-\zeta_{0,\,u}\big)^{2^u}\quad\text{(Eq. 5)}.$$

In light of $\varkappa^{2^{2u}}\neq 0$, this fact (Eq. (5)) contradicts Eq. (4). Then $d^0((x^{(2^u\text{ or }2^{2u})}+$

$x+1)P_{n-1}(x)) = n-1$. When it comes to $u = 1$ we use an analogous procedure. □

On the other hand, with respect to a piecewise function, its algebraic degree cannot in principle be obtained as the maximum nor as the sum of the degrees of the piecewise functions that define it. **Problem 4A** How could the algebraic degree of a piecewise function be calculated from the algebraic degrees of its piecewise functions?. **Controllability Grade** Note: Theorem 4.14 gives us some control over the nonlinearity of f, while Theorem 5.2 gives us some level of control over $d^0(f)$; for both situations by choosing a suitable mapping P_r. **Open Problem 4B** Looking at Theorem 4.14 and Theorem 5.2, we ask whether there is any equation that specifies such a fabulous connection between $nl(f)$ and $d^0(f)$, for the functions involved there, for instance, when $nl(F)$ is high.

Corollary 5.3 *Let $n > 3$, $n-3 \geq u \geq 1$, and $(a_i)_{i=1}^{n-1}$ a linearly independent set of $\mathbb{F}_2^n$. If n is odd, $\gcd(n,u) = 1$, and $Tr_n^1(a_1) = \ldots = Tr_n^1(a_{n-1}) = 0$, then:*

f is a permutation with $d^0(f) = n-1$, where $f(x) = x^{2^u+1} + (x^{2^u} + x + 1)Tr_n^1(a_1x)\ldots Tr_n^1(a_{n-1}x)$ or $f(x) = x^{2^{2u}-2^u+1} + (x^{2^{2u}-2^u} + x^{2^{2u}-(2)2^u+1} + x^{2^{2u}-(2)2^u} + x^{2^{2u}-(3)2^u+1} + x^{2^{2u}-(3)2^u} + \ldots + x^{2^u+1} + x^{2^u} + x + 1)Tr_n^1(a_1x)\ldots Tr_n^1(a_{n-1}x)$.

Proof. Every $x-\alpha_i$ divides P_r, actually, $P_r = D_rQ_r$ (referring to Theorem 5.1), for $r \leq n-1$. The function KP_{n-1} satisfies that $K(x)P_{n-1}(x) = \left(\frac{K(x_0)(x-x_1)}{\prod_{x'\neq x_0}(x_0-x')} + \frac{K(x_1)(x-x_0)}{\prod_{x''\neq x_1}(x_1-x'')} + Q_{n-1}(x-x_0)(x-x_1)\right)D_{n-1}(x)$, and since $x^{2^n} - x \mid Q_{n-1}(x-x_0)(x-x_1)D_{n-1}(x)$, then KP_{n-1} can be re-written as a single polynomial under mod $(x^{2^n}-x)$ determined by the equation $\frac{K(x)P_{n-1}(x)}{\frac{K(x_0)}{\prod_{x'\neq x_0}(x_0-x')}+\frac{K(x_1)}{\prod_{x''\neq x_1}(x_1-x'')}} = \left(x - \left(\frac{K(x_0)x_1}{\prod_{x'\neq x_0}(x_0-x')}+\frac{K(x_1)x_0}{\prod_{x''\neq x_1}(x_1-x'')}\right)\Big/\left(\frac{K(x_0)}{\prod_{x'\neq x_0}(x_0-x')}+\frac{K(x_1)}{\prod_{x''\neq x_1}(x_1-x'')}\right)\right)D_{n-1}(x)$, where $K_u(x) = x^{2^{2u}-2^u+1}$ (subsequently denoted without the parameter u: $K(x)$), $\frac{K(x_0)}{\prod_{x'\neq x_0}(x_0-x')}+\frac{K(x_1)}{\prod_{x''\neq x_1}(x_1-x'')} \neq 0$, $H_{a_1}\cap\cdots\cap H_{a_{n-1}} = \{x_0, x_1\}$, and $Q_{n-1} \in \mathbb{F}_{2^n}^*$. Then,

$$\deg\left(\left(x - \frac{\frac{K(x_0)x_1}{\prod_{x'\neq x_0}(x_0-x')}+\frac{K(x_1)x_0}{\prod_{x''\neq x_1}(x_1-x'')}}{\frac{K(x_0)}{\prod_{x'\neq x_0}(x_0-x')}+\frac{K(x_1)}{\prod_{x''\neq x_1}(x_1-x'')}}\right)D_{n-1}(x)\right) =$$

$$\deg\left(x - \frac{\frac{K(x_0)x_1}{\prod_{x'\neq x_0}(x_0-x')}+\frac{K(x_1)x_0}{\prod_{x''\neq x_1}(x_1-x'')}}{\frac{K(x_0)}{\prod_{x'\neq x_0}(x_0-x')}+\frac{K(x_1)}{\prod_{x''\neq x_1}(x_1-x'')}}\right) + \deg(D_{n-1}(x)) = 2^n - 1, \text{ that is,}$$

$$d^0(K(x)P_{n-1}(x)) = d^0\left(\left(x - \frac{\frac{K(x_0)x_1}{\prod_{x'\neq x_0}(x_0-x')} + \frac{K(x_1)x_0}{\prod_{x''\neq x_1}(x_1-x'')}}{\frac{K(x_0)}{\prod_{x'\neq x_0}(x_0-x')} + \frac{K(x_1)}{\prod_{x''\neq x_1}(x_1-x'')}}\right)D_{n-1}(x)\right) = n.$$

Applying Corollary 9.3 we arm ourselves with the equalities $d^0(\partial_{H=1}(KP_{n-1})(x)) = d^0(K(x)P_{n-1}(x)) - 1 = n-1$. Let the composition $f_K := K\mathrm{o}(Id + P_{n-1})$, where Id is the identity function, thus $d^0(f_K(x)) = d^0((f_K(x) - K(x)) + K(x)) = d^0(f_K(x) - K(x)) = d^0(\partial_1(K(x))P_{n-1}(x))$, if u is such that $d^0(K(x)) = u+1 < d^0(f_K(x) - K(x))$ (because adding a term of lower algegraic degree does not affect the underlying algegraic degree). The algebraic degree for K results as follows: $2^{2u} - 2^u + 1 = 2^{2u-1} + \ldots + 2^{u+1} + (2^{u-1} + \ldots + 2^0) + 2^0 + 2^0 = 2^{2u-1} + \ldots + 2^{u+1} + 2^u + 2^0$, where $u > 0$. Since $\partial_1(P_r)$ is zero, $\partial_{H=P_{n-1}(x)}(K)(x) = \partial_1(K(x))P_{n-1}(x) = \partial_1(KP_{n-1})(x)$, and it is also required that $u+1 < n-1$. We note that the Kasamis K_{n-u} and K_u (equal to $K_{n-u}\mathrm{o}A_u$) are EA-E by applying $A_u(x) = x^{2^{2u}}$, so let's just consider the Kasami sub-list for $1 \leq u \leq \frac{n-1}{2}$. Suppose $\frac{K(x_0)}{\prod_{x'\neq x_0}(x_0-x')} + \frac{K(x_1)}{\prod_{x''\neq x_1}(x_1-x'')} = 0$, then $\frac{K(x_0)}{D_{n-1}(x_0)(x_0-x_1)} + \frac{K(x_1)}{D_{n-1}(x_1)(x_1-x_0)} = 0$. The function $\partial_1(D_{n-1})$ is zero since $\partial_1(P_{n-1})$ is, besides $x_1 - x_0 = 1$ and $D_{n-1}(x_0) \neq 0$. Then $K(x_0) = K(x_1)$, which is a contradiction because K is 1-to-1, that is we get that $\frac{K(x_0)}{\prod_{x'\neq x_0}(x_0-x')} + \frac{K(x_1)}{\prod_{x''\neq x_1}(x_1-x'')} \neq 0$. Done!, $d^0(f_K(x)) = n-1$. Applying this same procedure to the Gold $G(x)$ instead of $K(x)$, we get that $d^0(f_G(x)) = n-1$, such that $d^0(G(x)) = 2 < n-1 = d^0(f_G(x) - G(x))$, i.e. $3 < n$.

It is known that the Gold x^{2^u+1} and Kasami $x^{2^{2u}-2^u+1}$ functions are permutations when n is odd and $\gcd(n,u) = 1$ (see Table 11 in this article and [104, 85]). By Lemma 4.5, the polynomial $x + Tr_n^1(a_1)\cdots Tr_n^1(a_{n-1})$ is a permutation. Thus the composition $f(x) = F(x + P(x))$ is a permutation too, where F is Gold or Kasami. □

The body of the Corollary 5.3 fills in the missing cases with respect to the parameter u in Theorem 5.2, when it comes to P_{n-1}. Let's see what happens more precisely below.

Corollary 5.4 *Let $(a_i)_{i=1}^{n-1}$ be a linearly independent set of $\mathbb{F}_2^n$, $n > 3$, $n - 3 \geq u \geq 1$, and P_{n-1} as given in Corollary 5.3 and Theorem 5.1. Then:*

1). If $3 < n$, then $d^0((x^{2^u} + x + 1)P_{n-1}(x)) = n-1$.

2). $d^0((x^{2^{2u}-2^u} + x^{2^{2u}-(2)2^u+1} + x^{2^{2u}-(2)2^u} + x^{2^{2u}-(3)2^u+1} + x^{2^{2u}-(3)2^u} + \cdots + x^{2^u+1} + x^{2^u} + x + 1)P_{n-1}(x)) = n-1$.

Theorem 5.5 *(Optimal algebraic degree involving, either, any bijection or any APN). Let $\mathfrak{F} : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be a function, $\{a_i\}_{i=1}^{n-1}$ a linearly independent set of $\mathbb{F}_2^n$, the parameters of $\mathfrak{F}$ (like u in Kasami) are such that $d^0(\mathfrak{F}(x)) < n-1$, $n > 3$, and the pair P_{n-2}, P_{n-1} as in Theorem 5.1. Then:*

If $\mathfrak{F}$ is bijective, then $d^0(\mathfrak{F}(x+P_{n-1}(x)))$ and $d^0(\partial_1(\mathfrak{F}(x))P_{n-1}(x))$ are optimal.

If $\mathfrak{F}$ is APN, then $d^0(\mathfrak{F}(x+P_{n-2}(x)))$ and $d^0(\partial_1(\mathfrak{F}(x))P_{n-2}(x))$ are optimal.

Proof. In the body of Corollary 5.3, we relax the function K to be a bijective function (we emphasize, not necessarily a monomial function), and whenever necessary we apply the fact that the derivative operator is linear on the space $\mathcal{F}(\mathbb{F}_{2^n}, \mathbb{F}_{2^{n'}})$, where n, $n' \in \mathbb{Z}^+$. As for the case, $\mathfrak{F}$ APN: $\mathfrak{F}(x)P_{n-2}(x) \mod (x^{2^n}-x) = D_{n-2}(x) \sum_{\omega_\ell \in H_{a_1}\cap\cdots\cap H_{a_{n-2}}} \frac{\mathfrak{F}(\omega_\ell) \prod_{\omega_c \in H_{a_1}\cap\cdots\cap H_{a_{n-2}}\setminus\{\omega_\ell\}} (x-\omega_c)}{\prod_{x'\neq\omega_\ell}(\omega_\ell - x')}$. Assuming that the coefficient of the term of degree 3 (let's call it C_3) in the sum to the right of $D_{n-2}(x)$ is equal to zero, that is, $0 = C_3 := \sum_{\omega_\ell \in H_{a_1}\cap\cdots\cap H_{a_{n-2}}} \frac{\mathfrak{F}(\omega_\ell)}{\prod_{x'\neq\omega_\ell}(\omega_\ell - x')}$. The $\mathbb{F}_{2^n}$-partition element $H_{a_1}\cap\cdots\cap H_{a_{n-2}} = \{\omega_0, \omega_1, \omega_2, \omega_3\}$ contains 4 distinct elements, moreover, $H_{a_1}\cap\cdots\cap H_{a_{n-2}}\cap H_{a_{n-1}^{(1)}} = \{\omega_0, \omega_1\}$, $H_{a_1}\cap\cdots\cap H_{a_{n-2}}\cap H_{a_{n-1}^{(2)}} = \{\omega_2, \omega_3\}$, necessarily $\omega_1 - \omega_0 = 1 = \omega_3 - \omega_2$, and $\{a_i\}_{i=1}^{n-2} \cup \{a_{n-1}^{(j)}\}$ is a *linearly independent set* of $\mathbb{F}_2^n$, for each $j : 1, 2$. Using the fact $\partial_1(D_{n-2}) = \partial_1(P_{n-2}) = 0$, then $C_3 = \frac{\partial_1(\mathfrak{F})(\omega_0)}{(\omega_0-\omega_2)(\omega_0-\omega_3)D_{n-2}(\omega_0)} + \frac{\partial_1(\mathfrak{F})(\omega_2)}{(\omega_2-\omega_0)(\omega_2-\omega_1)D_{n-2}(\omega_2)} = \frac{\partial_1(\mathfrak{F})(\omega_0)}{Q_{n-2}^{-1}(\omega_0-\omega_2)(\omega_0-\omega_3)} + \frac{\partial_1(\mathfrak{F})(\omega_2)}{Q_{n-2}^{-1}(\omega_2-\omega_0)(\omega_2-\omega_1)} = 0$. Then $\partial_1(\mathfrak{F})(\omega_0) = \partial_1(\mathfrak{F})(\omega_2) = \beta$, also $\partial_1(\mathfrak{F})(\omega_1) = \partial_1(\mathfrak{F})(\omega_3) = \beta$, for some $\beta \in \mathbb{F}_{2^n}$, but this violates the APN condition on $\mathfrak{F}$. Then such a leading coefficient, C_3, cannot be 0. Then,

$$\deg\left(D_{n-2}(x)\left(\sum_{\omega_\ell \in H_{a_1}\cap\cdots\cap H_{a_{n-2}}} \frac{\mathfrak{F}(\omega_\ell) \prod_{\omega_c \in H_{a_1}\cap\cdots\cap H_{a_{n-2}}\setminus\{\omega_\ell\}} (x-\omega_c)}{\prod_{x'\neq\omega_\ell}(\omega_\ell - x')}\right)\right) =$$

$$\deg\left(\sum_{\omega_\ell \in H_{a_1}\cap\cdots\cap H_{a_{n-2}}} \frac{\mathfrak{F}(\omega_\ell) \prod_{\omega_c \in H_{a_1}\cap\cdots\cap H_{a_{n-2}}\setminus\{\omega_\ell\}} (x-\omega_c)}{\prod_{x'\neq\omega_\ell}(\omega_\ell - x')}\right) + \deg(D_{n-2}(x)) = 2^n - 1, \text{ that}$$

$$\text{is, } d^0\left(D_{n-2}(x)\left(\sum_{\omega_\ell \in H_{a_1}\cap\cdots\cap H_{a_{n-2}}} \frac{\mathfrak{F}(\omega_\ell) \prod_{\omega_c \in H_{a_1}\cap\cdots\cap H_{a_{n-2}}\setminus\{\omega_\ell\}} (x-\omega_c)}{\prod_{x'\neq\omega_\ell}(\omega_\ell - x')}\right)\right)$$

$= d^0(\mathfrak{F}(x)P_{n-2}(x)) = n$. Applying Corollary 9.3 analogously as it was done in Corollary 5.3, we obtain that $d^0(\partial_1(\mathfrak{F}P_{n-2})(x)) = d^0(\mathfrak{F}(x)P_{n-2}(x)) - 1 = n-1$. Let $f_{\mathfrak{F}} := \mathfrak{F}\mathrm{o}(Id + P_{n-2})$, therefore $d^0(f_{\mathfrak{F}}(x)) = d^0(f_{\mathfrak{F}}(x) - \mathfrak{F}(x)) = d^0(\partial_1(\mathfrak{F}(x))P_{n-2}(x))$, if $d^0(\mathfrak{F}(x)) < d^0(f_{\mathfrak{F}}(x) - \mathfrak{F}(x))$. Since $\partial_1(P_{n-2})$ is zero, $\partial_{H=P_{n-2}(x)}(\mathfrak{F})(x) = \partial_1(\mathfrak{F}(x))P_{n-2}(x) = \partial_1(\mathfrak{F}P_{n-2})(x)$. Subject to $d^0(\mathfrak{F}(x)) < n-1 = d^0(f_{\mathfrak{F}}(x) - \mathfrak{F}(x))$, we have $d^0(\mathfrak{F}\mathrm{o}(Id + P_{n-2})) = n-1$. □

Theorem 5.5 can be applied in parts (1) and (3) of Theorem 4.2. Following the same argument as in Corollary 5.3, the algebraic degree of the other families in the statement of Theorem 4.2 can be obtained. Including the families with $n-2$ factors in trace form from item (2) in Theorem 4.2, they will also attain the optimal algebraic degree. **Open Problem 5.** Investigate $d^0(f_{K_u,r})$ when $r < n-1$, $1 < u$, for the function, $f_{K_u,r}(x) = x^{2^{2u}-2^u+1} + (x^{2^{2u}-2^u} + x^{2^{2u}-(2)2^u+1} + x^{2^{2u}-(2)2^u} + x^{2^{2u}-(3)2^u+1} +$

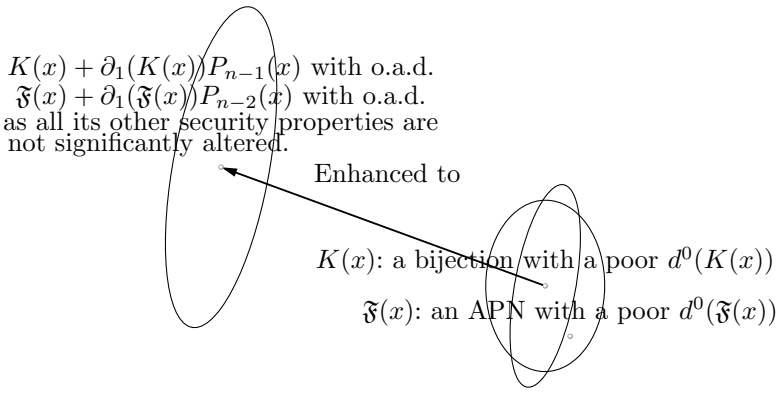

Figure 2: Transition to functions with optimal algebraic degree (o.a.d.)

$x^{2^{2u}-(3)2^u} + \cdots + x^{2^u+1} + x^{2^u} + x + 1)Tr_n^1(a_1x)\cdots Tr_n^1(a_rx)$, and in particular when $\gcd(n,u) = 1$. **Open Problem 6.** Obtain some version of Theorem 5.5 for $\mathbb{F}_{p^n}$ of odd charact. p.

Corollary 5.6 *Let $n \geq 3$, $n-1 \geq u \geq 1$, and $(a_i)_{i=1}^{n-1}$ a linearly independent set of $\mathbb{F}_2^n$. Then the families $f(x) = x^{2^u+1}+(x^{2^u}+x+1)Tr_n^1(a_1x)\ldots Tr_n^1(a_{n-1}x)$ and $f(x) = x^{2^{2u}-2^u+1} + (x^{2^{2u}-2^u} + x^{2^{2u}-(2)2^u+1} + x^{2^{2u}-(2)2^u} + x^{2^{2u}-(3)2^u+1} + x^{2^{2u}-(3)2^u} + \ldots + x^{2^u+1} + x^{2^u} + x + 1)Tr_n^1(a_1x)\ldots Tr_n^1(a_{n-1}x)$ are not EA-equivalent to power functions Gold, Kasami, and the Dobbertin's functions of the form $x^{2^{n/2}+2^{n/4}+1}$ (where $n/4$ is odd, discussed in [18, 27], and [59]), and the Bracken's binomial functions $\alpha x^{2^s+1} + \alpha^{2^k} x^{2^{-k}+2^{k+s}}$ in Table 3.*

Proof. Corollary 5.3 provide us that $d^0(f) = n-1$. Whereas, Gold $d^0(x^{2^u+1}) = 2$, Kasami $d^0(x^{2^{2u}-2^u+1}) = u+1$ (for the Kasami case: $u < n-1$), Dobbertin $d^0(x^{2^{n/2}+2^{n/4}+1}) = 3$, and Bracken's binomial $d^0(\alpha x^{2^s+1} + \alpha^{2^k} x^{2^{-k}+2^{k+s}}) = 2$. The algebraic degree of not affine functions is invariant under EA-equivalence. Then, for the Kasami case, with $u < n-2$, f is not EA-equivalent to Gold, Kasami, Dobbertin, and the Bracken's binomial. □

Note. It is of particular interest to remark that Theorem 4.2 establishes that the bases $\mathcal{B}^{(n)}$ of the Finite Field are those who provide the new function families.

Examples. Permutations based on Gold and Kasami (see tables 8 and 9). From Theorem Differentially δ-Uniform polynomial, $G_{k,j}(x) = x^{2^k+1} + (x^{2^k} + x + 1)Tr_n^1(a_1x)\ldots Tr_n^1(a_jx)$ and $K_{i,j}(x) = x^{2^{2i}-2^i+1} + (x^{2^{2i}-2^i} + x^{2^{2i}-(2)2^i+1} + x^{2^{2i}-(2)2^i} + x^{2^{2i}-(3)2^i+1} + x^{2^{2i}-(3)2^i} + \ldots + x^{2^i+1} + x^{2^i} + x + 1)Tr_n^1(a_1x)\ldots Tr_n^1(a_jx)$, where $Tr_n^1(a_1) = \ldots = Tr_n^1(a_j) = 0$. Cryptographic properties: $\Delta(f) =$ its differential δ uniformity. $nl(f) =$ its nonlinearity, depending on which family they are, they satisfy the inequalities: $nl(f) \geq nl(F)-2$ (or $nl(f) \geq nl(F)-4$),

where $nl(F)$ is the high nonlinearity of the Gold or Kasami. $d^0(f)$ = its algebraic degree. We wrote computer programs in SAGE-Python (based on the system MACSYMA developed by MIT) and Python software to fill each table in this research.

6 An Inherent Bound on $\mathfrak{Y}$

It is worth mentioning that the multiplicative inverse function, $\mathfrak{Y}$, is the S-Box used by the AES [51] and that, as we see in Section 8, it is vulnerable; in turn, such $\mathfrak{Y}$ is unsurpassed in terms of other nonlinearity qualities. We obtain the number of fixed points for the classes $\tilde{I}_{\tilde{x}_0,0}$, $\tilde{I}_{\tilde{x}_0}$, produced by our method, and there are coincidences with other procedures in this particular aspect. The goal of this section is to determine the inherent bound on $\mathfrak{Y}$, as given by Theorem 6.2, one of whose implications is Theorem 6.1. The second focus is the design of an optimal basis $\mathcal{B}_{\tilde{x}_0}$ that will give us sufficient control over $\tilde{I}_{\tilde{x}_0,0}$ and $\tilde{I}_{\tilde{x}_0}$. There is an extensive open problem at the end of the section. Consider the following optimization problem whose cost function is given by the size of the set of fixed points of $P_{n-1}\mathrm{o}(x^{-1}+\sigma)$ for $n \geq 2$, where the objective is to find the optimal parameters $\left(\sigma, (a_i)_{i=1}^{n-1}\right)$ that minimize it:

$$\min_{\sigma\in\mathbb{F}_{2^n};\,(a_i)_{i=1}^{n-1}\text{ is linearly independent}} |\text{Fixed points of } P_{n-1}\mathrm{o}(x^{-1}+\sigma)|$$

The Subfamilies $\tilde{I}_{\tilde{x}_0,0}$ *and* $\tilde{I}_{\tilde{x}_0}$: let P_{n-1} be such that its parameters $(a_i)_{i=1}^{n-1}$ form a *linearly independent set* of $\mathbb{F}_2^n$. We have that the equation $P_{n-1}(x)=1$ has a solution set equal to a coset $\tilde{x}_0+\mathbb{F}_2 = \{\tilde{x}_0, \tilde{x}_0+1\}$ verifying that $(\tilde{x}_0+\mathbb{F}_2)\cap\mathbb{F}_2 = \varnothing$, if $Tr_n^1(a_1) = \cdots = Tr_n^1(a_{n-1}) = 0$. So we immediately have that: $\mathfrak{T}_{\tilde{x}_0} \overset{\text{def}}{=} \{\frac{1}{\tilde{x}_0}, \frac{1}{\tilde{x}_0+1}\}$ (respectively $\mathbb{F}_2$) is the solution set of the equation $P_{n-1}(x^{-1})=1$ (respectively $\hat{P}_{n-1}(x)=1$), where $\hat{P}_{n-1}$ is the composition $P_{n-1}\mathrm{o}(x^{-1}+\tilde{x}_0)$. Depending on the purpose we have, we will consider function $\tilde{I}_{\tilde{x}_0,0}(x) \overset{\text{def}}{=} x^{2^n-2} + Tr_n^1(a_1x^{2^n-2})\cdots Tr_n^1(a_{n-1}x^{2^n-2})$ or $\tilde{I}_{\tilde{x}_0}(x) \overset{\text{def}}{=} x^{2^n-2} + \tilde{x}_0 + Tr_n^1(a_1(x^{2^n-2}+\tilde{x}_0))\cdots Tr_n^1(a_{n-1}(x^{2^n-2}+\tilde{x}_0))$, the reason of the subscript including $\tilde{x}_0$ lies in the design of a basis $\mathcal{B}_{\tilde{x}_0}$ of the type that will be seen shortly. With respect to the algebraic degree of these two families, it is the optimal one, because if their term x^{2^n-2} were eliminated by one coming from the part $P_{n-1}\mathrm{o}\ x^{-1}$ (respectively $P_{n-1}\mathrm{o}(x^{-1}+\tilde{x}_0)$), then they are still left with their term of degree 2^n-3 (whose algebraic degree is also optimal) coming (also) from the part $P_{n-1}\mathrm{o}\ x^{-1}$ (respectively $P_{n-1}\mathrm{o}(x^{-1}+\tilde{x}_0)$) (in the body of Theorem 5.2 you will find applicable relations independent of the Gold form).

Permutations $\tilde{I}_{\tilde{x}_0,0}$ *and* $\tilde{I}_{\tilde{x}_0}$ are *differentially* 4*-uniform* as we will see below.

Theorem 6.1 *Let n be even. For every $a \neq 0$ together with $\tilde{x}_0 \notin \mathbb{F}_2$, the mappings*

$$x \longrightarrow \tilde{I}_{\tilde{x}_0,0}(x+a) - \tilde{I}_{\tilde{x}_0,0}(x),\ x \longrightarrow \tilde{I}_{\tilde{x}_0}(x+a) - \tilde{I}_{\tilde{x}_0}(x)$$

are (at most) 4-to-1.

Proof. Let $\mathfrak{Y}(x) = x^{-1}$, $\mathrm{Id}(x) = x$, and ξ', ξ'' be two points such that $Tr_n^1(\mathfrak{Y}(\mathfrak{Y}(\xi')+1)) = Tr_n^1(\mathfrak{Y}(\mathfrak{Y}(\xi'')+1)) = 1$, and $\tilde{I}_{\tilde{x}_0,0}$ defined with a basis $\mathcal{B}_{\tilde{x}_0}$, as determined in Section 6. Then,

$\partial_a((\mathrm{Id}+P_{n-1})\mathrm{o}\mathfrak{Y})(x) = ((\mathrm{Id}+P_{n-1})\mathrm{o}\mathfrak{Y})(x+a) - ((\mathrm{Id}+P_{n-1})\mathrm{o}\mathfrak{Y})(x) = \mathfrak{Y}(x+a) - \mathfrak{Y}(x) = \partial_a\mathfrak{Y}(x)$, if $x \notin \{\mathfrak{Y}(\xi'), \mathfrak{Y}(\xi''), \mathfrak{Y}(\xi')+a, \mathfrak{Y}(\xi'')+a\}$.

If $x \in \{\mathfrak{Y}(\xi'), \mathfrak{Y}(\xi''), \mathfrak{Y}(\xi')+a, \mathfrak{Y}(\xi'')+a\}$, $\partial_a((\mathrm{Id}+P_{n-1})\mathrm{o}\mathfrak{Y})(x) = ((\mathrm{Id}+P_{n-1})\mathrm{o}\mathfrak{Y})(x+a) - ((\mathrm{Id}+P_{n-1})\mathrm{o}\mathfrak{Y})(x) = \mathfrak{Y}(x+a) - \mathfrak{Y}(x) + \gamma(a) = \partial_a\mathfrak{Y}(x) + \gamma(a)$, where $\gamma(a) \in \mathbb{F}_2$, $(\mathrm{Id}+P_{n-1})(\xi') = \xi'+1$, $(\mathrm{Id}+P_{n-1})(\xi'') = \xi''+1$.

Let $d = \frac{1}{3}(2^n-1)$, $d \in \mathbb{N}$ since $n \in 2\mathbb{N}$. There is a fact that connects us to Nyberg (1993), she observed that for each $a \in \mathbb{F}_{2^n}^*$, $\{0, a, a^{1+d}, a^{1+2d}\} \longrightarrow \mathfrak{Y}(a)$ is the only 4-to-1 shipment under the mapping $\partial_a\mathfrak{Y}$, its other shipments do not matter, they are 2-to-1. We wonder if there is any additional pair that contributes with a shipment to $\mathfrak{Y}(a)$, symbolically, $\{x, x+a\} \longrightarrow \mathfrak{Y}(a)$. Such a pair could only come from the set $\{\mathfrak{Y}(\xi'), \mathfrak{Y}(\xi''), \mathfrak{Y}(\xi')+a, \mathfrak{Y}(\xi'')+a\}$. Suppose, for example, that $\partial_a((\mathrm{Id}+P_{n-1})\mathrm{o}\mathfrak{Y})(\mathfrak{Y}(\xi')) = \partial_a\mathfrak{Y}(\mathfrak{Y}(\xi')) + 1$. Below we will show that $Tr_n^1(\mathfrak{Y}(\mathfrak{Y}(\xi')+1)) = 1$ (from the hypothesis) implies $\partial_a\mathfrak{Y}(\mathfrak{Y}(\xi')) - \mathfrak{Y}(a) \neq 1$, $\forall a \neq 0$. So $\partial_a((\mathrm{Id}+P_{n-1})\mathrm{o}\mathfrak{Y})(\mathfrak{Y}(\xi')) = \partial_a\mathfrak{Y}(\mathfrak{Y}(\xi')) + 1 \neq \mathfrak{Y}(a)$, i.e. such a shipment does not reach $\mathfrak{Y}(a)$. Then the shipments at most can be 4-to-1, proving that for each $a \neq 0$ the mapping $x \longrightarrow \tilde{I}_{\tilde{x}_0,0}(x+a) - \tilde{I}_{\tilde{x}_0,0}(x)$ is *differentially* 4*-uniform*. Applying the fact that a permutation f and its f^{-1} have the same uniform differentiability, we obtain that, $\Delta(\tilde{I}_{\tilde{x}_0,0}) = \Delta(\mathfrak{Y}\mathrm{o}(\mathrm{Id}+P_{n-1})) = \Delta((\mathfrak{Y}+\tilde{x}_0)\mathrm{o}(\mathrm{Id}+P_{n-1})) = \Delta(\tilde{I}_{\tilde{x}_0})$.

In this paragraph, let us prove that: given $(a,k) \in \left(\mathbb{F}_{2^n}^*\right)^2$, $\zeta \notin \mathfrak{Y}(k)\mathbb{F}_2$ such that $Tr_n^1(\mathfrak{Y}(k\zeta+1)) = 1$ implies $\partial_a\mathfrak{Y}(\zeta) - \mathfrak{Y}(a) \neq k$. Let $\zeta \notin \{a, 0, \mathfrak{Y}(k)\}$, the equation $\partial_a\mathfrak{Y}(\zeta) - \mathfrak{Y}(a) = k$ is equivalent (when multiplied by $\zeta a(\zeta+a)$) to, $(k\zeta+1)a^2 + (k\zeta^2+\zeta)a + \zeta^2 = 0$, then multiplying by $\mathfrak{Y}(\zeta^2(k\zeta+1))$, $(a\mathfrak{Y}(\zeta))^2 + a\mathfrak{Y}(\zeta) + \mathfrak{Y}(k\zeta+1) = 0$ (implying $Tr_n^1(\mathfrak{Y}(k\zeta+1)) = 0$). Consequently, if we choose (k,ζ) such that $Tr_n^1(\mathfrak{Y}(k\zeta+1)) = 1$, we have $\partial_a\mathfrak{Y}(\zeta) - \mathfrak{Y}(a) \neq k$. On the other hand, if $\zeta = a$, a simple evaluation and the definition of $\mathfrak{Y}$ show that $\partial_a\mathfrak{Y}(\zeta) - \mathfrak{Y}(a) = 0 \neq k$. This inference in question is thus proven. In particular, this implication is obtained for $k = 1$ and $\zeta = \mathfrak{Y}(\xi')$.

By virtue of Theorem 6.2, it is enough to choose $\xi' = \theta$ and $\xi'' = \theta+1$, and apply the linearity of the trace, to obtain $Tr_n^1(\mathfrak{Y}(\mathfrak{Y}(\xi')+1)) = Tr_n^1(\mathfrak{Y}(\mathfrak{Y}(\xi'')+1)) = 1$. For $\theta \notin \mathbb{F}_2$, the existence of such an (optimal) Basis $\mathcal{B}_{\tilde{x}_0}$ is always guaranteed, where $\theta = \tilde{x}_0$. □

The property of the multiplicative inverse function $\mathfrak{Y}$ shown below gives it a decisive advantage in terms of its applicability.

Theorem 6.2 (An inherent bound on $\mathfrak{Y}$). *There are no less than $2^{n-2}-\sqrt{2^{n-2}}+\frac{1}{4}$ and no more than $2^{n-2}+\sqrt{2^{n-2}}+\frac{1}{4}$ points $\theta\in\mathbb{F}_{2^n}$ verifying the identity:* $$Tr_n^1(\mathfrak{Y}(\theta))=Tr_n^1(\mathfrak{Y}(\theta+1))=1.$$

Proof. Let's start by defining the function $\psi(\theta):=\mathfrak{Y}(\theta+1)-\mathfrak{Y}(\theta)$. If we remove $\{0,a\}$ from $\{0,a,a^{1+d},a^{1+2d}\}$ for $a=1$, the derivative, ψ, becomes 2-to-1, when dealing with n even. Let's define the following sets, $\mathcal{O}_{\widetilde{\kappa}}^{\kappa}:=\{\theta\in\mathbb{F}_{2^n};Tr_n^1(\mathfrak{Y}(\theta+\kappa))=\widetilde{\kappa},Tr_n^1(\mathfrak{Y}(\theta))=Tr_n^1(\mathfrak{Y}(\theta+1))\}$, $\mathcal{I}_{\widetilde{\kappa}}^{\kappa}:=\{\theta\in\mathbb{F}_{2^n};Tr_n^1(\mathfrak{Y}(\theta+\kappa))=\widetilde{\kappa},Tr_n^1(\mathfrak{Y}(\theta))\neq Tr_n^1(\mathfrak{Y}(\theta+1))\}$, where $\kappa,\widetilde{\kappa}:0,1$. Let's show that $\big||\mathcal{O}_0^0\bigcup\mathcal{O}_1^0|-2^{n-1}-\frac{1}{2}\big|\leq\sqrt{2^n}$. For $\theta\notin\mathbb{F}_2$, applying the change of variable $u=\mathfrak{Y}(\theta)+1$ allows us to represent ψ as, $\psi(\theta)=\widetilde{\psi}(u):=u+\mathfrak{Y}(u)$, where $u\notin\mathbb{F}_2$. Even though $\psi(\mathbb{F}_2)\neq\widetilde{\psi}(\mathbb{F}_2)$, it happens that $Tr_n^1(\psi(\mathbb{F}_2))=Tr_n^1(\widetilde{\psi}(\mathbb{F}_2))=0$, and also $\mathbb{F}_2\subseteq\mathcal{O}_0^0\bigcup\mathcal{O}_1^0$. So, it will be equivalent to showing $\big||\{u\in\mathbb{F}_{2^n};Tr_n^1\big(\widetilde{\psi}(u)\big)=0\}|-2^{n-1}-\frac{1}{2}\big|\leq\sqrt{2^n}$. At this point we come across Kloosterman's sums $\mathcal{K}(a)$. By definition of $\mathcal{K}(a)$, it is immediate to deduce that $2|\{u\in\mathbb{F}_{2^n};Tr_n^1\big(\widetilde{\psi}(u)\big)=0\}|-2^n=\mathcal{K}(1)+1$, besides $W_{\mathfrak{Y}}(1,1)=\mathcal{K}(1)+1$, for n even or odd, with $a\in\mathbb{F}_{2^n}^*$. The Kloosterman sum $\mathcal{K}(1)$ is an integer of the form $\mathcal{K}(1)=-1 \mod(4)$ in the interval $[-2^{\frac{n}{2}+1},2^{\frac{n}{2}+1}]$, see Theorem 3.4 in [131, 86]. Then, $2|\{u\in\mathbb{F}_{2^n};Tr_n^1\big(\widetilde{\psi}(u)\big)=0\}|-2^n\in[-2^{\frac{n}{2}+1}+1,2^{\frac{n}{2}+1}+1]$, i.e., $2|\{u\in\mathbb{F}_{2^n};Tr_n^1\big(\widetilde{\psi}(u)\big)=0\}|\in[2^n-2^{\frac{n}{2}+1}+1,2^n+2^{\frac{n}{2}+1}+1]$. This gives $|\{u\in\mathbb{F}_{2^n};Tr_n^1\big(\widetilde{\psi}(u)\big)=0\}|\in[2^{n-1}-\sqrt{2^n}+1/2,2^{n-1}+\sqrt{2^n}+1/2]$.

Next, let's prove $|\mathcal{O}_1^0|=|\mathcal{O}_0^0\bigcup\mathcal{O}_1^0|/2$. Assuming that $|\mathcal{O}_0^{\kappa}|>|\mathcal{O}_1^{\kappa}|$ occurs; it is straightforward to see that $\big|\{\theta\in\mathbb{F}_{2^n};Tr_n^1(\mathfrak{Y}(\theta))=\widetilde{\kappa}\}\big|=2^{n-1}$, so $\big|\mathcal{I}^0_{(\widetilde{\kappa}+1) \mod(2)}\big|=|\mathcal{O}^0_{\widetilde{\kappa}}|$. So $\big|\mathcal{I}^1_{\widetilde{\kappa}}\big|=\big|\mathcal{I}^0_{(\widetilde{\kappa}+1) \mod(2)}\big|$. Then we have $|\{\theta\in\mathbb{F}_{2^n};Tr_n^1(\mathfrak{Y}(\theta+1))=\widetilde{\kappa}\}|=2|\mathcal{O}^0_{\widetilde{\kappa}}|$; therefore $|\mathcal{O}_0^1\bigcup\mathcal{I}_0^1|=2|\mathcal{O}_0^0|>2|\mathcal{O}_1^0|=|\mathcal{O}_1^1\bigcup\mathcal{I}_1^1|$, but this is a contradiction, because in fact $\widetilde{\kappa}\}|=|\mathcal{O}^1_{\widetilde{\kappa}}\bigcup\mathcal{I}^1_{\widetilde{\kappa}}|=2^{n-1}$, since the transformation $\mathfrak{Y}(\theta+1)$ permutes $\mathbb{F}_{2^n}$. That is, $|\mathcal{O}_0^0|\not>|\mathcal{O}_1^0|$. Analogously, we get $|\mathcal{O}_0^0|\not<|\mathcal{O}_1^0|$, so $|\mathcal{O}_0^0|=|\mathcal{O}_1^0|$. That is, $|\mathcal{O}_1^0|=\frac{1}{2}|\mathcal{O}_0^0\bigcup\mathcal{O}_1^0|$. Therefore, $2^{n-2}-\sqrt{2^{n-2}}+\frac{1}{4}\leq|\{\theta\in\mathbb{F}_{2^n};Tr_n^1(\mathfrak{Y}(\theta))=Tr_n^1(\mathfrak{Y}(\theta+1))=1\}|\leq 2^{n-2}+\sqrt{2^{n-2}}+\frac{1}{4}$. □

We can see that we have investigated the second coordinate function in the function $\theta\longrightarrow(Tr_n^1(\mathfrak{Y}(\theta+1))Tr_n^1(\mathfrak{Y}(\theta)),Tr_n^1(\mathfrak{Y}(\theta+1)-\mathfrak{Y}(\theta)))$ to investigate its first coordinate function.

Design of an Optimal Basis $\mathcal{B}_{\tilde{x}_0}=\big(\beta^{(i)}_{\tilde{x}_0}\big)_{i=1}^{n-1}$: consider the general family of the form $F^{-1}(x)+P_{n-1}(F^{-1}(x))$ (when invertible, it is the inverse of f of Theorem 4.12 for $Tr_n^1(a_1)=\cdots=Tr_n^1(a_{n-1})=0$) together with an arbitrary point $\tilde{x}_0\notin\mathbb{F}_2$, for some permutation F^{-1}. We wish to obtain a basis as in Theorem 4.9 such that the coset $\tilde{x}_0+\mathbb{F}_2$ solves its associated equation: $P_{n-1}(x)=1$. We solve this problem in this paragraph. Let $\Theta\in H_{\tilde{x}_0}\cap S_1$ be linearly independent with $\big(\beta^{(i)}\big)_{i=1}^{n-2}$, where $\big(\beta^{(i)}\big)_{i=1}^{n-1}$ is a basis of the subspace S_1, and $\big(\beta^{(i)}\big)_{i=1}^{n-2}$ is a basis of the subspace $S_1\cap S_{\tilde{x}_0}$. Based on Corollary

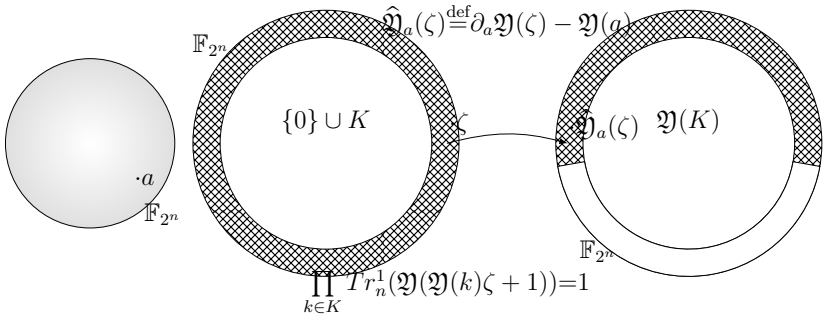

Figure 3: Mappings $\widehat{\mathfrak{Y}}_a$

4.13 and that $\{1,\tilde{x}_0\}$ is a linearly independent set, Θ exists. More precisely, we can choose $\Theta=\beta^{(n-1)}$. We know that $Tr_n^1(\tilde{x}_0\Theta)=1$ and $Tr_n^1(\Theta)=0$, due to the definition of Θ. To see the linear independence, assume that, $\sum_{i=1}^{n-2}c_i(\beta^{(i)}+\Theta)+c_{n-1}\Theta=0$, that is, $\sum_{i=1}^{n-2}c_i\beta^{(i)}+\left(\sum_{i=1}^{n-1}c_i\right)\beta^{(n-1)}=0$, in particular $c_{n-1}=-\sum_{i=1}^{n-2}c_i=0$. Then all c_i is zero. Finally, we obtain the desired basis $\{\beta^{(i)}+\Theta\}_{i=1}^{n-2}\cup\{\Theta\}=\{a_l\}_{l=1}^{n-1}\subseteq H_{\tilde{x}_0}$ for S_1, with $Tr_n^1(1\beta^{(i)}+\Theta)=0$ and $Tr_n^1(\Theta)=0$, for any $1\leq i\leq n-2$. That is, $P_{n-1}(\tilde{x}_0+\mathbb{F}_2)=1$. In sequel (to highlight the dependence on the point $\tilde{x}_0$) this basis for S_1 is denoted as $\mathcal{B}_{\tilde{x}_0}=\left(\beta_{\tilde{x}_0}^{(i)}\right)_{i=1}^{n-1}$. Note that we denote the bases by parentheses as well as by brackets.

Theorem 6.3 *The fixed point sets of $\tilde{I}_{\tilde{x}_0,0}$ and $\tilde{I}_{\tilde{x}_0}$ verify:*
A1). There exists $\tilde{x}_0\in\mathbb{F}_{2^n}\setminus\mathbb{F}_2$ such that $|$Fixed points of $\tilde{I}_{\tilde{x}_0,0}|\leq 2$.
A2). $|$Fixed points of $\tilde{I}_{\tilde{x}_0}|\leq 2$, for $\sigma=\tilde{x}_0\in\mathbb{F}_{2^n}\setminus\mathbb{F}_2$ and $(a_i)_{i=1}^{n-1}=\mathcal{B}_{\tilde{x}_0}$.
A3). If $\tilde{x}_0\in\mathbb{F}_{2^n}\setminus\mathbb{F}_2$ with $Tr_n^1(\tilde{x}_0^{-1})=1$, then $|$Fixed points of $\tilde{I}_{\tilde{x}_0}|=0$.

Proof. Let $\tilde{x}_0$ be a point outside $\mathbb{F}_2$. **Case I.** We look for the fixed points of $\tilde{I}_{\tilde{x}_0,0}(x)=x^{2^n-2}+Tr_n^1(\beta_{\tilde{x}_0}^{(1)}x^{2^n-2})\ldots Tr_n^1(\beta_{\tilde{x}_0}^{(n-1)}x^{2^n-2})$, where $\mathcal{B}_{\tilde{x}_0}$ is some basis determined by $\tilde{x}_0$ (the one recently obtained), such that $P_{n-1}(x^{-1})=1$ has $\mathfrak{T}_{\tilde{x}_0}$ as its solution set. From $\tilde{I}_{\tilde{x}_0,0}(x)=x$ we have $x^{2^n-2}=x+Tr_n^1(\beta_{\tilde{x}_0}^{(1)}x^{2^n-2})\ldots Tr_n^1(\beta_{\tilde{x}_0}^{(n-1)}x^{2^n-2})$. If $P_{n-1}(x^{2^n-2})=0$, then $x^{2^n-2}=x$, i.e, $x=0$ or $x^2-1=0$ $(x=1)$. We will consider finding two more fixed points for $\tilde{I}_{\tilde{x}_0,0}$. Furthermore, if $P_{n-1}(x^{2^n-2})=1$ (solved only by x in $\mathfrak{T}_{\tilde{x}_0}$), then we have the following equation independent of $\tilde{x}_0$, $x^{2^n-2}=x+1$, i.e. $x^2+x-1=0$, whose solution set is $\gamma+\mathbb{F}_2$, for some $\gamma\in\mathbb{F}_{2^n}$ with $(\gamma+\mathbb{F}_2)\cap\mathbb{F}_2=\varnothing$. Just by taking any of the lots of 2^n-4 candidates for $\tilde{x}_0$, $\tilde{x}_0\notin\mathbb{F}_2\cup(\frac{1}{\rho}+\mathbb{F}_2)$ for $\rho\in\gamma+\mathbb{F}_2$, , we have that $x^2+x-1\neq 0$ on $\mathbb{F}_{2^n}$. By choosing $\tilde{x}_0$ this way, we get $\tilde{I}_{\tilde{x}_0,0}$ to have no more than two fixed points, and also, *Fixed points of* $\tilde{I}_{\tilde{x}_0,0}\subseteq\mathbb{F}_2$. **Case**

II. Regarding $\tilde{I}_{\tilde{x}_0}$ the results change surprisingly. If $P_{n-1}(x^{2^n-2}+\tilde{x}_0)=1$, our $\tilde{I}_{\tilde{x}_0}$ has no fixed points. If $P_{n-1}(x^{2^n-2}+\tilde{x}_0)=0$, this brings us to $x\tilde{x}_0\neq 0$, $(\frac{x}{\tilde{x}_0})^2+\frac{x}{\tilde{x}_0}+\tilde{x}_0^{-2}=0$. Thus, $Tr_n^1(\tilde{x}_0^{-1})=0$. Besides, *Fixed points of* $\tilde{I}_{\tilde{x}_0}\subseteq\{x\in\mathbb{F}_{2^n}\setminus(\mathbb{F}_2\cup(\tilde{x}_0+\mathbb{F}_2));x^2+\tilde{x}_0x=1\}$ (2 fixed points at most). Therefore, |Fixed points of $P_{n-1}o(x^{-1}+\sigma)|\leq 2$, for $\sigma=\tilde{x}_0\notin\mathbb{F}_2$ and $(a_i)_{i=1}^{n-1}=\mathcal{B}_{\tilde{x}_0}$. It is even enough to choose $\tilde{x}_0$ such that $Tr_n^1(\tilde{x}_0^{-1})=1$ to have $\tilde{I}_{\tilde{x}_0}$ without fixed points: Fixed points of $\tilde{I}_{\tilde{x}_0}=\varnothing$ (there are a large number of $\tilde{x}_0$ points) □

This property of having a considerably small number of fixed points (2 points at most) propagates to the families $\tilde{I}^{(m)}_{\tilde{x}_0,0}(x)\stackrel{\text{def}}{=}x^{2^n-2}+Tr_n^1(\beta^{(1)}_{\tilde{x}_0}x^{2^n-2})\ldots Tr_n^1(\beta^{(m)}_{\tilde{x}_0}x^{2^n-2})$ and $\tilde{I}^{(m)}_{\tilde{x}_0}(x)\stackrel{\text{def}}{=}x^{2^n-2}+\tilde{x}_0+Tr_n^1(\beta^{(1)}_{\tilde{x}_0}(x^{2^n-2}+\tilde{x}_0))\ldots Tr_n^1(\beta^{(m)}_{\tilde{x}_0}(x^{2^n-2}+\tilde{x}_0))$, where $m\geq 1$. **Problem 7**. For each m and each point $\tilde{x}_0\notin\mathbb{F}_2$ a family of functions $\tilde{I}^{(m)}_{\tilde{x}_0}(x)$ is generated. Investigate whether these differentially δ-uniform classes contain subclasses with the best *differential δ-spectrum* within their general differentially δ-uniform class: that is, whose $\delta_f(a,b)$ coincides with $\Delta(f)(=\delta)$ in at most 2^n-1 occurrences where (a,b) belongs to some set $\{(a_1,b_1),\ldots,(a_{2^n-1},b_{2^n-1})\}$ (abstracting from the behavior of the mother reference x^{-1} (see the second paragraph in Theorem 6.1), although questionable in some of its aspects), where the $a_i(\neq 0)$ are distinct from each other, while the rest of the quantities $\delta_f(a,b)$ are bounded above by $\Delta(f)-2$. Still a *differential δ-spectrum* is one of the most relevant, if there were at most $(2^n-1)\sigma$ pairs $(a_1,b_{1,1}),(a_1,b_{1,2}),\ldots,(a_{2^n-1},b_{2^n-1,1}),(a_{2^n-1},b_{2^n-1,2})$, where all $\delta_f(a_i,b_{i,1})$ and $\delta_f(a_i,b_{i,2})$ are equal to $\Delta(f)$, where the $a_i\neq 0$ are distinct, for $\sigma=2$ (small). Besides, consider other families in Theorem 4.6. A candidate for F in Theorem 4.6 may be the Bracken and Leander function.

In [111], Chapter 4, the author finds bounds for the *nonlinearity* $(NL(f))$ of an infinite class of rather peculiar highly nonlinear functions, turning such a bounding mission into a remarkable optimization problem of the following style (**Open Problem 8:** give an answer to this discrete problem for the rest of the members of the classes in Theorems 4.2 and 4.12, as well as determining more precise bounds):

$$\max_{\mathfrak{u}_1\neq 1,\,(\mathfrak{u}_1,\mathfrak{u}_2,\mathfrak{z})\in\left(\mathbb{F}_{2^n}\right)^2\times\mathbb{Z}^+}|\{X\in\mathbb{F}_{2^n};Tr_n^1((\mathfrak{u}_1+1)X^{2^k+1})+\mathfrak{u}_2X)$$
$$+Tr_n^1(X^{2^k+1})Tr_n^1(X^{2^{\mathfrak{z}}+1})=0\}|.$$

In the oral part of Roberto R. Carranza's doctoral dissertation (year 2020), he proposed to refine the value of the differentiability of a function, as announced below. **Open Problem 9.** Given any diff. δ-uniform f_1, properly smooth this function into a new f_2 such that $\Delta(f_2)$ is strictly less than $\Delta(f_1)$, without sacrificing the properties of non-linearity, the algebraic degree, and

$|f_2(\mathbb{F}_{2^n})|$ should not decrease drastically. According to this sense, f_2 is called the *evolution* of f_1.

7 CCZ-inequivalence

The Walsh spectrum of the *almost bent* (AB) and Gold subfamilies can be found in the papers by Edel and Pott [67], Carlet, Charpin, and Zinoviev [34], and Dillon and Dobbertin [56]. In [112] R. Carranza added a new method to demonstrate CCZ-inequivalence between the Kasami-Welch family and other functions. The following result says that our function families are new.

Theorem 7.1 *The family of functions in Theorem 4.2 are CCZ-inequivalent to the Gold functions ([72, 104]), the Kasami functions ([78, 81]), the Dobbertin's functions of the form $x^{2^{n/2}+2^{n/4}+1}$ (where $n/4$ is odd, discussed in [18, 27], and [59]) and quadratic functions (including the Bracken's binomial), where $n > 4$.*

Proof. When n is even, the extended Walsh spectrum of the Gold, the Kasami and the Dobbertin's functions $x^{2^{2r}+2^r+1}$ is included in the (three valued) set $\{0, 2^{n/2}, 2^{n/2+1}\}$. Regarding to quadratic functions, the elements of their Walsh spectrum belong to the set $\{0, \pm 2^{n/2+l}$; where $l \geq 0\}$, namely, the elements of their extended Walsh spectrum are divisible by $2^{n/2}$. Now let's compute the form of the Walsh coeffcients of the functions in Theorem 4.2.

The equation $Tr_n^1(a_1x_0)\dots Tr_n^1(a_{n-1}x_0) = 1$ implies $Tr_n^1(a_1(x_0+1))\dots Tr_n^1(a_{n-1}(x_0+1)) = 1$, that means: If $x_0 \in H_{a_1} \cap \dots \cap H_{a_{n-1}}$, then $x_0 + 1 \in H_{a_1} \cap \dots \cap H_{a_{n-1}} - \{x_0\}$. Then, $x_1 = x_0 + 1$, in particular $\Delta_1 F(x_0) = \Delta_1 F(x_1)$. Then, $W_f(a,b) - W_F(a,b) = (-1)^{Tr_n^1(a\,x_0)}\left((-1)^{Tr_n^1(b\,F(x_0+1))} - (-1)^{Tr_n^1(b\,F(x_0))}\right) - (-1)^{Tr_n^1(a\,x_0+a)}\left((-1)^{Tr_n^1(b\,F(x_0+1))} - (-1)^{Tr_n^1(b\,F(x_0))}\right)$

$= (-1)^{Tr_n^1(a\,x_0)}\left(1 - (-1)^{Tr_n^1(a)}\right)\left((-1)^{Tr_n^1(b\,F(x_0+1))} - (-1)^{Tr_n^1(b\,F(x_0))}\right)$.

The function F is 1-to-1, then $\Delta_1 F(x_0) \neq 0$. **Case-I:** Choose $b \neq 0$ such that $Tr_n^1(b\Delta_1 F(x_0)) = 0$. Then the factor of $W_f(a,b) - W_F(a,b)$, given by $\left((-1)^{Tr_n^1(b\,F(x_0+1))} - (-1)^{Tr_n^1(b\,F(x_0))}\right)$ will be zero, then $W_f(a,b) = W_F(a,b)$, then $W_f(a,b) \in \{0, \pm 2^{n/2}, \pm 2^{n/2+1}\}$. **Case-II:** Choose $b \neq 0$ such that $Tr_n^1(b\Delta_1 F(x_0)) = 1$. Then the factor $\left((-1)^{Tr_n^1(b\,F(x_0+1))} - (-1)^{Tr_n^1(b\,F(x_0))}\right)$ will be ± 2, then $W_f(a,b) = W_F(a,b) \pm 2(-1)^{Tr_n^1(a\,x_0)}\left(1 - (-1)^{Tr_n^1(a)}\right) = W_F(a,b) \pm 2\left(1 - (-1)^{Tr_n^1(a)}\right)$. If $Tr_n^1(a) = 0$, then $W_f(a,b) = W_F(a,b)$. If $Tr_n^1(a) = 1$, then $W_f(a,b) = W_F(a,b) \pm 2^2$.

Only under the condition $Tr_n^1(b\Delta_1 F(x_0))Tr_n^1(a) = 1$, it appears new Walsh coefficients different from the coefficients $W_F(a,b)$. There are $2^{n-1}2^{n-1}$ of this new coefficients. There are $(3)2^{2n-2} - 2^n$ coefficients $W_F(a,b)$.

By Lemma 1.20, the extended Walsh spectra is a CCZ-invariant parameter. When $n > 4$, the number $2^{n/2}$ do not divides the coefficients $|W_f(a,b)|$. Then, the functions in Theorem 4.2 have different extended Walsh spectrum from the ones cited in Theorem 7.1. □

Definition 7.2 *Let $(a_i)_{i=1}^n$ be a basis of $\mathbb{F}_2^n$ (over $\mathbb{F}_2$, as usual), $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$, $Tr_n^m(x) = \sum_{i=0}^{\frac{n}{m}-1} x^{2^{im}}$, and $r \geq 1$, then $f(x) = F(x + Tr_n^1(a_1 x)\dots Tr_n^1(a_r x))$ is called an r-light function of F.*

Our method applied to the multiplicative inverse function leads to members of the families, $\tilde{I}_{\tilde{x}_{0,0}}^{(n-i)}(x) = x^{2^n-2} + Tr_n^1(a_1 x^{2^n-2})\cdots Tr_n^1(a_{n-i}x^{2^n-2}), \forall n-1 \geq i \geq 2$ and $\tilde{I}_{\tilde{x}_{0,0}}^{(n-1)}(x) := \tilde{I}_{\tilde{x}_{0,0}}(x) = x^{2^n-2} + Tr_n^1(a_1 x^{2^n-2})\cdots Tr_n^1(a_{n-1}x^{2^n-2})$, with optimal algebraic degree regardless of whether n is even or odd.

7.1 On Budaghyan-Carlet-Leander's CCZ-inequivalence Conjecture

Knowing an exceptional APN function is a sign of strength since we can be using a field and suddenly switch it to another one chosen at will from a number $\aleph_0$ (*countable infinity*, according to Georg Cantor) of *possibilities* that are its field extensions involved while employing the same function formula without losing the APN quality to maintain security; *exceptional* APN is better than APN. In cases where two functions are indistinguishable in terms of their invariants under CCZ-equivalence (having the same $\Delta_f = \Delta_g$ and $NL(f) = NL(g)$, for instance), determining whether or not they are (fully) CCZ-equivalent can become a serious headache. Recently, researcher R. Carranza constructed a new infinite class of APN functions, more precisely, the non-monomial exceptional APN (class $J_{(n_i)_{i=0}^{\infty}}$) for which he showed that the powerful Conjecture about CCZ-inequivalence proposed by Lilya Budaghyan, Claude Carlet, and Gregor Leander (who also gave the proof for the Gold, Dobbertin, and Inverse cases) also holds for their Kasami-Welch, Welch, and Niho cases [112], so that Table 1 is completely covered; the author introduced his *universal method* to investigate CCZ-inequivalence. The Dobbertin case can also be solved via the *universal method*. Conjecture-BCL has proven to be very decisive in the area. We will soon be introducing the function F_n, the Conjecture-BCL, we will also define the class $J_{(n_i)_{i=0}^{\infty}}$, providing the equations and algorithm applied to obtain it.

Theorem 7.3 *[26]. The switching neighbour $F_n(x) = x^3 + Tr_n^1(x^9)$ (other switching neighbours can be seen in the Ph.D. Dissertation [111]) satisfies:*

a1). For each dimension n, F_n (one F_n for each n) is APN on $\mathbb{F}_2^n$.

a2). is CCZ-inequivalent to the Gold, inverse and Dobbertin APN functions on $\mathbb{F}_{2^n}$ when $n \geq 7$.

a3). is EA-inequivalent to power functions on $\mathbb{F}_{2^n}$ when $n \geq 7$.

a4). is CCZ-inequivalent to power functions on $\mathbb{F}_{2^7}$.

Conjecture-BCL (*Budaghyan-Carlet-Leander*, 2nd page on [26]). For $n \geq 7$, $F_n(x) = x^3 + Tr_n^1(x^9)$ is CCZ-inequivalent to any power function ($F'(x) = x^t$).

Theorem 7.4 *[112]. The function $F_n(x) = x^3 + Tr_n^1(x^9)$ and the Kasami-Welch family of functions $K_r(x) = x^{4^r - 2^r + 1}$ are CCZ-inequivalent on $\mathbb{F}_{2^n}$, where $n > 7$ and $\gcd(r, n) = 1$. Moreover, F_n is CCZ-inequivalent to both functions, Welch $W(x) = x^{2^\omega + 3}$ and Niho $N_\gamma(x) = x^{2^\omega + 2^\gamma - 1}$, where $n = 2\omega + 1$, $\gamma = \frac{3\omega+1}{2}$ if ω is odd, and $\gamma = \frac{\omega}{2}$ if ω is even.*

Following is the coefficient—equaled to zero—of the linear term of degree 2^k in the equation that is generated when it is assumed that F' and F_n are CCZ-equivalent (see the body of Theorem 7.4 in [112]):

$$C^{2^\sigma} a_k + a_{k-\sigma}^{2^\sigma} C + a_{k-\sigma-1}^{2^\sigma} a_{k-1} + \boldsymbol{\epsilon}_{r,\frac{n}{3}} \left(b_{k-1+r-\sigma}^{2^\sigma} b_{k-1} + b_{k-1-\sigma}^{2^\sigma} b_{k-1+r} \right) +$$
$$\boldsymbol{\epsilon}_{r,\frac{n}{2}} \left(a_{k-1+r-\sigma}^{2^\sigma} b_{k-1} + b_{k-1-\sigma}^{2^\sigma} a_{k-1+r} \right) - a'_k + \sum_{\gamma \in \mathbb{Z}/n\mathbb{Z}} \Bigg(C^8 a_{k-\gamma} + a_{k-\gamma-3}^8 C$$
$$+ a_{k-\gamma-4}^8 a_{k-\gamma-1} + \boldsymbol{\epsilon}_{r,\frac{n}{3}} \left(b_{r+k-\gamma-4}^8 b_{k-\gamma-1} + b_{k-\gamma-4}^8 b_{r+k-\gamma-1} \right) + \boldsymbol{\epsilon}_{r,\frac{n}{2}} \Big($$
$$a_{r+k-\gamma-4}^8 b_{k-\gamma-1} + b_{k-\gamma-4}^8 a_{r+k-\gamma-1} \Big) \Bigg)^{2^\gamma} = 0.$$

Where the a_is, a'_is, b_is, and C define an affine permutation of $\mathbb{F}_{2^n}^2$, $\boldsymbol{\epsilon}_{i,j}$ is the Kronecker's delta, and $\sigma \geq 1$. Let $n_0 \in \mathbb{N}$, and $(n_k)_{k=1}^\infty$ a sequence of odd numbers other than 1. Let M be the domain $\mathbb{F}_{2^{n_0}}$ or any of its field extensions $\mathbb{F}_{2^{\prod_{k=0}^l n_k}}$ (for some l), or the union of all these extensions $\Omega = \bigcup_{l=1}^\infty \mathbb{F}_{2^{\prod_{k=0}^l n_k}}$. Let J_1 and J_2 be functions defined on Ω. The correspondence $J_{(n_i)_{i=0}^\infty}$ defined below is a function. $J_{(n_i)_{i=0}^\infty} : M \to M$, such that for each x in M an $J_{(n_i)_{i=0}^\infty}(x)$ is assigned as follows: set $\xi_x = \sum_{i=0}^{-1+n_0} J_2^{2^i}(x)$. If $\xi_x \in \mathbb{F}_2$, then define $J_{(n_i)_{i=0}^\infty}(x) = J_1(x) + \xi_x$, otherwise set $\xi_x = \sum_{i=0}^{-1+\prod_{k=0}^1 n_k} J_2^{2^i}(x)$. If $\xi_x \in \mathbb{F}_2$, then define $J_{(n_i)_{i=0}^\infty}(x) = J_1(x) + \xi_x$, otherwise set $\xi_x = \sum_{i=0}^{-1+\prod_{k=0}^2 n_k} J_2^{2^i}(x)$. If $\xi_x \in \mathbb{F}_2$, then define $J_{(n_i)_{i=0}^\infty}(x) = J_1(x) + \xi_x$, otherwise continue this process until ξ_x belongs to $\mathbb{F}_2$, then set $J_{(n_i)_{i=0}^\infty}(x) = J_1(x) + \xi_x$.

For every $l' > l$, the mapping $J_{(n_i)_{i=0}^\infty} : \mathbb{F}_{2^{\prod_{k=0}^{l'} n_k}} \to \mathbb{F}_{2^{\prod_{k=0}^{l'} n_k}}$ differs from Budaghyan's APN $x^3 + Tr_n^1(x^9)$: $\mathbb{F}_{2^{\prod_{k=0}^{l'} n_k}} \to \mathbb{F}_{2^{\prod_{k=0}^{l'} n_k}}$, where $n = \prod_{k=0}^l n_k$,

$J_1(x) = x^{2^\sigma+1}$, σ is chosen as 1, and $J_2(x) = x^9$. If a $(n_i)_{i=0}^{\infty}$ is established, then the *Carranza-Budaghyan* function (shortened) $J_{(n_i)_{i=0}^{\infty}}$ on M can also be named by J; R. Carranza constructed this new function by transforming an appropriate infinite sequence (corresponding to $(n_i)_{i=0}^{\infty}$) of different switching neighbors APNs of Budaghyan et al.; and also showed that the Conjecture-BCL (in [112]) proposed by Budaghyan et al. also holds for the other three main APN mappings in Table 1 (Kasami-Welch, Welch, and Niho (in its two subclasses)), guaranteeing in one fell swoop that $J_{(n_i)_{i=0}^{\infty}}$ has no equivalent with any APN function and that $J_{(n_i)_{i=0}^{\infty}}$ is *Exceptional* APN, read Figure 4. Only 3 exceptional APN families are known; see Table 2.

Table 2: The two Exceptional APN Monomial Classes and the Non-polynomial Class (it is enough to choose different sequences $(n_i)_{i=1}^{\infty}$, while n_0 can be chosen even or odd)

Function Name	Exceptional APN Functions	Constraints	Ref.
Gold (quadratic)	$x^{2^r+1} : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$	$gcd(r,n) = 1$	[72] [104]
Kasami-Welch (non-quadratic if it is not AE to x^3)	$x^{2^{2r}-2^r+1} : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$	$gcd(r,n) = 1$	[81] [78] [112]
Carranza-Budaghyan (non-polynomial, counting non-monomials)	$J_{(n_i)_{i=0}^{\infty}} : \bigcup_{l=0}^{\infty} \mathbb{F}_{2^{\Pi_{k=0}^{l} n_k}} \to \bigcup_{l=0}^{\infty} \mathbb{F}_{2^{\Pi_{k=0}^{l} n_k}}$ for $J_1(x) = x^{2^\sigma+1}$, $\sigma = 1$, $J_2(x) = x^9$	$n_k (\neq 1)$ are odd numbers, $\forall\, k \geq 1$, n_0 is *arbitrary* in $\mathbb{N}$	[112]

7.1.1 Mappings Applied in Conjecture-BCL

As far as the CCZ-inequivalence between the Gold family and the APN function (F_n) of Budaghyan-Carlet-Leander[6] (2009), they show that the following affine mapping on variable X, $L_1(X, F(X)) = L(X) + L'(F(X)) = d'' + Tr_n^1(d_1'X + d_2'F(X))$ is not a permutation (refer to [26]), where $d_1', d_2', d'' \in \mathbb{F}_{2^n}$, by virtue of the inequality:

$$|L_1(X, F(X))| \leq 2, \forall X \in \mathbb{F}_{2^n}.$$

As regards the CCZ-inequivalence between the Kasami-Welch large family (also the Welch and Niho families) and the beautiful Budaghyan[7]-Carlet-Leander Gold-based APN function, R. Carranza (2024) showed that the affine mapping $\tilde{L}_1(X) = (\eta + \zeta)(X) + C$ cannot be a permutation (refer to [112]), where $\chi_{l''}, C \in \mathbb{F}_{2^n}$. For this purpose, he obtained the equation

$$\eta + \zeta = \chi_{l''} (\eta + \zeta)^2 + (\eta + \zeta)^4$$

[6](recipient of the *George Boole International Prize*)

[7](winner of the *Emil Artin Junior Prize in Mathematics*)

The following inequality holds:

$$|\tilde{L}_1(\mathbb{F}_{2^n})| \leq 4.$$

It is decisive that the research continues in both directions with the common spirit of determining which functions are not Exceptional APN (in particular, there has been progress in this direction, considering the polynomial class) and which are. **Open problem 10** Discuss whether there are new Exceptional APN functions. Start by investigating whether it is possible to build another Exceptional APN function being: the sum of a Gold or the Kasami function with a Boolean function piecewise-defined along the field extensions. **Open problem 11** Similarly, what are the formulas for *Exceptional differentially δ-uniform functions*?, especially—to provide greater security—for δ as small as $2 < \delta \leq 6$.

8 Algebraic-Differential Analysis of Highly Resistant Functions (Part I)

Let's test a cypher implemented based upon any of the current x^{-1}-dependent functions, we mainly mean that we will see what opportunities these types of functions will have against the $\mathbf{AAtt}_{\mathbb{F}_{2^n}}(4)$-algebraic attack that we will describe shortly.

Definition 8.1 *We will say that a function $f : \mathbb{F}_2^n \to \mathbb{F}_2^n$ is x^{-1}–4th-dependent, which in short we call x^{-1}-dependent, if it has the form $F_{(\mathfrak{Y};\mathbf{B})}$ in Theorem 8.2, and that it is not resistant against an algebraic attack of 2-weight equal to 4 (this already includes algebraic attacks with a 2-weight less than 4).*

We state our next straightforward but very useful and decisive principle.

Theorem 8.2 *Let* $F_{(\mathfrak{Y};\mathbf{B})}(x) = \begin{cases} F(x), x \in \mathbf{B} \setminus \mathsf{InvIma}\big(F-\mathfrak{Y}\big)(0) \\ x^{2^n-2}, x \in \big(\mathbb{F}_{2^n} \setminus \mathbf{B}\big) \bigcup \mathsf{InvIma}\big(F-\mathfrak{Y}\big)(0) \end{cases}$ *be a function defined on $\mathbb{F}_{2^n}$, where F is a function defined on $\mathbb{F}_{2^n}$, $\mathsf{InvIma}\big(F-\mathfrak{Y}\big)(0)$ is the inverse image of $\{0\}$ under the function $F-\mathfrak{Y}$, $\mathfrak{Y}(x) = x^{2^n-2}$, and $1 \leq |\mathbf{B} \setminus \mathsf{InvIma}\big(F-\mathfrak{Y}\big)(0)| \leq |\big(\mathbb{F}_{2^n} \setminus \mathbf{B}\big) \bigcup \mathsf{InvIma}\big(F-\mathfrak{Y}\big)(0)|$. Let $\xi \geq 3$, with $|\mathbf{B} \setminus \mathsf{InvIma}\big(F-\mathfrak{Y}\big)(0)| = \xi - 2$, then is established the algebraic attack of 2-weight $\max\limits_{1\leq\lambda\leq\xi+1} w_2(\lambda)$ on $F_{(\mathfrak{Y};\mathbf{B})}$ given by the equation below:*

$$x\left(\prod_{\gamma\in\mathbf{B}\setminus\mathsf{InvIma}\left(F-\mathfrak{Y}\right)(0)} x+\gamma\right)\big(xF_{(\mathfrak{Y};\mathbf{B})}(x)+1\big) = 0.$$

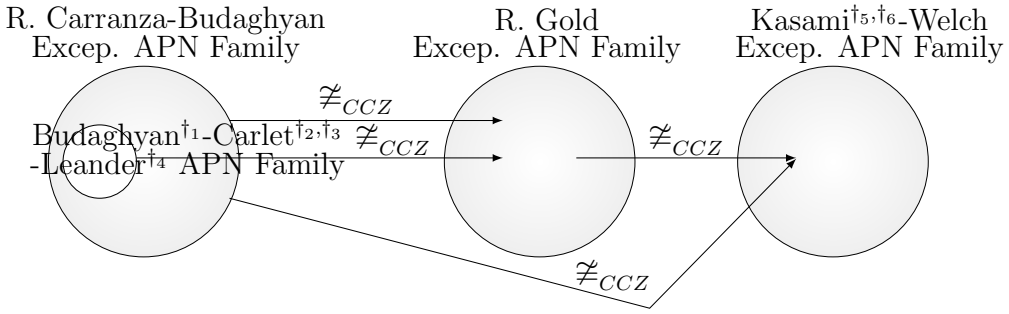

Figure 4: **The Three Exceptional APN Function Families.** $\not\cong_{CCZ}$: denotes CCZ-inequivalence. Excep.: short for exceptional. $\mathcal{W}_f$: denotes the Walsh-Hadamard spectrum of a function f. F_n: denotes the function of L. Budaghyan, C. Carlet, and G. Leander. $J_{(n_i)_{i=0}^{\infty}} : \bigcup_{l=0}^{\infty} \mathbb{F}_{2^{\Pi_{k=0}^{l} n_k}} \rightarrow \bigcup_{l=0}^{\infty} \mathbb{F}_{2^{\Pi_{k=0}^{l} n_k}}$ denotes the R. Carranza function. The Kasami-Welch (K-W) and Gold (Go) families where $\gcd(r,n) = 1$, and $J_{(n_i)_{i=0}^{\infty}}$, have the same Walsh-Hadamard spectrum, the same uniform differentiability (APN), and are exceptional APN, becoming almost indistinguishable. Facts:
(1). F. Hernando and G. McGuire proved that it is actually a theorem, the conjecture that the monomial functions $f(x) = x^t$ that are exceptional APN are only the Gold and Kasami-Welch families with $\gcd(r,n) = 1$ [77]. The strictly polynomial case remains open [5].
(2). $\mathcal{W}_{K\text{-}W} = \mathcal{W}_{Go}$ (J. F. Dillon and Hans Dobbertin [55, 56]).
(3). Gold functions are pairwise CCZ-inequivalent and they are in general CCZ-inequivalent to Kasami-Welch (and the Welch) functions (L. Budaghyan, C. Carlet, and G. Leander [25]).
(4). $\mathcal{W}_{F_n} = \mathcal{W}_{Go}$ (Carl Bracken, Eimear Byrne, Nadya Markin, and Gary McGuire [16]).
(5). $F_n \not\cong_{CCZ} Go$ (L. Budaghyan, C. Carlet, and G. Leander [26]), so $J_{(n_i)_{i=0}^{\infty}} \not\cong_{CCZ} Go$, where $J_{(n_i)_{i=0}^{\infty}}$ goes from and to the appropriate extension $\mathbb{F}_{2^n}$ of degree $n = \prod_{k=0}^{l} n_k$.
(6) $J_{(n_i)_{i=0}^{\infty}} \not\cong_{CCZ} K\text{-}W$, $F_n \not\cong_{CCZ} K\text{-}W$ (Conjecture-BCL: proved by R. Carranza [112]), where $J_{(n_i)_{i=0}^{\infty}}$ goes from and to the appropriate field extension $\mathbb{F}_{2^n}$ of degree $n = \prod_{k=0}^{l} n_k$.
(7). Construction of the non-polynomial exceptional APN function family $J_{(n_i)_{i=0}^{\infty}}$ (R. Carranza [112]).
$\dagger_1$: Emil Artin Junior Prize in Mathematics, $\dagger_2$: Mathematics in France Leader Award, $\dagger_3$: Computer Science in France Leader Award, $\dagger_4$: George Boole International Prize, $\dagger_5$: Claude E. Shannon Award, $\dagger_6$: Okawa Prize. **Open Problem 32.** Is there any pic similar to this for $\mathbb{F}_{p^n}$ with p odd?. **Open Problem 33.** (this problem will matter for p even) can there be a fourth Exceptional APN family?

Indeed, the attack is measured by $\max\limits_{1\leq\lambda\leq\xi+1} w_2(\lambda)$, that is, by ξ. Thus, a sufficiently strong $F_{(\mathfrak{Y};\mathbf{B})}$ will require a sufficiently large $|\mathbf{B}\diagdown \mathsf{InvIma}\big(F-\mathfrak{Y}\big)(0)|$. The set of equations with 2-weight at most $\max\limits_{1\leq\lambda\leq\xi+1} w_2(\lambda)$ that correspond to currently existing functions of the type $F_{(\mathfrak{Y};\mathbf{B})}$ as determined in Theorem 8.2 is denoted by $\mathbf{INE}_{\mathbb{F}_{2^n}}\big(\max\limits_{1\leq\lambda\leq\xi+1} w_2(\lambda)\big)$. On the other hand, we define the class consisting of the following polynomial equations containing polynomials of algebraic degree at most four,

$\mathbf{AAtt}_{\mathbb{F}_{2^n}}(4) = \{X^2Y = X,\ (X^2+X)XY = X^2+X,\ (X+(\alpha_0^{-1}+\alpha_{m+1}^{-1})X^2)\prod\limits_{i=0}^{m}(X+\alpha_i) = X^2\prod\limits_{i=0}^{m}(X+\alpha_i)Y,\ X^2(X+a)(X+a^{-1})(X+a+1)(X+a^{-1}+1)(X+(a+1)^{-1})(X+(a+1)^{-1}+1)Y = X(X+a)(X+a^{-1})(X+a+1)(X+a^{-1}+1)(X+(a+1)^{-1})(X+(a+1)^{-1}+1)$, $(X^{2^k}+X)XY = X^{2^k}+X$, $X^2(X+\omega)(X+\omega^2)Y = X(X+\omega)(X+\omega^2)$, $(X^2+X^5+X^6)Y = X+X^4+X^5$, $(X^{2^{k_1}}+X)(X^{2^{k_2}}+X)XY = (X^{2^{k_1}}+X)(X^{2^{k_2}}+X)$, $(X^4+X^2v^2)Y = X^3+Xv^2$, $(X^2+uX)(X^2+vX)Y = X(X+u)(X+v)$, $(X^{2^s}+X)XY = X^{2^s}+X$, $(X^{2^s}+X)Y = C(X)$, $(X^3+1)Y = Q(X)$, $(X^{2^k}+X)Y = C(X)$, $XY = X^{2^t}$, $(X^{2^s}+X+t_1)(X^4+t_2^2X^2)Y = C(X)\}$, where $m \leq 11$, while, C, Q, and A denote some element of the set of cubic, quadratic, and affine functions, respectively; the involved coefficients belong to the field extension $\mathbb{F}_{2^n}$, and the parameters in the exponents are greater than or equal to 1. This special set, $\mathbf{AAtt}_{\mathbb{F}_{2^n}}(4)$, establishes the algebraic attacks on the S-boxes that appear in Tables 3 to 7; among such S-boxes there are some diff. 6(also 8)-uniform, but notoriously almost all are diff. 4-uniform, also, $\mathbf{AAtt}_{\mathbb{F}_{2^n}}(4)$ contains fundamental part of $\mathbf{INE}_{\mathbb{F}_{2^n}}(4)$.

This attack leaves vulnerable the vast diversity of existing nonlinear functions built as x^{-1}-dependent, starting from the mother function x^{-1}; in other words, practically no known diff. 4-uniform function is not dependent on x^{-1}.

Regarding the leading properties of S-boxes. It can be considered that in block ciphers (for instance: XSL ciphers), the only non-linear part is their S-boxes, meaning that the security of the block cipher rests on the strength of the S-box they use. Among the conspicuous design criteria for Boolean functions in an S-box $F = (F_i) : \mathbb{F}_2^n \to \mathbb{F}_2^n$, where $y_i = F_i(x_1, \cdots, x_n)$, we list the following:

$a1$). Should be highly nonlinear to provide confusion (refer to Definition 1.17);

$a2$). Any F_i should have a high algebraic degree (to provide resistance against algebraic attacks);

$a3$). A rarely applied aspect of S-box design is that there should not be any implicit equation $Q(x_1, \cdots, x_n, y_1, \cdots, y_n) = 0$ with a low algebraic degree. Furthermore, the greater the number of these implicit equations, the more compromised the security of the block cipher is. **Note.** We recommend that all

researchers in this domain consider this important property in their functions.

The design criterion for a substitution transformation (F), including round functions of a DES-like cipher, is identified by Kaisa Nyberg[1] [104] as follows:

$b1$). F must be balanced (automatically satisfied if F is a permutation);

$b2$). High nonlinearity, large distance from affine functions ($NL(F)$ high);

$b3$). High nonlinear order, the degrees of the output bit functions are large (to provide resistance to algebraic attacks);

$b4$) Resistance against differential cryptanalysis (δ_F low; since the S-Box performs the crucial task of: Confusion); and

$b5$) Efficient construction and computability.

One way to place the secret key K inside the S-box S is such that the S-box to be used is $f(x) := S(x + K) : \mathbb{F}_2^n \to \mathbb{F}_2^m$.

Regarding the Rijndael S-box (encryption adopted by the U.S. National Institute of Standards and Technology, replacing the Data Encryption Standard algorithm), this is the multiplicative inverse function on $\mathbb{F}_{256}$, which we denote as $\tilde{y}$, composed (to resist plain attacks of an algebraic nature) of a multivariate affine mapping on $\mathbb{F}_2^8$, denoted by $\texttt{Aff}$, which can also be represented on $\mathbb{F}_{2^8}$. That is, $y = \text{Rijndael S-box}(x) = \texttt{Aff}(\tilde{y}(x))$. The fact $x = \tilde{y}x^2$ is equivalent to having 8 bi-affine equations between the variables x_i, y_j, since $\texttt{Aff}$ is a permutation. In a similar way, one can obtain a collection of equations with which we break the Rijndael security recovering its secret key. In general, when an S-box is an affine mapping of the multiplicative inverse function on $\mathbb{F}_{2^n}$, one can obtain a system of bi-affine equations to recover the secret key. EA-equivalent S-boxes to the multiplicative inverse can be ideal against attacks classified as linear, differential and high-order differential [30, 104], but it has been investigated by Courtois and Pieprzyk [47] that they are the worst possible in the sense of producing many bi-affine equations, as pointed out by the ($a3$) criterion for the design of an S-box.

From the list of permutations in Tables 3 to 7 we can identify possible candidates for the following (with an earlier version proposed by Courtois and Pieprzyk; note that this new version is more restrictive) **open problem 12:** *of finding any non-linear S-box F not EA-equivalent (preferably CCZ-inequivalent) to the multiplicative inverse function over some field $\mathbb{F}_{2^n}$ that admits so many implicit equations of the form $Q(x_1, \cdots, x_n, y_1, \cdots, y_n) = 0$ such that Q has a low algebraic degree ($d^0(Q)$ can be considered to be in the range 2 to 4), but such that both F defining the explicit equation $y - F(x) = 0$ and its inverse function F^{-1} are of high algebraic degree.* Candidates should be carefully selected to ensure that they are not CCZ-equivalent to the multiplicative inverse function (most of them comply with this because the large percentage of crypto properties listed in these tables are CCZ-invariant; a CCZ-invariant

[1] (winner of the *Magnus Ehrnrooth Prize*)

often serves as an indicator of whether two functions are CCZ-equivalent or not).

From $\mathbf{AAtt}_{\mathbb{F}_{2^n}}(4)$ we can observe the subclass of bi-affine equations and more generally the quadratic $\mathbf{INE}_{\mathbb{F}_{2^n}}(2)\bigcup\{XY = X^{2^t}\}$, where $\mathbf{INE}_{\mathbb{F}_{2^n}}(2) = \{X + X^2Y = 0,\ X^3 + Xv^2 + (X^4 + X^2v^2)Y = 0\}$. Moreover, with respect to $X^3 + Xv^2 + (X^4 + X^2v^2)Y = 0$, we obtain a bi-affine system very similar to the one governing the multiplicative inverse, that is, n equations are true with very high probability no less than $1 - \frac{1}{2^{n-1}}$, and another $2n$ that are true with probability no less than $1 - \frac{1}{2^n}$, this system applies to an S-box (being diff. 4-uniform over fields with degree of the form $n = 4r + 2$, and diff. 6-uniform when $n = 4r$) CCZ-inequivalent to the multiplicative inverse whose $NL(f)$ values in both generally differ. Further, it is not difficult to show that $I_{(0,v)}(X)$ and its inverse have the same optimal algebraic degree, based on Affine-equivalence, noting that the inverse satisfies $I^{-1}_{(0,v)} - I_{(0,\frac{1}{v})} \equiv 0$ for $v \neq 0$, and also on the **Theorem**: For any (X, Y) in $\mathbb{F}^2_{2^n}$, $(X+Y)^{-1} = X^{-1} + Y^{-1} + \sum_{i=1}^{2^{n-1}-2} Y^{2i}X^{2^n-2i-2}$, where X^{-1} denotes the multiplicative inverse of X. In this very gratifying way, we solve the open problem of the previous paragraph, and in particular the version proposed by Courtois and Pieprzyk. The function referred to by the equation $XY = X^{2^t}$ (produces bi-affine equations) isn't a x^{-1}-dependent (further, it is CCZ-inequivalent to x^{-1}) among those attacked by the $\mathbf{AAtt}_{\mathbb{F}_{2^n}}(4)$-*algebraic attack*.

By applying this algebraic attack on all functions corresponding to the class $\mathbf{AAtt}_{\mathbb{F}_{2^n}}(4)$ we guarantee $n-1$ bi-affine equations with constant term equal to zero, being true for $X = 0$, which are true with probability greater than or equal to $1 - \frac{|\mathbf{B}\setminus \mathsf{InvIma}(F-\mathfrak{Y})(0)|}{2^n}$, plus one more equation that is true with probability greater than or equal to $1 - \frac{|(\mathbf{B}\setminus \mathsf{InvIma}(F-\mathfrak{Y})(0))\bigcup\{0\}|}{2^n}$, since $XY = 1$ for all $X \notin \big(\mathbf{B}\setminus \mathsf{InvIma}\big(F-\mathfrak{Y}\big)(0)\big)\bigcup\{0\}$. Further, the identity $X^{2^\theta} - X^{2^{\theta+1}}Y^{2^\theta} = Y^{2^\theta} - Y^{2^{\theta+1}}X^{2^\theta} = 0$ holds for arbitrary $\theta \geq 0$ with probability greater than or equal to $1 - \frac{|(\mathbf{B}\setminus \mathsf{InvIma}(F-\mathfrak{Y})(0))\setminus\{0\}|}{2^n}$, and from which other bi-affine equations can be produced. In this section we have investigated an attack on all block ciphers whose security shielding is given by some member listed in the class $\mathbf{AAtt}_{\mathbb{F}_{2^n}}(4)$, in this way we contribute to the novel theoretical-practical attack investigated in 2002 by Courtois and Pieprzyk, generalizing it to a world of S-boxes that are non-CCZ-equivalent to the multiplicative inverse function.

8.1 Algebraic Attack to the Best Current Permutations

We have investigated each of the currently known competitive differentially δ-uniform (non-APN) permutations on $\mathbb{F}_{2^n}$ for degree n even (this field is of central interest due to the problems involved; not a single infinite family of permutations such that $\delta = 2$ has yet been found on these fields), for the best

three values of δ, i.e. $8 \geq \delta > 2$. We perform the comparison based upon the set of chief attacks as a whole, to determine the few most resistant families for n odd and n even. In this part, we address the essential cryptanalytic aspect that will lead us to the Achilles' heel of current S-BOXes.

Each of these participating families of functions—in Tables 3 to 7—is competitive, presenting some level of resistance against at least one of the dominant cryptographic attacks: linear, differential, and algebraic degree based attacks. See Table 1 in [127] for the cryptographic properties of functions. Almost every function in this list is tied to the algebraic degree $n-1$ (classified as x^{-1}-dependent, see Definition 8.1), which unfortunately cannot be removed by EA transformations, since it is an EA-invariant; I would suggest non-trivial transformations of the graph $\mathcal{G}_f$. **Remark.** In the face of a sudden algebraic attack based on the parameter $n-1$, almost every current diff. 4-uniform function is simply helpless; there are members of the diff. 4-uniform family that do not exhibit such a weakness. One of our functions is also affected by this algebraic attack, but not our other functions. Remember that this topic is hot, so it attracts persevering people. All participating functions present architectures with the potential to be applied to more than one problem. After such an attack, effective results are almost nonexistent. **Open Problem 13.** We invite the design of new families of permutations—even almost permutations (f) with $\Delta_f \leq 6$, for example, functions that are between 2-to-1 and 1-to-1—with high algebraic degrees without being extremal, keeping $NL(f)$ high and Δ_f low (we recommend exploring the $\Delta_f = 6$ case in more detail). Following our signature style, we achieve top-notch results. Other authors obtain top-tier functions with different cryptographic properties than ours.

The permutation $x^s + Tr_n^1(x^s)$ for $s = -1$ presents an attractive formula, but it is EA-Equivalent to x^{-1}; as for the permutation $x^{2^j+1} + \gamma Tr_n^1(x^{2^j+1})$ [38] for j and n relatively prime, and $Tr_n^1(\gamma) = 0$, this is A-Equivalent to the Gold (APN). Either way, both are attractive instances. Concerning tables 3 to 7, the notations $Tr(x)$, $tr(x)$, $Tr_1^n(x)$, $Tr_n^1(x)$, used by other authors mean $Tr_n^1(x)$, we will prefer to keep some notations where appropriate. Notes:

Weakness (1^*): having a not high $d^0(f)$.

Weakness (2^*): only one (or two) function(s) per finite field.

Just a note: (3^*): it was obtained as a piecewise function or not exhibit an explicit polynomial formula.

Just a note: (4^*): the given non-monomial function, f, exhibits an explicit polynomial formula.

Just a note: (5^*): F^{-1} is the inverse function of F. Whereas just x^{-1} denotes the multiplicative inverse function on $\mathbb{F}_{2^n}$ (i.e. $\frac{1}{x}$, with the convention that $0^{-1} := 0$).

Just a note: (6^*): $\mathcal{L}_1$ and $\mathcal{L}_2$ are affine permutations over the proper subfield $\mathbb{F}_{2^{\frac{n}{5}}}$, where $5 \mid n$.

Weakness (7*): is immobilized by the $\mathbf{AAtt}_{\mathbb{F}_{2^n}}(4)$-algebraic attack.

Weakness: we are aware that there is a type of attack that, if not on the encoding, then on the decoding, that is, targeting the inverse function f^{-1} when it is subject to a poor algebraic degree.

We recall that the inverse function of any permutation (say f) shares with f the following: $\Delta_{f^{-1}} = \Delta_f$ and $NL(f^{-1}) = NL(f)$; the second property was observed by Kaisa Nyberg (1992, [103]).

Table 3:

Competitive Diff. δ-Uniform Permutation f ($8 \geq \delta > 2$)	n: **EVEN DEGREE** (the degree of interest) Constraints:	Lower Bound on Nonlinearity	$d^0(f)$	Ref.
With $\Delta(f) = 4$:				
x^{2^r+1}	$n = 2k$, k odd, $\gcd(r, n) = 2$	$2^{n-1} - 2^{\frac{n}{2}}$	2	[72, 104]
$x^{2^{2r}-2^r+1}$	$n = 2k$, k odd, $\gcd(r, n) = 2$	$2^{n-1} - 2^{\frac{n}{2}}$	$r + 1$	[81]
x^{-1} ($:= x^{2^n-2}$)	n is **any even**, (2*, 7*)	$2^{n-1} - 2^{\frac{n}{2}}$	$n - 1$	[104]
$x^{2^{2r}+2^r+1}$ (2*)	$n = 4r$, r odd	$2^{n-1} - 2^{\frac{n}{2}}$	3	[59, 18]
$\alpha x^{2^s+1} + \alpha^{2^k} x^{2^{-k}+2^{k+s}}$ (quadratic binomial) (4*)	$n = 3k$, k even, $(k, 3) = 1$, $k/2$ odd, $\gcd(s, 3k) = 2$, $3 \mid k + s$, α : primitive element of $\mathbb{F}_{2^n}$	$2^{n-1} - 2^{\frac{n}{2}}$	2	[17]
$F_u(x)$ and $F'_u(x) = F_u(x) + x$ (3*) From applying EA-equivalence to quadratic APN bijections. Always, the inverse of F_u can be attacked instead, as long as F_u^{-1} has a low $d^0(F_u^{-1})$	Theorem 4 (and 5), Proposition 1, 2 in [93] F_u, F'_u, ${F'_u}^{-1}$ F_u^{-1}	$2^{n-1} - 2^{\frac{n}{2}}$	$\frac{n+2}{2} \leq 3$	[32, 93]
$F'(x)$ (3*)	Theorem 6 in [93] $n + 1 = 3k$, $k \in \mathbb{N}$ F' ${F'}^{-1}$	$2^{n-1} - 2^{\frac{n}{2}}$	$\frac{n+2}{2} \leq 7$	[32, 93]
$x^{\frac{1}{2^i+1}} + Tr(x) = F_{i,\gamma}(x)$ (EA-E to the inverse of the Gold). Its inverse $F_{i,\gamma}^{-1}$ can be attacked instead, since $d^0(F_{i,\gamma}^{-1})$ is too low	$\gamma = 1$, $n = 2m$, m odd $\gcd(i, n) = 2$, $2 \leq i \leq m$ (4*) $d^0(F_{i,\gamma}^{-1}) \leq 3$	$2^{n-1} - 2^{\frac{n}{2}}$	$\frac{n}{2}$	[38]
$\pi(x)^{-1} = \sum_{i=0}^{2^n-3} x^i$ (2*), (4*), (7*)	$n = 2k$, k odd, Corollary 1 in [92], applies the transposition $\pi = (0, 1)$	$2^{n-1} - 2^{\frac{n}{2}}$	$n - 1$	[92]
$\pi(x)^{-1} = x^{-1} + \sum_{i=0}^{m}(x + \alpha_i)^{2^n-1}(\alpha_i^{-1} + \alpha_{i+1}^{-1})$ by choosing a cycle $\pi(x) = (\alpha_0, \cdots, \alpha_m)$ over $\mathbb{F}_{2^n}$, (4*). If $m \leq 3$: $Q(x)\pi(x)^{-1} = Q'(x)$	$n = 2k$, k odd, $m \geq 2$. Sufficient conditions for $\pi(x)^{-1}$ having differential uniformity 4 are given. Q, Q' are the quadratics: $Q : x^2 \prod_{i=0}^{m}(x + \alpha_i)$ $Q' : (x + (\alpha_0^{-1} + \alpha_{m+1}^{-1})$ $x^2) \prod_{i=0}^{m}(x + \alpha_i)$	$2^{n-1} - 2^{\frac{n}{2}} - m - 1$		[92]
First class in [109] $x^{2^n-2} + Tr(x^2(x + 1)^{2^n-2})$ (4*), (2*)		$2^{n-1} - (2)2^{\frac{n}{2}} - 2$	$n - 1$	[109]
Second class in [109] $x^{2^n-2} + Tr(x^{(2^n-2)d} + (x^{2^n-2} + 1)^d)$ (4*)	$d = 3(2^t + 1)$, $2 \leq t \leq n/2 - 1$	$2^{n-2} - 2^{\frac{n}{2}-1} - 1$	$n - 1$	[109]

Table 4: -continued from previous page

Competitive Diff. δ-Uniform Permutation f	n: **EVEN DEGREE** (the degree of interest) Constraints:	Lower Bound on Nonlinearity	$d^0(f)$	Ref.
With $\Delta(f) = 4$:				
$I_F(x) = F\left(\frac{1}{F^{-1}(x)}\right)$, Carlitz form $F = [a_{m+1}, a_m, \cdots, a_2, a_1 + a_0 x]$ (3^*), (5^*)	Construction 1 in [79]	$2^{n-1} - 2^{\frac{n}{2}} - 4$	$n-1$	[79]
	Construction 2 in [79] F^{-1} denotes the compositional inverse of F	$2^{n-1} - 2^{\frac{n}{2}} - 6$	$n-1$	
$F(x)$ (3^*)	$U = U_{\max}$	$2^{n-1} - (3)2^{\frac{n}{2}} - 2$	$n-1$	[127]
	$0 < \lvert U\rvert < \frac{2^{n-1} - 2^{\frac{n}{2}} - 6}{3}$	$2^{n-1} - 2^{\frac{n}{2}} - \lvert U\rvert$	$n-1$	
	$U = U_{m_0}$	$2^{n-1} - 2^{\frac{n}{2}+2} - 2$	$n-1$	
	$U = U_{m_1}$	$2^{n-1} - 2^{\frac{n}{2}+2} - 2$	$n-1$	
$f(x) = x^{-1} + (1 + (x^{2^k} + x)^{2^n - 1})$ (4^*), (7^*)	k is even or $k = 1, 3$ & $\frac{n}{2}$ is odd (Theor. 3.4)	$2^{n-1} - 2^{\frac{n}{2}} - 2^k$ (Theorem 1 in ArXiv)	$n-1$	[140]
$f(x) = x^{-1} + (1 + (x^2 + (\omega + \omega^2)x + 1)^{2^n - 1})$ $(2^*, 4^*)$, (7^*)	$\frac{n}{2}$ is odd, $\omega^3 = 1$ in Theorem 3.14	$2^{n-1} - 2^{\frac{n}{2}} - 2$ (Theorem 6 in ArXiv)	$n-1$	[140]
$f(x) = x^{-1} + \delta_S(x)$ $S = \{x \in \mathbb{F}_{2^n}; x^{-4} = x^{-1} + 1\}$ $(2^*, 4^*)$, (7^*)	$\frac{n}{4}$ is odd, $\gcd(n, 5) = 1$ (Theorem 3.15)	$2^{n-1} - 2^{\frac{n}{2}} - 4$ (Theorem 7 in ArXiv)	$n-1$	[140]
$f(x) = x^{-1} + \delta_S(x)$ $S = \mathbb{F}_{2^{k_1}} \cup \mathbb{F}_{2^{k_2}}$ (4^*), (7^*) Besides, the functions in Theorems 3.8-3.9 in [140] have the same formula as f	$k1 \mid k2 \Rightarrow$ $k_1 = 3$, $\gcd(k_2, 3) = 1 \Rightarrow$ (Proposition 4.4)	$2^{n-1} - \lfloor 2^{\frac{n}{2}} \rfloor - \lfloor 2^{\frac{k_2}{2}+1} \rfloor$ $2^{n-1} - \lfloor 2^{\frac{n}{2}} \rfloor - \lfloor 2^{\frac{k_2}{2}+1} \rfloor - 6$ (Proposition 3 in ArXiv)	$n-1$ $n-1$	[140]
$F = Inv \circ (0,1)(\alpha, \beta)$ (the composition of Inv with disjoint cycles) The elements in $\{0, 1, \alpha, \beta\}$ are distinct. $Inv(x) = x^{-1}$ (3^*)	n: **any even**. Sufficient conditions for F with differential uniformity 4 are given. F (in 2022) generalizes $\pi(x)^{-1}$ in [92] (when $0 \in P$). **Continued-open research** on F.	$2^{n-1} - 2^{\frac{n}{2}} - 2$ More generally: $2^{n-1} - 2^{\frac{n}{2}} - \#P$ $4 \leq \#P$: size of P (set of all elements in the component cycles of F)		[80]
$F = \begin{cases} (x+1)^{-1} + 1, & x \in U \\ x^{-1}, & x \in \mathbb{F}_{2^n} \setminus U \end{cases}$ (3^*), (7^*): If $U = S_a$: $x^2(\prod_{l \in U} x + l)F(x) = x \prod_{l \in U} x + l$, i.e. a cubic factor times F gives another cubic factor	$4 \leq n$ (**any even**) U(union of the sets S_a) $U \neq \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^2}$, $a \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^2}$, $S_a = \{a, a^{-1}, a+1, (a+1)^{-1}, a^{-1}+1, (a+1)^{-1}+1\}$	$2^{n-1} - 2^{\frac{n}{2}} - \lvert U\rvert$ (if $\lvert U\rvert \leq 2^{n-1} - 2$) $\lvert U\rvert$ is a multiple of 6. Note: S_a and S_b are disjoint iff $b \notin S_a$	$n-1$	[134]
$(x+v)^{-1} + v(x^2 + vx)^{-1} = I_{(0,v)}(x)$ (4^*), (7^*)	$\frac{n}{2} = 2r + 1$ $v \neq 0$, $\Delta(I_{(0,v)}) \leq 4$	$2^{n-1} - 2^{\frac{n}{2}} - 2$		[136]
$I_{(u,v)}(x) = \begin{cases} v^{-1}, & x = u \\ u^{-1}, & x = v \\ x^{-1}, & x \neq u, v \end{cases}$ Its differentiability does not change if it is slightly generalized to a function $L_2 \circ I_{(L_1(u), L_1(v))} \circ L_1$, through affine functions L_1, L_2. If we take L_2 as a permutation, we also preserve the nonlinearity	n is **any even**, $u \neq v$, $u \neq 0$, $v \neq 0$, $Tr(uv^{-1}) = Tr(u^{-1}v) = 1$ L_1: affine permutation (7^*)	$2^{n-1} - 2^{\frac{n}{2}} - 2$		[136]
$f_1 = x^{-1} + t(x^{2^s} + x)^{2^n - 1} + t$ (4^*), (7^*)	$1st$ construction in [138] $t \in \mathbb{F}_{2^s}^*$	$2^{n-1} - 2^{\frac{n}{2}} - 2^s$	$n-1$	[138]
$f_2 = t_1 x^{-1} + ((t_1+1)x^{-1} + t_2)(x^{2^s} + x)^{2^n - 1} + t_2$ (4^*), (7^*)	$2nd$ construction in [138] $t_1, t_2 \in \mathbb{F}_{2^s}$ $Tr(t_1^{-1}) = 1$	$2^{n-1} - 2^{\frac{n}{2}} - 2^s$	$n-1$	[138]

Table 5: -continued from previous page

Competitive Diff. δ-Uniform Permutation f	n: **EVEN DEGREE** (the degree of interest) Constraints:	Lower Bound on Nonlinearity	$d^0(f)$	Ref.
With $\Delta(f) = 4$:				
$\tilde{I}_{\tilde{x}_0,0}(x) = x^{2^n-2} + Tr_n^1(a_1 x^{2^n-2}) \cdots Tr_n^1(a_{n-1}x^{2^n-2})$ (4^*)	n: **any even**	$\mathbf{2^{n-1} - 2^{\frac{n}{2}} - 2}$	$n-1$	**This paper**
$\tilde{I}_{\tilde{x}_0}(x) = x^{2^n-2} + Tr_n^1(\beta_{\tilde{x}_0}^{(1)}(x^{2^n-2} + \tilde{x}_0)) \cdots Tr_n^1(\beta_{\tilde{x}_0}^{(n-1)}(x^{2^n-2} + \tilde{x}_0)) + \tilde{x}_0$ (4^*). It is interesting that: permutation $\tilde{I}_{\tilde{x}_0}$, in general, is not an involution, since $\tilde{I}_{\tilde{x}_0}(\tilde{I}_{\tilde{x}_0}(0)) \neq 0$ (for: $x_0 \notin \mathbb{F}_2$ and $x_0^2 + x_0 \neq 1$). But it has several properties in common with them.	n: **any even**	$\mathbf{2^{n-1} - 2^{\frac{n}{2}}}$	$n-1$	**This paper**
With $\Delta(f) = 6$:				
$\tilde{I}^{(n-i)}_{\tilde{x}_0,0}(x) = x^{2^n-2} + Tr_n^1(a_1 x^{2^n-2}) \cdots Tr_n^1(a_{n-i}x^{2^n-2}), \forall n-1 \geq i \geq 2$ $4 \leq \Delta(\tilde{I}^{(n-i)}_{\tilde{x}_0,0}) \leq 6$, (4^*)	n: **any even**	$\mathbf{2^{n-1} - 2^{\frac{n}{2}} - 2^i}$	$n-1$	**This paper**
F in Corollary 4.1: $f(x) + (f(x) + x^{2^k+1})(x^{2^s} + x)^{2^n-1} = F(x)$ where $f = A_1 \circ Inv \circ A_2$, $Inv(x) = x^{-1}$; (7^*)	$n = sm$, s even, $\frac{s}{2}$ and m are odd, $\gcd(k, n) = 2$. A_1, A_2 are affine permutations over $\mathbb{F}_{2^s}$, (4^*).	$2^{n-1} - 2^{\frac{n}{2}} - 2^{\frac{s}{2}+1}$	$n-1$ (if $s > 2$)	[28]
F in Corollary 4.2: $f(x) + (f(x) + x^{2^{2k}+2^k+1})(x + x^{2^s})^{2^n-1}$ where $f = A_1 \circ Inv \circ A_2$, $Inv(x) = x^{-1}$	$n = 4k = sm$, k and m are odd, A_1, A_2 are affine permutations over $\mathbb{F}_{2^s}$, (4^*)	$2^{n-1} - 2^{\frac{n}{2}} - 2^{\frac{s}{2}+1}$	$n-1$ (if $s > 4$)	[28]
$f = \begin{cases} \frac{1}{x^2+x}, \text{ if } Tr_n^1(\delta x) = 0, \\ \frac{1}{\delta x}, \text{ if } Tr_n^1(\delta x) = 1 \end{cases}$ $\Delta(f) \leq 6$, (3^*)	n (**any even**) $\delta \in \mathbb{F}_{2^n}$, $Tr_n^1(\delta) = 1$	$2^{n-1} - (3)2^{\frac{n}{2}} - 1$ (if $n \geq 6$)	$n-1$	[128]
$f_1 = x^{2^i+1} + (t_1^{2^i+1} + t_2^{2^i+1})((x^2 + (t_1+t_2)x + t_1t_2)^{2^n-1} + 1)$ $f_2 = x^{2^i+1} + (x^{2^k} + x)^{2^n-1} + 1$ $f_3 = (\omega^2 + \omega(x^3+1)^{2^n-1})x^{2^i+1}$ (4^*), (7^*): $(x^3+1)f_3(x) = Q(x)$, $(x^{2^k} + x)f_2(x) = C(x)$, Lf_1 is a cubic. Mapping f_1 is better than f_2, f_3 in the sense that L depends on $(t_1, t_2) \in (\mathbb{F}_{2^n})^2$	$\frac{n}{2}$ is odd, $t_1 \neq t_2$, $\gcd(n, i) = 2$ for f_1, f_2, and f_3. k is even, $\omega^3 = 1$ Q: quadratic function C: cubic function L: affine function	$2^{n-1} - 2^{\frac{n}{2}} - 2$ $2^{n-1} - 2^{\frac{n}{2}} - 2^{\frac{k}{2}+1}$ $2^{n-1} - 2^{\frac{n}{2}} - 2$	$n-1$ $n-1$ $n-1$	[139]
$G_t(x) = x^{2^t-1}$ where $t = \frac{kn+1}{3}$ ($k = 1$ or 2 depending of n) $(2^*, 4^*)$, (7^*)	$n \not\equiv 0 \mod (3)$, $kn \equiv 2 \mod (3)$		$\frac{kn+1}{3}$	[14]
$G_s(x) = x^{2^s-1}$ where $s = \frac{(3-k)n+2}{3}$ ($k = 1$ or 2 depending of n) $(2^*, 4^*)$, (7^*)	$n \equiv \pm 1 \mod (6)$, $kn \equiv 2 \mod (3)$		$\frac{(3-k)n+2}{3}$	[14]
$(x+v)^{-1} + v(x^2+vx)^{-1} = I_{(0,v)}(x)$ (4^*), (7^*)	$\frac{n}{2} = 2r$ $v \neq 0$	$2^{n-1} - 2^{\frac{n}{2}} - 2$		[136]
$I_{(u,v)}(x) = \begin{cases} v^{-1}, & x = u \\ u^{-1}, & x = v \\ x^{-1}, & x \neq u, v \end{cases}$ (7^*)	n: **any even** $u \neq v$, $u \neq 0$, $v \neq 0$, $Tr(uv^{-1})Tr(u^{-1}v) = 0$	$2^{n-1} - 2^{\frac{n}{2}} - 2$		[136]
$x^{-1} + \gamma Tr(x^{2^{n-1}-2^{i-1}-1}) = F_{i,\gamma}(x)$ $4 \leq \Delta(F_{i,\gamma}) \leq 6$	n (**any even**), $i \neq \frac{n}{2}$, $\gcd(2i, n) = k$, $1 \leq i < n$, $\gamma \in \mathbb{F}_{2^k}^*$, $Tr(\gamma^{2^i+1}) = 0$, (4^*)			[38]
$f_1 = x^{-1} + t(x^{2^s} + x)^{2^n-1} + t$ (4^*), (7^*)	1st construction in [138] $t \in \mathbb{F}_{2^s}^*$, s is odd, $\frac{n}{s}$ is even. $s \geq 5$, or $s = 1, 3$ and $\frac{n}{2s}$ is even	$2^{n-1} - 2^{\frac{n}{2}} - 2^s$ where $s : \begin{cases} \geq 5, \text{ if } n \text{ is even} \\ 1 \text{ or } 3, \text{ if } n/2 \text{ is even} \end{cases}$	$n-1$	[138]
$f_3 = (x+t_2)^{-1} + (x^{2^s} + x + t_1)^{2^n-1}(x^{-1} + (x+t_2)^{-1})$ $\Delta(f_3) \leq 6$, (4^*) (7^*) Based on t_1, t_2, the f_3 offers more resistance than f_1, f_2 in [138]	3rd construction in in [138] (Theorem 6) $t_2 \in \mathbb{F}_{2^s}^*$, $t_1 \in \mathbb{F}_{2^n}^*$, $Tr_n^s(t_1) = 0$,	$2^{n-1} - 2^{\frac{n}{2}} - 2^s$	$n-1$	[138]
Function families $G_{k',g}(x)$ in Theorem 4.2 (4^*), $6 \leq \Delta(G_{k',g}) \leq 8$, $\exists G_{k',g}(x)$s reaching $\Delta(G_{k',g}) = 8$.	$n = 2m$, m is odd $\gcd(n, k') = 2$	$\mathbf{2^{n-1} - 2^{\frac{n}{2}} - 2}$ (if $g = n-1$) $\mathbf{2^{n-1} - 2^{\frac{n}{2}} - 4}$ (if $g = n-2$)	$\mathbf{n-1}$	**This paper**
$G_{k',\sigma}(x) = x^{2^{k'}+1} + (x^{2^{k'}} + x + 1)Tr_n^1(a_1 x) \cdots Tr_n^1(a_\sigma x)$ (4^*), $6 \leq \Delta(G_{k',\sigma}) \leq 8$	$n = 2m$, m is odd, $\gcd(n, k') = 2$, $\sigma \leq n-2$	$\mathbf{2^{n-1} - 2^{\frac{n}{2}} - 2^{n-\sigma}}$	$\sigma + 1$ **(from 2 to n-1)**	**This paper**

Table 6:

Competitive Diff. δ-Uniform Permutation f	n: **ODD DEGREE** Constraints:	Lower Bound on Nonlinearity	$d^0(f)$	Ref.
With $\Delta(f) = 4$:				
f in Corollary 3.5-(i) in [130], (3^*), (6^*)	f in Proposition 3.8 and Corollary 3.6 ($m = \frac{n}{5} - 1$) f in Proposition 3.8 and Corollary 3.6 ($m = \frac{\frac{n}{5}+1}{2}$)	$2^{n-1} - 2^{\frac{3n-3}{4}} - 2^{\frac{k-1}{2}} - 2^{k-1}$ (where $k = \frac{n}{5}$)	$n-1$ $d^0(f) \geq \frac{9n+5}{10}$	[130]
$F = \begin{cases} (x+1)^{-1}+1, & x \in U \\ x^{-1}, & x \in \mathbb{F}_{2^n} \setminus U \end{cases}$ (3^*)	$3 \leq n$ (**any odd**) U(union of the sets S_a) $U \neq \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^2}$, $a \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^2}$, $S_a = \{a, a^{-1}, a+1, (a+1)^{-1}, a^{-1}+1, (a+1)^{-1}+1\}$	open case	$n-1$	[134]
$x^{-1} + \gamma Tr(x^{2^{n-1}-2^{i-1}-1}) = F_{i,\gamma}(x)$ $\Delta(F_{i,\gamma}) \leq 4$	n (**any odd**), $i \neq \frac{n}{2}$, $\gcd(2i, n) = k$, $1 \leq i < n$, $\gamma \in \mathbb{F}^*_{2^k}$, $Tr(\gamma^{2^i+1}) = 0$, (4^*)			[38]
$f_1 = x^{-1} + t(x^{2^s}+x)^{2^n-1} + t$ (4^*), (7^*)	$1st$ construction in [138] $t \in \mathbb{F}^*_{2^s}$	$2^{n-1} - 2^{\frac{n}{2}} - 2^s$	$n-1$	[138]
$f_2 = t_1 x^{-1} + ((t_1+1)x^{-1} + t_2)(x^{2^s}+x)^{2^n-1} + t_2$ (4^*), (7^*)	$2nd$ construction in [138] $t_1, t_2 \in \mathbb{F}_{2^s}$ $Tr(t_1^{-1}) = 1$	$2^{n-1} - 2^{\frac{n}{2}} - 2^s$	$n-1$	[138]
Function families $f_{k,g}(x)$ and $K_{i,g}(x)$ in Theorem 4.2 parameter $g = n-1$	(4^*)	$\mathbf{2^{n-1} - 2^{\frac{n-1}{2}} - 2}$	$n-1$	**This paper**
Function families $f_{k,g}(x)$ and $K_{i,g}(x)$ in Theorem 4.2 parameter $g = n-2$	(4^*)	$\mathbf{2^{n-1} - 2^{\frac{n-1}{2}} - 4}$	$n-1$	**This paper**
$\tilde{I}_{\tilde{x}_0,0}(x) = x^{2^n-2} + Tr^1_n(a_1 x^{2^n-2}) \cdots Tr^1_n(a_{n-1}x^{2^n-2})$ (4^*)	n: **any odd**	$\lfloor 2^{n-1} - 2^{\frac{n}{2}} \rfloor \epsilon_{2,\gcd(\lfloor 2^{n-1}-2^{\frac{n}{2}} \rfloor, 2)} - 2 +$ $(\lfloor 2^{n-1} - 2^{\frac{n}{2}} \rfloor - 1)\epsilon_{2,\gcd(\lfloor 2^{n-1}-2^{\frac{n}{2}} \rfloor - 1, 2)}$ where $\lfloor x \rfloor := \ell \in \mathbb{Z}$, $\ell \leq x < \ell + 1$, $\epsilon_{i,j}$: Kronecker's delta	$n-1$	**This paper**
$\tilde{I}_{\tilde{x}_0}(x) = x^{2^n-2} + Tr^1_n(\beta^{(1)}_{\tilde{x}_0}(x^{2^n-2} + \tilde{x}_0)) \cdots Tr^1_n(\beta^{(n-1)}_{\tilde{x}_0}(x^{2^n-2}+\tilde{x}_0)) + \tilde{x}_0$, (4^*)	n: **any odd**	$\lfloor 2^{n-1} - 2^{\frac{n}{2}} \rfloor \epsilon_{2,\gcd(\lfloor 2^{n-1}-2^{\frac{n}{2}} \rfloor, 2)} - 2 +$ $(\lfloor 2^{n-1} - 2^{\frac{n}{2}} \rfloor - 1)\epsilon_{2,\gcd(\lfloor 2^{n-1}-2^{\frac{n}{2}} \rfloor - 1, 2)}$	$n-1$	**This paper**
$\tilde{I}^{(n-i)}_{\tilde{x}_0,0}(x) = x^{2^n-2} + Tr^1_n(a_1 x^{2^n-2}) \cdots Tr^1_n(a_{n-i}x^{2^n-2}), \forall n-1 \geq i \geq 2$ (4^*)	n: **any odd**	$\lfloor 2^{n-1} - 2^{\frac{n}{2}} \rfloor \epsilon_{2,\gcd(\lfloor 2^{n-1}-2^{\frac{n}{2}} \rfloor, 2)} - 2^i +$ $(\lfloor 2^{n-1} - 2^{\frac{n}{2}} \rfloor - 1)\epsilon_{2,\gcd(\lfloor 2^{n-1}-2^{\frac{n}{2}} \rfloor - 1, 2)}$	$n-1$	**This paper**
With $\Delta(f) = 6$:				
$G_t(x) = x^{2^t-1}$ where $t = \frac{kn+1}{3}$ ($k = 1$ or 2 depending of n) $(2^*, 4^*)$, (7^*)	$n \not\equiv 0 \mod 3$, $kn \equiv 2 \mod 3$		$\frac{kn+1}{3}$	[14]
$G_s(x) = x^{2^s-1}$ where $s = \frac{(3-k)n+2}{3}$ ($k = 1$ or 2 depending of n) $(2^*, 4^*)$, (7^*)	$n \equiv \pm 1 \mod 6$, $kn \equiv 2 \mod 3$		$\frac{(3-k)n+2}{3}$	[14]
$G_t(x) = x^{2^t-1}$ ($\Delta(G_t) = 6$ or 8 depending of n) where $t = \frac{n-1}{2}$ $(2^*, 4^*)$, (7^*)	$n > 3$ $n \not\equiv 0 \mod 3$ Theorem 9 in [13]		$\frac{n-1}{2}$	[14], [13]
$G_s(x) = x^{2^s-1}$ where $s = \frac{n+3}{2}$ $(2^*, 4^*)$, (7^*)	$n \not\equiv 0 \mod 3$		$\frac{n+3}{2}$	[14]
f in Corollary 3.5-(ii) in [130], (3^*), (6^*)		$2^{n-1} - 2^{\frac{3n-3}{4}} - 2^{\frac{k-1}{2}} - 2^{k-1}$ (where $k = \frac{n}{5}$)		[130]

Table 7: -continued from previous page

Competitive Diff. δ-Uniform Permutation f	n: **ODD DEGREE** Constraints:	Lower Bound on Nonlinearity	$d^0(f)$	Ref.
With $\Delta(f) = 6$:				
$f_3 = (x+t_2)^{-1} + (x^{2^s} + x + t_1)^{2^n-1}(x^{-1} + (x+t_2)^{-1})$ $\Delta(f_3) \leq 6$, (4^*), (7^*)	$3rd$ construction $t_2 \in \mathbb{F}_{2^s}^*$, $t_1 \in \mathbb{F}_{2^n}^*$, $Tr_n^s(t_1) = 0$	$2^{n-1} - 2^{\frac{n}{2}} - 2^s$	$n-1$	[138]
With $\Delta(f) = 8$:				
$G_t(x) = x^{2^t-1}$ where $t = \frac{n-1}{2}$ $(2^*, 4^*)$, (7^*)	$n > 3$ $n \equiv 0 \mod (3)$ Theorem 9 in [13]		$\frac{n-1}{2}$	[14], [13]
$x^{\frac{1}{2^i+1}} + \gamma Tr(x) = F_{i,\gamma}(x)$ (EA-E to the inverse of the Gold). Its inverse $F_{i,\gamma}^{-1}$ can be attacked instead, since $d^0(F_{i,\gamma}^{-1})$ is too low	n (**any odd**) $\gcd(i,n) = 3$, $2 \leq i \leq m$ $\gamma \in \mathbb{F}_8$, $Tr(\gamma) = 0$, (4^*) $d^0(F_{i,\gamma}^{-1}) = 3$	$2^{n-1} - (2)2^{\frac{n-1}{2}}$	$\frac{n-1}{2}$	[38]

Functions Unbroken to $\mathbf{AAtt}_{\mathbb{F}_{2^n}}(4)$*-Algebraic Attack*: while also being up to par with fulfilling the priority cryptographic properties, subject to automatically choosing efficient values for their parameters, i, m, s, $|U|$, and g, at least the following functions can be named:

Function families $f_{k,g}(x)$ and $K_{i,g}(x)$ in Theorem 4.2;
$\pi(x)^{-1} = x^{-1} + \sum_{i=0}^{m}(x+\alpha_i)^{2^n-1}(\alpha_i^{-1} + \alpha_{i+1}^{-1})$, refer to [92];
$\tilde{I}^{(n-i)}_{\tilde{x}_0,0}(x) = x^{2^n-2} + Tr_n^1(a_1x^{2^n-2})\ldots Tr_n^1(a_{n-i}x^{2^n-2})$ for $\forall n-1 \geq i \geq 2$;
$F(x)$ for $0 < |U| < \frac{2^{n-1}-2^{\frac{n}{2}}-6}{3}$, refer to [127];
$F(x) = \begin{cases} (x+1)^{-1}+1, & x \in U \\ x^{-1}, & x \in \mathbb{F}_{2^n} \setminus U \end{cases}$ for U(union of the sets S_a), refer to [134];
$G_{k',g}(x) = x^{2^{k'}+1} + (x^{2^{k'}} + x+1)Tr_n^1(a_1x)\ldots Tr_n^1(a_gx)$; and
$F(x) = f(x) + (f(x) + x^{2^{n/2}+2^{n/4}+1})(x + x^{2^s})^{2^n-1}$, ref. Corollary 4.2 in [28].

Challenges to Overcome: the scientific community knows this topic is extremely competitive. Now we, the scientists in these domains, have the experience we need, gained from differentially 4-uniform functions, to take a new look at differentially δ-uniform functions, starting with $\delta = 6$ and 8.

Open Problem 14: Bound the second nonlinearity $nl_2(f)$ for these functions.

Supplement I-A

Tables 10 and 11 include the Walsh Spectrum and other cryptographic properties of the monomial family x^{2^d+1} (to read about *Classical Walsh Spectrum* see [67]). These permit us to see the variety of cases that can occur. Denote: n = field degree, Δ = its differential δ uniformity. Unusual values that are not mentioned in the papers, and that these values represent a weakness of the Gold family, as for example having $\Delta = 16$, Walsh Spectrum of the forms $\{\mathbf{2^{n-3}}, 2^{\frac{n}{2}}, 0\}$, $\{\mathbf{2^{n-4}}, 2^{\frac{n}{2}}, 0\}$, $\{\mathbf{2^{\frac{n+3}{2}}}, 0\}$ and $\{\mathbf{2^{\frac{n+5}{2}}}, 0\}$ are highlighted in bold letter. A complete information about it, up to the finite field of degree 15, is a matter of interest for authors in this research area.

Supplement I-B

Table 12 list the primitive polynomials $p(x)$ we used to construct some finite fields of degree n for this research work.

n	$f(x)$	$\Delta(f)$	1-to-1	$nl(f)$	$d^0(f)$
6	Gold x^5	4	yes	24	2
$= 2(3)$	$x^5 + (x^4 + x + 1)tr(x)tr(ax)$	6	yes	22	5
3 *odd*	$tr(a^2x)tr(a^4x)tr(a^5x)$				
	$x^5 + (x^4 + x + 1)tr(x)tr(ax)$	6	yes	20	5
	$tr(a^2x)tr(a^4x)$				
	Kasami x^{13}	4	yes	24	3
	$x^{13} + (x^{12} + x^9 + x^8 + x^5 + x^4 + x +$	6	yes	22	5
	$1)tr(x)tr(ax)tr(a^2x)tr(a^4x)tr(a^5x)$				
	$x^{13} + (x^{12} + x^9 + x^8 + x^5 + x^4 + x +$	**8**	yes	20	5
	$1)tr(x)tr(ax)tr(a^2x)tr(a^4x)$	$4 \leq \mathbf{8} \leq 2(4)$			
7	Kasami x^{13}	2	yes	56	3
	$x^{13} + (x^{12} + x^9 + x^8 + x^5 + x^4 + x + 1)$	4	yes	54	6
	$tr(ax)tr(a^2x)tr(a^3x)tr(a^4x)tr(a^5x)tr(a^6x)$				
	$x^{13} + (x^{12} + x^9 + x^8 + x^5 + x^4 + x + 1)$	4	yes	52	6
	$tr(ax)tr(a^2x)tr(a^3x)tr(a^4x)tr(a^5x)$				
	Gold x^9	2	yes	56	2
	$x^9 + (x^8 + x + 1)tr(ax)tr(a^2x)$	4	yes	54	6
	$tr(a^3x)tr(a^4x)tr(a^5x)tr(a^6x)$				
	$x^9 + (x^8 + x + 1)tr(ax)$	4	yes	52	6
	$tr(a^2x)tr(a^3x)tr(a^4x)tr(a^5x)$				
	Gold x^5	2	yes	56	2
	$x^5 + (x^4 + x + 1)tr(ax)tr(a^2x)$	4	yes	54	6
	$tr(a^3x)tr(a^4x)tr(a^5x)tr(a^6x)$				
	$x^5 + (x^4 + x + 1)tr(ax)$	4	yes	52	6
	$tr(a^2x)tr(a^3x)tr(a^4x)tr(a^5x)$				
	Gold x^3	2	yes	56	2
	$x^3 + (x^2 + x + 1)tr(ax)tr(a^2x)$	4	yes	54	6
	$tr(a^3x)tr(a^4x)tr(a^5x)tr(a^6x)$				
	$x^3 + (x^2 + x + 1)tr(ax)$	4	yes	52	6
	$tr(a^2x)tr(a^3x)tr(a^4x)tr(a^5x)$				

Table 8: *Gold* and *Kasami based permutations* with *optimal algebraic degree* (oad). Where $a = \alpha$ is a primitive element such that the trace of each power of a appearing in f is zero.

n	$f(x)$	$\Delta(f)$	1-to-1	$nl(f)$	$d^0(f)$
10	Gold x^{17}	4	yes	480	2
$= 2(5)$	$x^{17} + (x^{16} + x + 1)tr(x)tr(ax)tr(a^2x)tr(a^3x)$	6	yes	478	9
5 *odd*	$tr(a^4x)tr((a^5 + a^7)x)tr(a^6x)tr(a^8x)tr(a^9x)$				
	$x^{17} + (x^{16} + x + 1)tr(x)tr(ax)tr(a^2x)tr(a^3x)$	6	yes	476	9
	$tr(a^4x)tr(a^6x)tr(a^8x)tr(a^9x)$				
	Gold x^5	4	yes	480	2
	$x^5 + (x^4 + x + 1)tr(x)tr(ax)tr(a^2x)tr(a^3x)$	6	yes	478	9
	$tr(a^4x)tr((a^5 + a^7)x)tr(a^6x)tr(a^8x)tr(a^9x)$				
	$x^5 + (x^4 + x + 1)tr(x)tr(ax)tr(a^2x)tr(a^3x)$	**8**	yes	476	9
	$tr(a^4x)tr(a^6x)tr(a^8x)tr(a^9x)$				

Table 9: *Gold* and *Kasami based permutations* with *optimal algebraic degree* (oad). Where $a = \alpha$ is a primitive element such that the trace of each power of a appearing in f is zero.

n even	x^{2^d+1}	Δ	1-to-1	*Walsh coeff.* $\lvert W_{x^{2^d+1}}(a,b)\rvert$	$\lvert\mathcal{W}_{x^{2^d+1}}\rvert$ *form*
$n = 2$	x^3	2	no	[(0, 3), (4, 1)]; [(2, 4)]	$\{\mathbf{2^n}, 2^{\frac{n}{2}}, 0\}$
$n = 4$	x^5	4	no	[(0, 15), (16, 1)]; [(4, 16)]	$\{\mathbf{2^n}, 2^{\frac{n}{2}}, 0\}$
	x^3	2	no	[(0, 12), (8, 4)]; [(4, 16)]	$\{2^{\frac{n+2}{2}}, 2^{\frac{n}{2}}, 0\}$
$n = 6$	x^9	8	no	[(0, 63), (64, 1)]; [(8, 64)]	$\{\mathbf{2^n}, 2^{\frac{n}{2}}, 0\}$
$= 2(3)$	x^5	4	yes	[(0, 48), (16, 16)]	$\{2^{\frac{n+2}{2}}, 0\}$
3 *odd*	x^3	2	no	[(0, 48),(16, 16)]; [(8, 64)]	$\{2^{\frac{n+2}{2}}, 2^{\frac{n}{2}}, 0\}$
$n = 8$	x^{17}	16	no	[(0, 255), (256, 1)]; [(16, 256)]	$\{\mathbf{2^n}, 2^{\frac{n}{2}}, 0\}$
	x^9, x^3	2	all	[(0, 192), (32, 64)]; [(16, 256)]	$\{2^{\frac{n+2}{2}}, 2^{\frac{n}{2}}, 0\}$
	x^5	4	over	[(0, 240), (64, 16)]; [(16, 256)]	$\{\mathbf{2^{n-2}}, 2^{\frac{n}{2}}, 0\}$
$n = 10$	x^{33}	32	no	[(0, 1023), (1024, 1)], [(32, 1024)]	$\{\mathbf{2^n}, 2^{\frac{n}{2}}, 0\}$
$= 2(5)$	x^{17}, x^5	4	yes	[(0, 768), (64, 256)]	$\{2^{\frac{n+2}{2}}, 0\}$
5 *odd*	x^9, x^3	2	no	[(0, 768), (64, 256)]; [(32, 1024)]	$\{2^{\frac{n+2}{2}}, 2^{\frac{n}{2}}, 0\}$
$n = 12$	x^{65}	64	no	[(0, 4095), (4096, 1)], [(64, 4096)]	$\{\mathbf{2^n}, 2^{\frac{n}{2}}, 0\}$
	x^{33}, x^3	2	no	[(0, 3072), (128, 1024)], [(64, 4096)]	$\{2^{\frac{n+2}{2}}, 2^{\frac{n}{2}}, 0\}$
	x^{17}	**16**	yes	[(0, 3840), (256, 256)]	$\{\mathbf{2^{n-4}}, 0\}$
	x^9	**8**	no	[(0, 4032), (512, 64)], [(64, 4096)]	$\{\mathbf{2^{n-3}}, 2^{\frac{n}{2}}, 0\}$
	x^5	4	no	[(0, 3840), (256, 256)], [(64, 4096)]	$\{\mathbf{2^{n-4}}, 2^{\frac{n}{2}}, 0\}$
$n = 14$	x^{129}	–	no	[(0, 16383), (16384, 1)], [(128, 16384)]	$\{\mathbf{2^n}, 2^{\frac{n}{2}}, 0\}$
$= 2(7)$	x^{65}, x^{17}, x^5	4	yes	[(0, 12288), (256, 4096)]	$\{2^{\frac{n+2}{2}}, 0\}$
7 *odd*	x^{33}, x^9, x^3	2	no	[(0, 12288), (256, 4096)], [(128, 16384)]	$\{2^{\frac{n+2}{2}}, 2^{\frac{n}{2}}, 0\}$

Table 10: A variety of extended Walsh Spectrum $\lvert\mathcal{W}_{x^{2^d+1}}\rvert$

n odd	x^{2^d+1}	Δ	1-to-1	*Walsh coeff.* $\lvert W_{x^{2^d+1}}(a,b)\rvert$	$\lvert\mathcal{W}_{x^{2^d+1}}\rvert$ *form*
$n=3$	x^3	2	yes	[(0, 4), (4, 4)]	$\{2^{\frac{n+1}{2}}, 0\}$
$n=5$	x^5, x^3	2	yes	[(0, 16), (8, 16)]	$\{2^{\frac{n+1}{2}}, 0\}$
$n=7$	x^9, x^5, x^3	2	yes	[(0, 64), (16, 64)]	$\{2^{\frac{n+1}{2}}, 0\}$
$n=9$	x^{17}, x^5, x^3	2	yes	[(0, 256), (32, 256)]	$\{2^{\frac{n+1}{2}}, 0\}$
	x^9	**8**	yes	[(0, 448), (64, 64)]	$\{\mathbf{2}^{\frac{\mathbf{n+3}}{\mathbf{2}}}, 0\}$
$n=11$	x^{33}, x^{17}, x^9, x^5, x^3	2	yes	[(0, 1024), (64, 1024)]	$\{2^{\frac{n+1}{2}}, 0\}$
$n=13$	x^{65}, x^{33}, x^{17}, x^9, x^5	2	yes	[(0, 4096), (128, 4096)]	$\{2^{\frac{n+1}{2}}, 0\}$
	x^3	–	yes		
$n=15$	x^{129}, x^{17}, x^5, x^3	–	yes	[(0, 16384), (256, 16384)]	$\{2^{\frac{n+1}{2}}, 0\}$
	x^{65}, x^9	–	all	[(0, 28672), (512, 4096)]	$\{\mathbf{2}^{\frac{\mathbf{n+3}}{\mathbf{2}}}, 0\}$
	x^{33}	–	over	[(0, 31744), (1024, 1024)]	$\{\mathbf{2}^{\frac{\mathbf{n+5}}{\mathbf{2}}}, 0\}$

Table 11: A variety of extended Walsh Spectrum $\lvert\mathcal{W}_{x^{2^d+1}}\rvert$

$p(x)$
x^2+x+1, x^3+x+1,x^4+x+1,x^5+x^2+1,x^6+x+1,$x^6+x^4+x^3+x+1$,x^7+x+1, $x^8+x^4+x^3+x^2+1$, x^9+x^4+1, $x^{10}+x^3+1$,$x^{10}+x^6+x^5+x^3+x^2+x+1$, $x^{11}+x^2+1$,$x^{12}+x^6+x^4+x+1$, $x^{12}+x^7+x^6+x^5+x^3+x+1$, $x^{13}+x^4+x^3+x+1$,$x^{14}+x^5+x^3+x+1$,$x^{14}+x^7+x^5+x^3+1$, $x^{15}+x+1$,$x^{15}+x^5+x^4+x^2+1$

Table 12: Toolkit: primitive polynomials $p(x)$ used for some $\mathbb{F}_{2^n}$.

9 Analysis of Differential Equations under the Galois Field ($\mathbb{F}_{p^n}$) Perspective and Its Impact on Communications Security

In this section we produce the analysis with exclusive dedication to differential operators between Galois fields, in different aspects (in the past there have been somewhat related constructions that took a completely different route in which the functions involved had co-domains different from $\mathbb{F}_{p^n}$), containing surprising analogies with the continuous case, which also—contrary to what happens in $\mathbb{F}_{p^n}$—is endowed with a total order [73] compatible with the algebraic structure of the field. Under the following Kerckhoffs's principle reformulated by Claude Shannon, *"the enemy knows the system being used"* [120], the security of the system relies on the strength of the S-Box being used to hide the key. Therefore the real need to know its weaknesses is a higher spirit that accompanies this article. The adversary could be masterminding some contemporary attack like the following ones, Differential Fault Attack (DFA) on Stream Ciphers, Filter Permutator FLIP and Improved Filter Permutator FiLIP, in which the equation $s_i - \dot{s}_i = f(\rho_i(\kappa \oplus \mathbf{u}_\gamma)) - f(\rho_i(\kappa)) = \partial_{\rho_i(\mathbf{u}_\gamma)} f(\rho_i(\kappa))$ is formulated, where $\partial_{\rho_i(\mathbf{u}_\gamma)} f(\rho_i(\kappa)) = f(\rho_i(\kappa \oplus \mathbf{u}_\gamma)) - f(\rho_i(\kappa))$.

Definition 9.1 $\partial^{(r)}_{H^r}(R[X]) := \{f \in R[X]; \exists \phi \in R[X]$ *such that* $f = \partial^{(r)}_{H^r}(\phi)\}$, *where* $r \geq 1$, $H \in R^*$. *This definition can be extended to other rings besides* $R[X] = \mathbb{F}_{p^n}[X]$.

It can be verified that the derivative operator decreases the algebraic degree of a function by one or more. Classes of our functions, composed with the trace function, are Boolean functions whose derivatives are also strong, which solve the problem proposed by Méaux and Roy [98].

There is no loss of generality if we consider that a function $f : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ is in general in its $\mod (X^{p^n} - X)$ format, that is, we will always consider $f = F \mod (X^{p^n} - X)$ for some $F \in \mathbb{F}_{p^n}[X]$. Our next result is the criterion for the algebraic degree of the derivative of a function in general, keeping in mind that the derivation over the field $\mathbb{F}_{p^n}$ is linear.

Theorem 9.2 ***(Fashionable Theorem)****(General characterization of the algebraic degree of the derivative of a function on* $\mathbb{F}_{p^n}$*). Let* $f = F \mod (X^{p^n} - X)$ *be a function such that* $F \in \mathbb{F}_{p^n}[X]$, $2 \leq d^0(f) \leq (p-1)(n-1)$, p *a prime, and* $H \in \mathbb{F}_{p^n} \setminus \{0\}$ *(an arbitrary direction). Then: the part of maximum*

algebraic degree in f is not an expression of the form

$$\sum_{\mathfrak{S}_\Omega X^\Omega \in \mathbb{O}_{\prec p;f;n\succ}} \mathfrak{S}_\Omega \sum_{\substack{\psi_\Theta^{(\Omega)} \text{ is a term in} \\ \partial_{H^{p-1}}^{(p-1)}(X^\Omega) \text{ such} \\ \text{that } d^0(\psi_\Theta^{(\Omega)})=d^0(f)}} \psi_\Theta^{(\Omega)}, \text{ for some non-empty set}$$

$$\mathbb{O}_{\prec p;f;n\succ} \subseteq \{\mathfrak{S}_\Omega X^\Omega \in \mathbb{F}_{p^n}[X] \setminus \{0\}; d^0(\mathfrak{S}_\Omega X^\Omega) - p + 1 = d^0(f)\},$$

is a necessary and sufficient condition for $d^0\big(\partial_H(f)\big) + 1 = d^0(f)$.

Proof. Let $\mathfrak{L}X^{\mathfrak{U}}$ be a term of *m.a.d.*(maximun algebraic degree) in f, then there exists the monomial $\mathfrak{S}X^\Omega$ with algebraic degree $p + d^0(f) - 1$ such that $\Omega = \Omega(p) = \sum_{i=1}^{p-1}\big(p^{k_i^\dagger} + \frac{\mathfrak{U}}{p-1}\big)$, with $k_i^\dagger \geq 0$ for all i. Let's think of $\Omega(p)$ as a polynomial evaluated at p; let's express it in such a way that all its terms have positive coefficients. The part of *m.a.d.* in $\partial_{H^{p-1}}^{(p-1)}(\mathfrak{S}X^\Omega)$ is given below, which we obtain by repeated application of the derivative with respect to H:

$$\sum_{\substack{\{\zeta_{k_1},\ldots,\zeta_{k_{p-1}}\}\subseteq\mathbb{Z}[p], \\ \text{where:} \\ \zeta_{k_1} \text{ is a term in } \Omega(p), \\ \cdots, \\ \zeta_{k_{p-1}} \text{ is a term in} \\ \Omega(p)-\sum_{\ell=1}^{p-2}\frac{\zeta_{k_\ell}}{\mathrm{cff}(\zeta_{k_\ell})}}} \left(\mathfrak{S}H^{\sum_{\ell=1}^{p-1}\frac{\zeta_{k_\ell}}{\mathrm{cff}(\zeta_{k_\ell})}} \prod_{\gamma=1}^{p-1}\mathrm{cff}(\zeta_{k_\gamma})\right) X^{\Omega(p)-\sum_{\ell=1}^{p-1}\frac{\zeta_{k_\ell}}{\mathrm{cff}(\zeta_{k_\ell})}} \quad \text{(Eq. I)}$$

(moreover, this formula works for an arbitrary monomial $\mathfrak{S}X^\Omega$) where $\mathrm{cff}(\zeta_{k_\gamma})$ denotes the coefficient, in this case corresponding to ζ_{k_γ} in $\Omega(p) - \sum_{\ell\leq\gamma-1}\frac{\bar{\epsilon}_{\gamma,1}\zeta_{k_\ell}}{\mathrm{cff}(\zeta_{k_\ell})} = \begin{cases} \Omega(p), & \text{if } \gamma = 1 \\ \Omega(p) - \sum_{\ell\leq\gamma-1}\frac{\zeta_{k_\ell}}{\mathrm{cff}(\zeta_{k_\ell})}, & \text{if } \gamma \geq 2 \end{cases}$. Where $\bar{\epsilon}_{\gamma,1} = 1 - \epsilon_{\gamma,1}$, and $\epsilon_{i,j}$ is the Kronecker's delta. Additionally, $\mathfrak{L}X^{\mathfrak{U}}$ appears in this summation when the $\frac{\zeta_{k_i}}{\mathrm{cff}(\zeta_{k_i})}$ are equal to $\frac{\zeta_{k_i}}{\mathrm{cff}(\zeta_{k_i})} = p^{k_i^\dagger}$, and furthermore, $\mathfrak{S}$ is uniquely determined.

Let $\mathfrak{L}'X^{\mathfrak{U}'}$ be any other term in f such that terms in its derivative $\partial_H(\mathfrak{L}'X^{\mathfrak{U}'})$ contribute to eliminating *m.a.d.* terms in $\partial_H(\mathfrak{L}X^{\mathfrak{U}})$. Then necessarily $\big|\mathfrak{U}'_{\mathrm{set}}\big| - 1 \not> \big|\mathfrak{U}_{\mathrm{set}} \cap \mathfrak{U}'_{\mathrm{set}}\big|$, where $U_{\mathrm{set}} := \bigcup_{\substack{\Xi \text{ is a term of } U \text{ (seen} \\ \text{as a polynomial in } p)}} \{1, \cdots, \mathrm{cff}(\Xi)\} \times \{\frac{\Xi}{\mathrm{cff}(\Xi)}\}$, also the induced mapping $U \xrightarrow{\Gamma_{\mathrm{set}}} U_{\mathrm{set}}$ is invertible. Furthermore, when applying the operator ∂_H to $\mathfrak{L}X^{\mathfrak{U}}$ and $\mathfrak{L}'X^{\mathfrak{U}'}$, these have at most one *m.a.d.* term in common (which we shall call Observation 1).

In general, a term of *m.a.d.* in $\partial_H(\mathfrak{L}X^{\mathfrak{U}})$, $\overset{\star}{\mathfrak{F}}_{k_p}(X)$, is of the form:

$$\begin{aligned}\overset{\star}{\mathfrak{F}}_{k_p}(X) =&\mathfrak{L}H^{\frac{\overset{\star}{\varphi}_{k_p}}{\mathrm{cff}(\overset{\star}{\varphi}_{k_p})}}\mathrm{cff}(\overset{\star}{\varphi}_{k_p})X^{\mathfrak{U}(p)-\frac{\overset{\star}{\varphi}_{k_p}}{\mathrm{cff}(\overset{\star}{\varphi}_{k_p})}}\\ =&\mathfrak{S}H^{\frac{\overset{\star}{\varphi}_{k_p}}{\mathrm{cff}(\overset{\star}{\varphi}_{k_p})}+\sum\limits_{\ell=1}^{p-1}p^{k_\gamma^\dagger}}\mathrm{cff}(\overset{\star}{\varphi}_{k_p})\Bigg(\prod_{\gamma=1}^{p-1}\mathrm{cff}(p^{k_\gamma^\dagger})\text{ in }\Omega(p)-\\ &\sum_{\ell\leq\gamma-1}\bar{\epsilon}_{\gamma,1}p^{k_\gamma^\dagger}\Bigg)X^{\Omega(p)-\frac{\overset{\star}{\varphi}_{k_p}}{\mathrm{cff}(\overset{\star}{\varphi}_{k_p})}-\sum\limits_{\ell=1}^{p-1}p^{k_\gamma^\dagger}},\end{aligned}$$

where $\overset{\star}{\varphi}_{k_p}$ is a term in the polynomial $\mathfrak{U}=\mathfrak{U}(p)$. Additionally, we use $\mathrm{cff}(p^{k_\gamma^\dagger})$ to denote the coefficient of the term whose literal part is $p^{k_\gamma^\dagger}$, i.e., the property $\mathrm{cff}(p^{k_\gamma^\dagger})=\mathrm{cff}(\mathrm{cff}(p^{k_\gamma^\dagger})p^{k_\gamma^\dagger})$ is fulfilled. Next, we will identify those $\mathfrak{L}'X^{\mathfrak{U}'}$ such that a term in its derivative contributes to eliminating the function $\overset{\star}{\mathfrak{F}}_{k_p}(X)$. We will begin with the case where the powers $p^{k_i^\dagger}$ are mutually distinct. We introduce $p^{k_p^\dagger}$ such that $\mathrm{cff}(\overset{\star}{\varphi}_{k_p})p^{k_p^\dagger}=\overset{\star}{\varphi}_{k_p}$, which need not be different from the $p^{k_i^\dagger}$s introduced previously. For each $p^{k_i^\dagger}$, let us differentiate in the direction H the term

$$\mathfrak{L}_{[\overset{\star}{\varphi}_{k_p},i]}X^{\mathfrak{U}_{[\overset{\star}{\varphi}_{k_p},i]}}\overset{\text{def}}{=}$$

$$\begin{cases}\mathfrak{S}H^{\sum\limits_{\gamma=1,\gamma\neq i}^{p}p^{k_\gamma^\dagger}}\Bigg(\prod\limits_{\gamma=1,\gamma\neq i}^{p}1+\left(\mathrm{cff}(p^{k_\gamma^\dagger})\text{ in }\Gamma_{\mathrm{set}}^{-1}\left(\mathfrak{U}_{\mathrm{set}}\cap\mathfrak{U}'_{\mathrm{set}}\right)\right)\Bigg)X^{\Gamma_{\mathrm{set}}^{-1}\left(\mathfrak{U}_{\mathrm{set}}\cap\mathfrak{U}'_{\mathrm{set}}\right)+p^{k_i^\dagger}},\\ \qquad\qquad\text{if }(\mathbb{P}_0^{\rtimes})_{\mathrm{set}}\bigcap\{(1,p^{k_p^\dagger})\}=\varnothing.\\ \mathfrak{S}\mathcal{M}_{1/2}H^{\sum\limits_{\gamma=1,\gamma\neq i}^{p}p^{k_\gamma^\dagger}}\Bigg(\prod\limits_{\gamma=1,\gamma\neq i}^{p}1+\left(\mathrm{cff}(p^{k_\gamma^\dagger})\text{ in }\Gamma_{\mathrm{set}}^{-1}\left(\mathfrak{U}_{\mathrm{set}}\cap\mathfrak{U}'_{\mathrm{set}}\right)\right)\Bigg)X^{\Gamma_{\mathrm{set}}^{-1}\left(\mathfrak{U}_{\mathrm{set}}\cap\mathfrak{U}'_{\mathrm{set}}\right)+p^{k_i^\dagger}},\\ \qquad\text{where }\mathcal{M}_{1/2}=\frac{2+\mathrm{cff}(p^{k_p^\dagger})\text{ in }\Gamma_{\mathrm{set}}^{-1}\left(\mathfrak{U}_{\mathrm{set}}\cap\mathfrak{U}'_{\mathrm{set}}\right)}{1+\mathrm{cff}(p^{k_p^\dagger})\text{ in }\Gamma_{\mathrm{set}}^{-1}\left(\mathfrak{U}_{\mathrm{set}}\cap\mathfrak{U}'_{\mathrm{set}}\right)},\text{ if }(\mathbb{P}_0^{\rtimes})_{\mathrm{set}}\bigcap\{(1,p^{k_p^\dagger})\}\neq\varnothing.\end{cases}$$

Then, from its derivative, we select the *m.a.d.* term given below:

$$\mathfrak{L}_{[\overset{\star}{\varphi}_{k_p},i]}H^{p^{k_i^\dagger}}\left(\mathrm{cff}(p^{k_i^\dagger})\text{ in }\Gamma_{\mathrm{set}}^{-1}\left(\mathfrak{U}_{\mathrm{set}}\cap\mathfrak{U}'_{\mathrm{set}}\right)+p^{k_i^\dagger}\right)X^{\Gamma_{\mathrm{set}}^{-1}\left(\mathfrak{U}_{\mathrm{set}}\cap\mathfrak{U}'_{\mathrm{set}}\right)}=$$

$$\begin{cases}\mathfrak{S}H^{\sum\limits_{\gamma=1}^{p}p^{k_\gamma^\dagger}}\Bigg(\prod\limits_{\gamma=1}^{p}1+\left(\mathrm{cff}(p^{k_\gamma^\dagger})\text{ in }\Gamma_{\mathrm{set}}^{-1}\left(\mathfrak{U}_{\mathrm{set}}\cap\mathfrak{U}'_{\mathrm{set}}\right)\right)\Bigg)X^{\Gamma_{\mathrm{set}}^{-1}\left(\mathfrak{U}_{\mathrm{set}}\cap\mathfrak{U}'_{\mathrm{set}}\right)},\\ \qquad\qquad\text{if }(\mathbb{P}_0^{\rtimes})_{\mathrm{set}}\bigcap\{(1,p^{k_p^\dagger})\}=\varnothing.\\ \mathfrak{S}\mathcal{M}_{1/2}H^{\sum\limits_{\gamma=1}^{p}p^{k_\gamma^\dagger}}\Bigg(\prod\limits_{\gamma=1}^{p}1+\left(\mathrm{cff}(p^{k_\gamma^\dagger})\text{ in }\Gamma_{\mathrm{set}}^{-1}\left(\mathfrak{U}_{\mathrm{set}}\cap\mathfrak{U}'_{\mathrm{set}}\right)\right)\Bigg)X^{\Gamma_{\mathrm{set}}^{-1}\left(\mathfrak{U}_{\mathrm{set}}\cap\mathfrak{U}'_{\mathrm{set}}\right)},\\ \qquad\text{where }\mathcal{M}_{1/2}=\frac{2+\mathrm{cff}(p^{k_p^\dagger})\text{ in }\Gamma_{\mathrm{set}}^{-1}\left(\mathfrak{U}_{\mathrm{set}}\cap\mathfrak{U}'_{\mathrm{set}}\right)}{1+\mathrm{cff}(p^{k_p^\dagger})\text{ in }\Gamma_{\mathrm{set}}^{-1}\left(\mathfrak{U}_{\mathrm{set}}\cap\mathfrak{U}'_{\mathrm{set}}\right)},\text{ if }(\mathbb{P}_0^{\rtimes})_{\mathrm{set}}\bigcap\{(1,p^{k_p^\dagger})\}\neq\varnothing.\end{cases}$$

$$=\phi(X,\overset{\star}{\varphi}_{k_p},p^{k_1^\dagger},\cdots,p^{k_p^\dagger}),\text{ for }\Gamma_{\mathrm{set}}^{-1}\left(\mathfrak{U}_{\mathrm{set}}\cap\mathfrak{U}'_{\mathrm{set}}\right)=\mathfrak{U}(p)-p^{k_p^\dagger},\text{ where }\mathbb{P}_0^{\rtimes}:=$$

$\sum_{i=1}^{p-1} p^{k_i^\dagger}$. Summing the functions $\phi(X, \overset{\star}{\varphi}_{k_p}, p^{k_1^\dagger}, \cdots, p^{k_p^\dagger})$ whose sum is denoted by $S^{(X, \overset{\star}{\varphi}_{k_p}, p^{k_1^\dagger}, \cdots, p^{k_p^\dagger})}$ we have that p divides $S^{(X, \overset{\star}{\varphi}_{k_p}, p^{k_1^\dagger}, \cdots, p^{k_p^\dagger})}$, that is, equals zero, and the $\mathfrak{L}_{[\overset{\star}{\varphi}_{k_p}, i]} X^{\mathfrak{U}_{[\overset{\star}{\varphi}_{k_p}, i]}}$ are our $\mathfrak{L}' X^{\mathfrak{U}'}$, and even our $\mathfrak{L} X^{\mathfrak{U}}$. It is worth noting that no matter which $p^{k_i^\dagger}$ we use, we obtain the same $\phi(X, \overset{\star}{\varphi}_{k_p}, p^{k_1^\dagger}, \cdots, p^{k_p^\dagger})$. We observe that the $\mathfrak{L}_{[\overset{\star}{\varphi}_{k_p}, i]} X^{\mathfrak{U}_{[\overset{\star}{\varphi}_{k_p}, i]}}$ are terms of the same $\partial_{H^{p-1}}^{(p-1)}(\mathfrak{S} X^{\Omega})$.

Similarly, new $\mathfrak{L}_{[\overset{\star}{\varphi}_{k_p}, i]} X^{\mathfrak{U}_{[\overset{\star}{\varphi}_{k_p}, i]}}$ are defined for when the powers $p^{k_i^\dagger}$s (now a term in $\mathbb{P}_0^{\rtimes}$ can have its coefficient different from 1) are not necessarily different from each other, knowing this, we will then deal with the rest of the terms with *m.a.d.* generated by the derivative of the $\mathfrak{L}_{[\overset{\star}{\varphi}_{k_p}, i]} X^{\mathfrak{U}_{[\overset{\star}{\varphi}_{k_p}, i]}}$. For all $\ell \in [1, p]$ we have that $\{\mathcal{X}^{(\infty)}_{\ell, \overset{\star}{\varphi}_{k_{p,1}}} \text{ in } \partial_H\big(\mathfrak{L}_{[\overset{\star}{\varphi}_{k_{p,1}}, \ell]} X^{\mathfrak{U}_{[\overset{\star}{\varphi}_{k_{p,1}}, \ell]}}\big)\} \setminus \bigcup_{s=1,\, p^{k_s^\dagger} \neq p^{k_\ell^\dagger}}^{p} \{\mathcal{X}^{(\infty)}_{s, \overset{\star}{\varphi}_{k_{p,1}}} \text{ in } \partial_H\big(\mathfrak{L}_{[\overset{\star}{\varphi}_{k_{p,1}}, s]} X^{\mathfrak{U}_{[\overset{\star}{\varphi}_{k_{p,1}}, s]}}\big)\} = \{\mathcal{X}_{\ell, \overset{\star}{\varphi}_{k_{p,1}}} \text{ in } \partial_H\big(\mathfrak{L}_{[\overset{\star}{\varphi}_{k_{p,1}}, \ell]} X^{\mathfrak{U}_{[\overset{\star}{\varphi}_{k_{p,1}}, \ell]}}\big)\}$, because the $\mathfrak{L}_{[\overset{\star}{\varphi}_{k_{p,1}}, s]} X^{\mathfrak{U}_{[\overset{\star}{\varphi}_{k_{p,1}}, s]}}$ are different from $\mathfrak{L}_{[\overset{\star}{\varphi}_{k_{p,1}}, \ell]} X^{\mathfrak{U}_{[\overset{\star}{\varphi}_{k_{p,1}}, \ell]}}$, followed by the application of Observation 1 (an alternative reason is based on restricting X adequately, e.g. to range $\mathbb{F}_{p^n} \setminus \{0, 1\}$, then we apply that $\mathrm{cff}(p^{k_\ell^\dagger})$ in $\log_X\big(\frac{\mathcal{X}_{\ell, \overset{\star}{\varphi}_{k_{p,1}}}}{\mathrm{cff}\big(\mathcal{X}_{\ell, \overset{\star}{\varphi}_{k_{p,1}}}\big)}\big) > \mathrm{cff}(p^{k_\ell^\dagger})$ in $\log_X\big(\frac{\mathcal{X}_{s, \overset{\star}{\varphi}_{k_{p,1}}}}{\mathrm{cff}\big(\mathcal{X}_{s, \overset{\star}{\varphi}_{k_{p,1}}}\big)}\big) \geq 0$, where the discrete logarithm verifies that $\log_X X^a$ is a, with $0 \leq a \leq p^n - 1$), where $\mathcal{X}^{(\infty)}_{i, \overset{\star}{\varphi}_{k_{p,1}}}$ means a term of *m.a.d.* in a given function, and $\mathcal{X}_{i, \overset{\star}{\varphi}_{k_{p,1}}}$ means a term of *m.a.d.* in a given function, fulfilling $\mathcal{X}_{i, \overset{\star}{\varphi}_{k_{p,1}}} \neq \phi(X, \overset{\star}{\varphi}_{k_{p,1}}, p^{k_1^\dagger}, \cdots, p^{k_{p,1}^\dagger})$, where ϕ has already been exploited before. Otherwise, if $p^{k_\ell^\dagger} = p^{k_s^\dagger}$, where $1 \leq s \leq p$, $s \neq \ell$, then $\{\mathcal{X}^{(\infty)}_{\ell, \overset{\star}{\varphi}_{k_{p,1}}} \text{ in } \partial_H(\mathfrak{L}_{[\ell, \overset{\star}{\varphi}_{k_{p,1}}]} X^{\mathfrak{U}_{[\ell, \overset{\star}{\varphi}_{k_{p,1}}]}})\} = \{\mathcal{X}^{(\infty)}_{s, \overset{\star}{\varphi}_{k_{p,1}}} \text{ in } \partial_H(\mathfrak{L}_{[s, \overset{\star}{\varphi}_{k_{p,1}}]} X^{\mathfrak{U}_{[s, \overset{\star}{\varphi}_{k_{p,1}}]}})\}$, and considering the chain of equal sets in this way, adding produces the terms $\mu \mathcal{X}^{(\infty)}_{\ell, \overset{\star}{\varphi}_{k_{p,1}}}$, for some $\mu = \mathrm{cff}\big(p^{k_\ell^\dagger}\big)$ in $\mathbb{P}_0^{\rtimes} + \frac{\overset{\star}{\varphi}_{k_{p,1}}}{\mathrm{cff}(\overset{\star}{\varphi}_{k_{p,1}})}$, and $2 \leq \mu < p$, such that the value of $d^0(\mathfrak{S} X^{\Omega})$ is maintained. In either of these two scenarios, none of the *m.a.d.* terms in the derivative of one of the functions $\mathfrak{L}_{[s, \overset{\star}{\varphi}_{k_{p,1}}]} X^{\mathfrak{U}_{[s, \overset{\star}{\varphi}_{k_{p,1}}]}}$ can contribute to eliminating the $\mathcal{X}_{\ell, \overset{\star}{\varphi}_{k_{p,1}}}$ of another, or it is not sufficient to eliminate it. It

is essential to ensure that the $\mathcal{X}_{\ell,\overset{\star}{\varphi}_{k_{p,1}}}$ in $\partial_H\big(\mathfrak{L}_{[\ell,\overset{\star}{\varphi}_{k_{p,1}}]}X^{\mathfrak{U}_{[\ell,\overset{\star}{\varphi}_{k_{p,1}}]}}\big)$ terms are eliminated. Terms of type $\mathcal{X}^{(\infty)}_{\ell,\overset{\star}{\varphi}_{k_{p,1}}}$ (include the $\mathcal{X}_{\ell,\overset{\star}{\varphi}_{k_{p,1}}}$) always exist, being the target to eliminate even if we had to obtain 0ϕ repeatedly. So the purpose is to find all the eliminator terms. An essential aspect is that, since the algebraic degree of $X^{\mathbb{P}_0^{\rtimes}}$ is $p-1$, we always have the following representation: $\mathbb{P}_0^{\rtimes}=\sum_{\ell=1}^{r}\mu_\ell p^{a_\ell^\star}$ and $\mathfrak{U}=\sum_{\ell=1}^{r}\overline{\mu}_\ell p^{a_\ell^\star}+\sum_{\ell'=r+1}^{n}z_{\ell'}p^{a_{\ell'}^\star}$ are such that $\mu_\ell+\overline{\mu}_\ell\leq p-1$ $\forall\ell\leq r$, in order that the value of $d^0(\mathfrak{S}X^\Omega)$ is maintained, $\sum_{\ell=1}^{r}\mu_\ell=p-1$, for some $r\leq p-1$, and $\{a_i^\star\}_{i=1}^n$ can be seen as the ring with cyclic additive group $\mathbb{Z}/n\mathbb{Z}$. Thus, $d^0(\mathfrak{L}X^{\mathfrak{U}})=\sum_{\ell=1}^{r}\overline{\mu}_\ell+\sum_{\ell'=r+1}^{n}z_{\ell'}\leq\sum_{\ell=1}^{r}p-1-\mu_\ell+\sum_{\ell'=r+1}^{n}z_{\ell'}$ $\leq(r-1)(p-1)+\sum_{\ell'=r+1}^{n}p-1$, i.e. $d^0(f)\leq(p-1)(n-1)$. When $p=2$, $(\mathbb{P}_0^{\rtimes})_{\text{set}}\cap\mathfrak{U}_{\text{set}}=\varnothing$, in order to maintain the value of $d^0(\mathfrak{S}X^\Omega)$.

An eliminator term belonging to $\partial^{(p-1)}_{H^{p-1}}(\mathfrak{S}X^\Omega)$ necessarily has the form (the following type of term is required) $\mathfrak{L}_{[\overset{\star}{\varphi}_{k_{p,1}},i_1,\overset{\star}{\varphi}_{k_{p,2}},i_2,\cdots,\overset{\star}{\varphi}_{k_{p,\vartheta}},i_\vartheta]}X^{\mathfrak{U}_{[\overset{\star}{\varphi}_{k_{p,1}},i_1,\overset{\star}{\varphi}_{k_{p,2}},i_2,\cdots,\overset{\star}{\varphi}_{k_{p,\vartheta}},i_\vartheta]}}$, for all $\vartheta\geq 2$, so that it eliminates the *m.a.d.* term $\mathfrak{L}_{[\overset{\star}{\varphi}_{k_{p,1}},i_1,\overset{\star}{\varphi}_{k_{p,2}},i_2,\cdots,\overset{\star}{\varphi}_{k_{p,\vartheta}}]}$ $X^{\mathfrak{U}_{[\overset{\star}{\varphi}_{k_{p,1}},i_1,\overset{\star}{\varphi}_{k_{p,2}},i_2,\cdots,\overset{\star}{\varphi}_{k_{p,\vartheta}}]}}$ (these are the $\mathcal{X}_{\ell,\overset{\star}{\varphi}_{k_{p,1}}}$ in $\partial_H\big(\mathfrak{L}_{[\overset{\star}{\varphi}_{k_{p,1}},\ell]}X^{\mathfrak{U}_{[\overset{\star}{\varphi}_{k_{p,1}},\ell]}}\big)$, for $\vartheta=2$) that appears in the derivative of its predecessor $\mathfrak{L}_{[\overset{\star}{\varphi}_{k_{p,1}},i_1,\cdots,\overset{\star}{\varphi}_{k_{p,\vartheta-1}},i_{\vartheta-1}]}X^{\mathfrak{U}_{[\overset{\star}{\varphi}_{k_{p,1}},i_1,\cdots,\overset{\star}{\varphi}_{k_{p,\vartheta-1}},i_{\vartheta-1}]}}$, where $\mathfrak{U}_{[\overset{\star}{\varphi}_{k_{p,1}},i_1,\overset{\star}{\varphi}_{k_{p,2}},i_2,\cdots,\overset{\star}{\varphi}_{k_{p,\vartheta}}]}=$ $\mathfrak{U}_{[\overset{\star}{\varphi}_{k_{p,1}},i_1,\cdots,\overset{\star}{\varphi}_{k_{p,\vartheta-1}},i_{\vartheta-1}]}-\frac{\overset{\star}{\varphi}_{k_{p,\vartheta}}}{\text{cff}(\overset{\star}{\varphi}_{k_{p,\vartheta}})}$, $\mathfrak{U}_{[\overset{\star}{\varphi}_{k_{p,1}},i_1,\overset{\star}{\varphi}_{k_{p,2}},i_2,\cdots,\overset{\star}{\varphi}_{k_{p,\vartheta}},i_\vartheta]}=\mathfrak{U}_{[\overset{\star}{\varphi}_{k_{p,1}},i_1,\overset{\star}{\varphi}_{k_{p,2}},i_2,\cdots,\overset{\star}{\varphi}_{k_{p,\vartheta}}]}+$ $\frac{i_\vartheta}{\text{cff}(i_\vartheta)}$, $\overset{\star}{\varphi}_{k_{p,1}}$ is a term in $\mathfrak{U}(p)$, and $\overset{\star}{\varphi}_{k_{p,\vartheta}}$ is a term in $\mathfrak{U}(p)-\sum_{r=1}^{\vartheta-1}\frac{\overset{\star}{\varphi}_{k_{p,r}}}{\text{cff}(\overset{\star}{\varphi}_{k_{p,r}})}$. Specifically, the following is satisfied: for all $\overset{\star}{\varphi}_{k_{p,\vartheta}}$, we have that,

$$\sum_{\substack{i_\vartheta\text{ is a term in }\frac{\overset{\star}{\varphi}_{k_{p,\vartheta}}}{\text{cff}(\overset{\star}{\varphi}_{k_{p,\vartheta}})}+\\ \mathbb{P}_0^{\rtimes}+\sum_{r=1}^{\vartheta-1}\frac{\overset{\star}{\varphi}_{k_{p,r}}}{\text{cff}(\overset{\star}{\varphi}_{k_{p,r}})}-\frac{i_r}{\text{cff}(i_r)}}}\mathfrak{L}_{[\overset{\star}{\varphi}_{k_{p,1}},i_1,\cdots,\overset{\star}{\varphi}_{k_{p,\vartheta}},i_\vartheta]}H^{\frac{i_\vartheta}{\text{cff}(i_\vartheta)}}\big(\text{cff}(i_\vartheta)\text{ in }\mathfrak{U}_{[\overset{\star}{\varphi}_{k_{p,1}},i_1,\cdots,\overset{\star}{\varphi}_{k_{p,\vartheta}},i_\vartheta]}\big)$$

$X^{\mathfrak{U}_{[\overset{\star}{\varphi}_{k_{p,1}},i_1,\cdots,\overset{\star}{\varphi}_{k_{p,\vartheta}}]}}=$

$$\sum_{\substack{i_\vartheta \text{ is a term in } \frac{\overset{\star}{\varphi}_{k_{p,\vartheta}}}{\mathrm{cff}(\overset{\star}{\varphi}_{k_{p,\vartheta}})}+ \\ \mathbb{P}_0^{\rtimes}+\sum_{r=1}^{\vartheta-1}\frac{\overset{\star}{\varphi}_{k_{p,r}}}{\mathrm{cff}(\overset{\star}{\varphi}_{k_{p,r}})}-\frac{i_r}{\mathrm{cff}(i_r)}}} \mathfrak{S}H^{\mathbb{P}_\vartheta^{\rtimes}+\frac{i_\vartheta}{\mathrm{cff}(i_\vartheta)}}\left(\prod_{\gamma=1}^{p-1}\mathrm{cff}(j_{\vartheta_\gamma})\text{ in }\Omega(p)-\sum_{\ell\leq\gamma-1}\frac{\bar{\epsilon}_{\gamma,1}j_{\vartheta_\ell}}{\mathrm{cff}(j_{\vartheta_\ell})}\right)\big(\mathrm{cff}(i_\vartheta)\text{ in }$$

$$\mathfrak{U}_{[\overset{\star}{\varphi}_{k_{p,1}},i_1,\cdots,\overset{\star}{\varphi}_{k_{p,\vartheta}},i_\vartheta]}\big)\ X^{\mathfrak{U}_{[\overset{\star}{\varphi}_{k_{p,1}},i_1,\cdots,\overset{\star}{\varphi}_{k_{p,\vartheta}}]}}=$$

$$\sum_{\substack{i_\vartheta \text{ is a term in } \frac{\overset{\star}{\varphi}_{k_{p,\vartheta}}}{\mathrm{cff}(\overset{\star}{\varphi}_{k_{p,\vartheta}})}+ \\ \mathbb{P}_0^{\rtimes}+\sum_{r=1}^{\vartheta-1}\frac{\overset{\star}{\varphi}_{k_{p,r}}}{\mathrm{cff}(\overset{\star}{\varphi}_{k_{p,r}})}-\frac{i_r}{\mathrm{cff}(i_r)}}} \mathfrak{S}H^{\overline{\mathbb{P}_\vartheta^{\rtimes}}}\left(\prod_{\gamma=1}^{p}\mathrm{cff}(\pi_{\vartheta_\gamma})\text{ in }\Omega(p)-\right.$$

$$\left.\sum_{\ell\leq\gamma-1}\frac{\bar{\epsilon}_{\gamma,1}\pi_{\vartheta_\ell}}{\mathrm{cff}(\pi_{\vartheta_\ell})}\right)\ X^{\mathfrak{U}_{[\overset{\star}{\varphi}_{k_{p,1}},i_1,\cdots,\overset{\star}{\varphi}_{k_{p,\vartheta}}]}}=0$$, this sum cancels out because the addend within the summation is constant, , which is being added p times, thus producing the elimination, where we take the term i_1 in $\frac{\overset{\star}{\varphi}_{k_{p,1}}}{\mathrm{cff}(\overset{\star}{\varphi}_{k_{p,1}})}+\mathbb{P}_0^{\rtimes}$, and i_ℓ in $\frac{\overset{\star}{\varphi}_{k_{p,\ell}}}{\mathrm{cff}(\overset{\star}{\varphi}_{k_{p,\ell}})}+\mathbb{P}_0^{\rtimes}+\sum_{r=1}^{\ell-1}\frac{\overset{\star}{\varphi}_{k_{p,r}}}{\mathrm{cff}(\overset{\star}{\varphi}_{k_{p,r}})}-\frac{i_r}{\mathrm{cff}(i_r)}$, for all $\ell\leq\vartheta$, $\vartheta\leq d^0(f)$, in addition, $\mathbb{P}_\vartheta^{\rtimes}=\mathbb{P}_0^{\rtimes}+\sum_{r=1}^{\vartheta}\frac{\overset{\star}{\varphi}_{k_{p,r}}}{\mathrm{cff}(\overset{\star}{\varphi}_{k_{p,r}})}-\frac{i_r}{\mathrm{cff}(i_r)}$. Let j_{ϑ_1} be a term in $\mathbb{P}_\vartheta^{\rtimes}$, and the next j_{ϑ_γ} be a term in $\mathbb{P}_\vartheta^{\rtimes}-\sum_{r=1}^{\gamma-1}\frac{j_{\vartheta_r}}{\mathrm{cff}(j_{\vartheta_r})}$ for $\gamma\geq 2$. Additionally, $j_{\vartheta_p}:=\frac{i_\vartheta}{\mathrm{cff}(i_\vartheta)}$, which is equivalent to considering an enumeration (the π_{ϑ_γ}s) in $\overline{\mathbb{P}_\vartheta^{\rtimes}}=\mathbb{P}_\vartheta^{\rtimes}+\frac{i_\vartheta}{\mathrm{cff}(i_\vartheta)}$, in the same way, it is respected that π_{ϑ_γ} is a term in $\overline{\mathbb{P}_\vartheta^{\rtimes}}-\sum_{r=1}^{\gamma-1}\frac{\pi_{\vartheta_r}}{\mathrm{cff}(\pi_{\vartheta_r})}$, based on the associativity and commutativity of the composition between derivative operators. In particular, the $j_{\vartheta_{\gamma'}}$s are π_{ϑ_γ}s. These terms that we shall call eliminators take place successively, and for this purpose we define $W_{\prec X,\overset{\star}{\varphi}_{k_p},p^{k_1^\dagger},\cdots,p^{k_p^\dagger}\succ}$ as the set that collects this type of terms.

On the other hand, a term of the form $\mathfrak{L}''X^{\mathfrak{U}_{[\overset{\star}{\varphi}_{k_{p,1}},i_1,\overset{\star}{\varphi}_{k_{p,2}}]}}$ in $\partial_H\big(\mathfrak{L}_{[\overset{\star}{\varphi}_{k_{p,1}},i_1]}$ $X^{\mathfrak{U}_{[\overset{\star}{\varphi}_{k_{p,1}},i_1]}}\big)$ can in general be eliminated via terms of algebraic degree $d^0(f)$ of the form $\widetilde{\mathfrak{L}}_{[\overset{\star}{\varphi}_{k_{p,1}},i_1,\overset{\star}{\varphi}_{k_{p,2}},\widetilde{i_2}]}X^{\mathfrak{U}_{[\overset{\star}{\varphi}_{k_{p,1}},i_1,\overset{\star}{\varphi}_{k_{p,2}},\widetilde{i_2}]}}$ where $\widetilde{i_2}\in\frac{\overset{\star}{\varphi}_{k_{p,2}}}{\mathrm{cff}(\overset{\star}{\varphi}_{k_{p,2}})}+\widetilde{\mathbb{P}_0^{\rtimes}}+\frac{\overset{\star}{\varphi}_{k_{p,1}}}{\mathrm{cff}(\overset{\star}{\varphi}_{k_{p,1}})}-\frac{i_1}{\mathrm{cff}(i_1)}$, such that $\widetilde{\mathbb{P}_0^{\rtimes}}$ is not necessarily equal to $\mathbb{P}_0^{\rtimes}$. That is, $\widetilde{\mathfrak{L}}_{[\overset{\star}{\varphi}_{k_{p,1}},i_1,\overset{\star}{\varphi}_{k_{p,2}},\widetilde{i_2}]}$ $X^{\mathfrak{U}_{[\overset{\star}{\varphi}_{k_{p,1}},i_1,\overset{\star}{\varphi}_{k_{p,2}},\widetilde{i_2}]}}\in\partial_{H^{p-1}}^{(p-1)}(\widetilde{\mathfrak{S}}X^{\widetilde{\Omega}})$ for some $\widetilde{\Omega}\neq\Omega$. We define the following

set of functions: $\widetilde{W}_{\prec X,\overset{\star}{\varphi}_{k_p},p^{k_1^\dagger},\cdots,p^{k_p^\dagger}\succ} \overset{\text{def}}{=} \big\{\widetilde{\mathfrak{L}}_{[\overset{\star}{\varphi}_{k_{p,1}},i_1,\overset{\star}{\varphi}_{k_{p,2}},\widetilde{i_2}]}X^{\mathfrak{U}_{[\overset{\star}{\varphi}_{k_{p,1}},i_1,\overset{\star}{\varphi}_{k_{p,2}},\widetilde{i_2}]}},\ldots,$ $\widetilde{\mathfrak{L}}_{[\overset{\star}{\varphi}_{k_{p,1}},i_1,\overset{\star}{\varphi}_{k_{p,2}},\widetilde{i_2},\cdots,\overset{\star}{\varphi}_{k_{p,\vartheta}},\widetilde{i_\vartheta}]}X^{\mathfrak{U}_{[\overset{\star}{\varphi}_{k_{p,1}},i_1,\overset{\star}{\varphi}_{k_{p,2}},\widetilde{i_2},\cdots,\overset{\star}{\varphi}_{k_{p,\vartheta}},\widetilde{i_\vartheta}]}};d^0(f)\geq\vartheta\geq 2\big\}\bigcup\big\{\mathfrak{L}_{[\overset{\star}{\varphi}_{k_{p,1}},i_1]}$ $X^{\mathfrak{U}_{[\overset{\star}{\varphi}_{k_{p,1}},i_1]}}\big\}$, such that when $\frac{\widetilde{i_2}}{\mathrm{cff}(\widetilde{i_2})}$ is $\frac{\overset{\star}{\varphi}_{k_{p,2}}}{\mathrm{cff}(\overset{\star}{\varphi}_{k_{p,2}})}$, the term $\widetilde{\mathfrak{L}}_{[\overset{\star}{\varphi}_{k_{p,1}},i_1,\overset{\star}{\varphi}_{k_{p,2}},\widetilde{i_2}]}$ $X^{\mathfrak{U}_{[\overset{\star}{\varphi}_{k_{p,1}},i_1,\overset{\star}{\varphi}_{k_{p,2}},\widetilde{i_2}]}}$ coincides with $\mathfrak{L}_{[\overset{\star}{\varphi}_{k_{p,1}},i_1]}X^{\mathfrak{U}_{[\overset{\star}{\varphi}_{k_{p,1}},i_1]}}$. Then $\widetilde{\mathfrak{L}}_{[\overset{\star}{\varphi}_{k_{p,1}},i_1,\overset{\star}{\varphi}_{k_{p,2}},\overset{\star}{\varphi}_{k_{p,2}}]}=$ $\mathfrak{L}_{[\overset{\star}{\varphi}_{k_{p,1}},i_1]}$, i.e.

$$\widetilde{\mathfrak{S}}H^{\widetilde{\mathbb{P}_2^{\bowtie}}}\prod_{\theta_{(\vartheta=2)_\gamma}\text{ in }\widetilde{\mathbb{P}_2^{\bowtie}}}\big(\mathrm{cff}(\theta_{(\vartheta=2)_\gamma})\text{ in }\widetilde{\Omega(p)}-\sum_{\ell\leq\gamma-1}\tfrac{\bar{\epsilon}_{\gamma,1}\theta_{(\vartheta=2)_\ell}}{\mathrm{cff}(\theta_{(\vartheta=2)_\ell})}\big)=$$

$\mathfrak{S}H^{\mathbb{P}_1^{\bowtie}}\prod_{j_{(\vartheta=1)_\gamma}\text{ in }\mathbb{P}_1^{\bowtie}}\big(\mathrm{cff}(j_{(\vartheta=1)_\gamma})\text{ in }\Omega(p)-\sum_{\ell\leq\gamma-1}\frac{\bar{\epsilon}_{\gamma,1}j_{(\vartheta=1)_\ell}}{\mathrm{cff}(j_{(\vartheta=1)_\ell})}\big)$, where $\widetilde{i_1}$ is i_1, while the $\theta_{(\vartheta=2)_\gamma}$s are terms in $\widetilde{\mathbb{P}_2^{\bowtie}}:=\widetilde{\mathbb{P}_0^{\bowtie}}+\sum_{r=1}^{2}\frac{\overset{\star}{\varphi}_{k_{p,r}}}{\mathrm{cff}(\overset{\star}{\varphi}_{k_{p,r}})}-\frac{\widetilde{i_r}}{\mathrm{cff}(\widetilde{i_r})}$ respecting that $\theta_{(\vartheta=2)_\gamma}$ is a term in $\widetilde{\mathbb{P}_2^{\bowtie}}-\sum_{r=1}^{\gamma-1}\frac{\theta_{(\vartheta=2)_r}}{\mathrm{cff}(\theta_{(\vartheta=2)_r})}$ for $\gamma\geq 2$, in particular this equation works for $H=1$, providing us with the respective identity between their coefficients. Then considering H arbitrary again, we have, $H^{\widetilde{\mathbb{P}_2^{\bowtie}}}=H^{\mathbb{P}_1^{\bowtie}}$ for all $H\in\mathbb{F}_{p^n}\setminus\{0\}$, and including 0, then $\widetilde{\mathbb{P}_0^{\bowtie}}+\sum_{r=1}^{2}\frac{\overset{\star}{\varphi}_{k_{p,r}}}{\mathrm{cff}(\overset{\star}{\varphi}_{k_{p,r}})}-\frac{\widetilde{i_r}}{\mathrm{cff}(\widetilde{i_r})}=$ $\mathbb{P}_1^{\bowtie}$. Since $\frac{\widetilde{i_2}}{\mathrm{cff}(\widetilde{i_2})}=\frac{\overset{\star}{\varphi}_{k_{p,2}}}{\mathrm{cff}(\overset{\star}{\varphi}_{k_{p,2}})}$, we have $\widetilde{\mathbb{P}_0^{\bowtie}}=\mathbb{P}_0^{\bowtie}$. Then $\widetilde{W}_{\prec X,\overset{\star}{\varphi}_{k_p},p^{k_1^\dagger},\cdots,p^{k_p^\dagger}\succ}=$ $W_{\prec X,\overset{\star}{\varphi}_{k_p},p^{k_1^\dagger},\cdots,p^{k_p^\dagger}\succ}$.

It is possible that the polynomial mapping $\partial^{(p-1)}_{H^{p-1}}(\mathfrak{S}X^\Omega)$ contains some *m.a.d.* term outside $W_{\prec X,\overset{\star}{\varphi}_{k_p},p^{k_1^\dagger},\cdots,p^{k_p^\dagger}\succ}$. Next we guarantee that there are no surplus *m.a.d.* terms in $\partial^{(p-1)}_{H^{p-1}}(\mathfrak{S}X^\Omega)$, that is to say that those eliminators $\mathfrak{L}_{[\overset{\star}{\varphi}_{k_{p,1}},i_1,\overset{\star}{\varphi}_{k_{p,2}},i_2,\cdots,\overset{\star}{\varphi}_{k_{p,\vartheta}},i_\vartheta]}X^{\mathfrak{U}_{[\overset{\star}{\varphi}_{k_{p,1}},i_1,\overset{\star}{\varphi}_{k_{p,2}},i_2,\cdots,\overset{\star}{\varphi}_{k_{p,\vartheta}},i_\vartheta]}}$ are all. We provide an enumeration to the terms of the form $\frac{\Xi}{\mathrm{cff}(\Xi)}$ (i.e., monic) such that $\big(1,\frac{\Xi}{\mathrm{cff}(\Xi)}\big)$ does not belong to $(\mathbb{P}_0^{\bowtie})_{\mathrm{set}}$, which are subtracted (due to the derivation processes involved) from $\mathfrak{U}$, as follows: $t_{\hat{\omega}_1},\cdots,t_{\hat{\omega}_\beta}$. And we enumerate the terms of the form $\frac{\Xi}{\mathrm{cff}(\Xi)}$ (i.e., $\frac{\Xi_1}{\mathrm{cff}(\Xi_1)},\ldots,\frac{\Xi_\beta}{\mathrm{cff}(\Xi_\beta)}$), such that $\big(\sum_{1\leq\ell\leq\beta}\frac{\Xi_\ell}{\mathrm{cff}(\Xi_\ell)}\big)_{\mathrm{set}}\subseteq$ $\big(\mathbb{P}_0^{\bowtie}-\sum_{\sigma\in\{\text{terms of form }\frac{\Xi}{\mathrm{cff}(\Xi)}\text{ subtracted from }\mathbb{P}_0^{\bowtie}\}}\sigma\big)_{\mathrm{set}}$, as follows: $p_{\omega_1},\ldots,p_{\omega_\beta}$, where $0<\beta\leq p-1$. Let $g(X)$ be any term of *m.a.d.* in $\partial^{(p-1)}_{H^{p-1}}(\mathfrak{S}X^\Omega)\setminus\{X^{\mathfrak{U}},\mathfrak{L}X^{\mathfrak{U}}\}$ (except these), we write it in the form $g(X)=\mathfrak{L}_gX^{\mathfrak{U}+p_{\omega_1}-t_{\hat{\omega}_1}+\ldots+p_{\omega_\beta}-t_{\hat{\omega}_\beta}}$. The term $g(X)$ can be rewritten as follows,

$$g(X)=\mathfrak{L}_gX^{\mathfrak{U}+p_{\omega_1}-t_{\hat{\omega}_1}+\ldots+p_{\omega_\beta}-t_{\hat{\omega}_\beta}+t_{\hat{\omega}_{\beta+1}}-t_{\hat{\omega}_{\beta+1}}+\ldots+t_{\hat{\omega}_m}-t_{\hat{\omega}_m}}$$

$=\mathfrak{L}_gX^{\mathfrak{U}+\sum_{c=1}^{m}\xi_{\omega_c}-t_{\hat{\omega}_c}}$, where $m=d^0(f)$, $\mathfrak{L}_g\in\mathbb{F}_{p^n}^*$, $\xi_{\omega_c}=p_{\omega_c}$ for all $c\leq\beta$,

$\xi_{\omega_c} = t_{\widehat{\omega}_c}$ for all $m \geq c \geq \beta+1$, $(1, p_{\omega_1}) \in \left(\mathbb{P}_0^{\rtimes}\right)_{\text{set}}$, $(1, p_{\omega_c}) \in \left(\mathbb{P}_0^{\rtimes} - \sum_{\ell=1}^{c-1} p_{\omega_\ell}\right)_{\text{set}}$ for all $\beta \geq c \neq 1$. That is, $(1, p_{\omega_c}) \in \left(t_{\widehat{\omega}_c} + \mathbb{P}_0^{\rtimes} + \sum_{\ell=1}^{c-1} t_{\widehat{\omega}_\ell} - p_{\omega_\ell}\right)_{\text{set}}$ for all $\beta \geq c \neq 1$. In all cases $(1, \xi_{\omega_c}) \in \left(t_{\widehat{\omega}_c} + \mathbb{P}_0^{\rtimes} + \sum_{\ell=1}^{c-1} t_{\widehat{\omega}_\ell} - p_{\omega_\ell}\right)_{\text{set}}$ for all $m \geq c \neq 1$, and $(1, \xi_{\omega_1}) \in \left(t_{\widehat{\omega}_1} + \mathbb{P}_0^{\rtimes}\right)_{\text{set}}$, satisfying $\varnothing \neq \left(\mathbb{P}_0^{\rtimes}\right)_{\text{set}} \setminus \left(\sum_{1=\ell\leq\beta-1} p_{\omega_\ell}\right)_{\text{set}}$. Additionally, $\mathfrak{L}_g X^{\mathfrak{U}+\sum_{c=1}^{m} \xi_{\omega_c} - t_{\widehat{\omega}_c}} = \mathfrak{L}_g X^{\Omega - (\mathbb{P}_0^{\rtimes} + \sum_{c=1}^{m} t_{\widehat{\omega}_c} - \xi_{\omega_c})} = \mathfrak{L}_g X^{\mathfrak{U}_{[\overset{\star}{\varphi}_{k_{p,1}}, i_1, \overset{\star}{\varphi}_{k_{p,2}}, i_2, \cdots, \overset{\star}{\varphi}_{k_{p,\beta}}, i_\beta]}} = \mathfrak{L}_g X^{\mathfrak{U}_{[\overset{\star}{\varphi}_{k_{p,1}}, i_1, \overset{\star}{\varphi}_{k_{p,2}}, i_2, \cdots, \overset{\star}{\varphi}_{k_{p,m}}, i_m]}}$, where this choice of parameters satisfies $t_{\widehat{\omega}_c} = \frac{\overset{\star}{\varphi}_{k_{p,c}}}{\text{cff}(\overset{\star}{\varphi}_{k_{p,c}})}$ and $\xi_{\omega_c} = \frac{i_c}{\text{cff}(i_c)}$, for all $c \leq m$. Since $g(X)$ is the term in $\partial_{H^{p-1}}^{(p-1)}(\mathfrak{S}X^{\Omega})$ of degree $\mathfrak{U}_{[\overset{\star}{\varphi}_{k_{p,1}}, i_1, \overset{\star}{\varphi}_{k_{p,2}}, i_2, \cdots, \overset{\star}{\varphi}_{k_{p,\beta}}, i_\beta]}$, then $\mathfrak{L}_g = \mathfrak{L}_{[\overset{\star}{\varphi}_{k_{p,1}}, i_1, \overset{\star}{\varphi}_{k_{p,2}}, i_2, \cdots, \overset{\star}{\varphi}_{k_{p,\beta}}, i_\beta]}$. Remember that $W_{\prec X, \overset{\star}{\varphi}_{k_p}, p^{k_1^\dagger}, \cdots, p^{k_p^\dagger} \succ}$ contains $\mathfrak{L}X^{\mathfrak{U}}$. Then, the set of terms of *m.a.d.* in $\partial_{H^{p-1}}^{(p-1)}(\mathfrak{S}X^{\Omega}) \subseteq W_{\prec X, \overset{\star}{\varphi}_{k_p}, p^{k_1^\dagger}, \cdots, p^{k_p^\dagger} \succ}$. Since $W_{\prec X, \overset{\star}{\varphi}_{k_p}, p^{k_1^\dagger}, \cdots, p^{k_p^\dagger} \succ}$ is contained in the set of terms of *m.a.d.* in $\partial_{H^{p-1}}^{(p-1)}(\mathfrak{S}X^{\Omega})$, we obtain the equality: the set of terms of *m.a.d.* in $\partial_{H^{p-1}}^{(p-1)}(\mathfrak{S}X^{\Omega}) = W_{\prec X, \overset{\star}{\varphi}_{k_p}, p^{k_1^\dagger}, \cdots, p^{k_p^\dagger} \succ}$, and this happens for each $\mathfrak{L}X^{\mathfrak{U}}$. Let us denote by $\mathfrak{S}_{\Omega}\psi_{\Theta}^{(\Omega)}$ the elements of $W_{\prec X, \overset{\star}{\varphi}_{k_p}, p^{k_1^\dagger}, \cdots, p^{k_p^\dagger} \succ}$. Then these $\mathfrak{S}_{\Omega}\psi_{\Theta}^{(\Omega)}$ are all the *m.a.d.* terms required in f so that the *m.a.d.* terms in the $\partial_H(\mathfrak{S}_{\Omega}\psi_{\Theta}^{(\Omega)})$s eliminate the corresponding ones present in $\partial_H(\mathfrak{L}X^{\mathfrak{U}})$ and each other, which is equivalent to: the *m.a.d.* terms in f (such that $d^0\big(\partial_H(f)\big) \neq d^0(f)-1$) add up to $\sum_{\mathfrak{S}_{\Omega}X^{\Omega} \in \mathbb{O}_{\prec p;f;n\succ}} \mathfrak{S}_{\Omega} \sum_{\psi_{\Theta}^{(\Omega)} \text{ is a term in } \partial_{H^{p-1}}^{(p-1)}(X^{\Omega})} \psi_{\Theta}^{(\Omega)}$, with $d^0(\psi_{\Theta}^{(\Omega)}) = d^0(f)$, for some non-empty set $\mathbb{O}_{\prec p;f;n\succ} \subseteq \{\mathfrak{S}_{\Omega}X^{\Omega} \in \mathbb{F}_{p^n}[X] \setminus \{0\}; d^0(\mathfrak{S}_{\Omega}X^{\Omega}) - p + 1 = d^0(f)\}$. Thus, taking the negation of this equivalence gives us an equivalence again, which is effectively the statement of this theorem. □

Corollary 9.3 *Let $f = F \mod (X^{2^n} - X)$ be a function such that $F \in \mathbb{F}_{2^n}[X]$, $2 \leq d^0(f) \leq n-1$, and $H \in \mathbb{F}_{2^n} \setminus \{0\}$ (an arbitrary direction). Then: the part of maximum algebraic degree in f is not an expression of the form*

$$\sum_{\mathfrak{S}_{\Omega}X^{\Omega} \in \mathbb{O}_{\prec 2;f;n\succ}} \mathfrak{S}_{\Omega} \sum_{\substack{\psi_{\Theta}^{(\Omega)} \text{ is a term in} \\ \partial_H(X^{\Omega}) \text{ such} \\ \text{that } d^0(\psi_{\Theta}^{(\Omega)}) = d^0(f)}} \psi_{\Theta}^{(\Omega)}, \text{ for some non-empty set}$$

$$\mathbb{O}_{\prec 2;f;n\succ} \subseteq \{\mathfrak{S}_{\Omega}X^{\Omega} \in \mathbb{F}_{2^n}[X] \setminus \{0\}; d^0(\mathfrak{S}_{\Omega}X^{\Omega}) - 1 = d^0(f)\},$$

is a necessary and sufficient condition for $d^0\big(\partial_H(f)\big) + 1 = d^0(f)$.

If $d^0(f) > n-1$, then $d^0\big(\partial_H(f)\big) + 1 = d^0(f)$.

Proof. Applying Theorem 9.2, it only remains to investigate the case $d^0(f) > n-1$. An f of this size (in this form) has a single term of *m.a.d.* whose derivative consists of terms of algebraic degree $n-1$. Moreover, $\partial_H(J) \neq$ the function 0, for any non-constant monomial J. Thus, $d^0\big(\partial_H(f)\big) = d^0(f) - 1$. □

$\partial^{(p-1),\, d^0=r}_{H^{p-1}}\mathbb{F}_{p^n}[X] \stackrel{\text{def}}{=} \mathbb{F}^{d^0=r}_{p^n}[X] \bigcap \partial^{(p-1)}_{H^{p-1}}(\mathbb{F}_{p^n}[X] \mod (X^{p^n}-X))$ will be called the *Near 0 Kelvin-Galois-Carranza's Class of Degree r*—its element with maximum number of terms will be called *Near 0 Kelvin-Carranza Function of Degree r*—while $\mathbb{F}^{d^0\leq r}_{p^n}[X] \bigcap \partial^{(p-1)}_{H^{p-1}}(\mathbb{F}_{p^n}[X] \mod (X^{p^n}-X))$ is called the *Kelvin-Galois-Carranza Space of Degree r*, also *KGC Space of Degree r*. This results in the astonishing existence of non-constant functions of a vast diversity of degrees whose derivative (under Definition I of derivative, in accordance with Subsection 1.1) is zero, just as is the case with constant functions. In this sense we have discovered abstract functions of the constant function. Note that if we consider a function, ψ, from the Space of Piecewise Constant Functions on $\mathbb{F}_{p^n}$, which we denote as $S(\mathbb{F}_{p^n})$, then in general $\partial_h(\psi)$ is distinct from the function 0[1] [2] [3]. We give an urgent concern in the following **Open Problem 15:** *explore the existence of any other space or structure of functions whose derivative is zero. Also achieve the unification of these structures.* The supplementary case of Theorem 9.2 can be demonstrated in a similar way to that established by this theorem in mention; furthermore, **Little Open Problem 16.** Prove Theorem 9.2 regarding the case $d^0(f) > (p-1)(n-1)$, but by a substantially different channel than the applicable analogous procedure corresponding to the one established in Theorem 9.2.

Those interested in Markov ciphers can read Xuejia Lai, James L. Massey, and Sean Murphy [87, 88], where in Propositions 1-2 in [87] the algebraic degree of the derivative of a multivariate function is observed for the inequality case. We answer (by an if and only if) the question of when equality is possible. On the other hand, to see research on functions $f : GF(p)^n \to GF(p)$ where their codomain is the prime field $GF(p)$, and various results in another direction, you can see the article by Ana Sălăgean, Richard Winter, Matei Mandache-Sălăgean, and Raphael C.-W. Phan. [126].

A salient inference from the algebraic degree analysis is that in the $\mathbb{F}_{p^n}$-algebra, $\mathbb{F}_{p^n}[X]$, there will not exist a function analogous to the transcendental function $y = \exp(x)$, which is very beneficial in Euclidean spaces. We shall

[1] Let us for a moment consider the case of the normed Lebesgue space $L^1(\mathbb{R})$ (constituted by equivalence classes of equal functions, except for a set of zero measure). The important Step Function Space $S(\mathbb{R})$ (its functions, $\phi : \mathbb{R} \to \mathbb{R}$, are finite sums of the form $\phi = \sum_{k=1}^{m} A_k X_{I_k}$, i.e. bounded functions, where each characteristic function X_{I_k} equals 1 on the bounded interval I_k and 0 outside it) is a dense vector subspace of $L^1(\mathbb{R})$.

[2] Now, any of the side derivatives (with respect to the usual definition in $\mathbb{R}$, endowed with its usual metric) of ϕ at every point equals zero, too.

[3] In the context of $\mathbb{F}_{p^n}$, the derivative is also taken with respect to some direction $h(\neq 0)$.

see that $\mathbb{F}_{2^n}[X]$ was made to make Laplace's equation hold. One can directly confirm that the derivative operator $\partial_h(.)$ is linear; there are other equations that are obtained fairly straightforwardly. Just as the historical Gaussian quantity $i \in \mathbb{C} \setminus \mathbb{R}$ appearing in the *Schrödinger equation*, for our formulation of the $\mathbb{F}_{p^n}$-*Schrödinger equation*, one could pick out the analogous element to i in some difference of fields, $\mathbb{F}_{2^{\ell_1}} \setminus \mathbb{F}_{2^{\ell_2}}$. Our approach is to work properly with functions whose codomain is the Galois field, which by the way does not accept a total ordering, as a substantial difference compared to the f assumed in the theory of *weighted graphs* or *networks* where the codomain of f is $\mathbb{R}_0^+$, which is also associated with a *Lebesgue* measure (see Royden [116]), the treatment being different and of course such theory does not cover finite fields. The fundamental theorem of calculus as well as a product rule are fulfilled, all exclusively-"vip" for functions between Galois fields. Here we will give a brief approach with notable steps in this direction of the theory. The reader interested in differential equations on *networks* can find information in that direction in the articles by Richard James Duffin, Edward B. Curtis, James A. Morrow, Enrique Bendito, Ángeles Carmona, Andrés M. Encinas, Soon-Yeong Chung, Yun-Sung Chung, and Jong-Ho Kim [64, 49, 9, 48]. In the $\mathbb{F}_{p^n}$-context, the new solutions will no longer be the conventional wavefunctions (defined on a *separable Hilbert space*) in quantum mechanics, they will suffer a truly dramatic transformation in their nature, pointing out the fact that some of their properties collapse. According to the Corollary 9.4, we have that a significant range of differential equations over $\mathbb{F}_{p^n}$ will have no solution, in this sense differential equations with solutions become scarce. In the literature written in German and English, there is the research of Bernd Steinbach and Christian Posthoff [123], who developed Boolean Differential Equations (BDE), as equations that include derivative operations and differential operators of a set of unknown Boolean functions $f : GF(2)^n \to GF(2)$. Additionally, they gave their Boolean Differential Calculus (BDC) published in the *Journal of Computational and Theoretical Nanoscience*. For our part, independently of the elegant research on BDE, we have developed Differential Equations for functions over finite fields, $f : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$, which generalizes the Boolean approach. Based upon the fact that $d^0(f)-1 \geq d^0(\partial_h(f))$, the algebraic degree on both sides of the equation is not the same, then the next two conclusions follow directly. For $\lambda \in \mathbb{F}_{p^n} \setminus \{0\}$, the differential operator $\sum_{\sigma=1}^{m} A_{h_1 \cdots h_\sigma} \partial^{(\sigma)}_{h_1 \cdots h_\sigma} : \mathbb{F}_{p^n}[X] \to \mathbb{F}_{p^n}[X]$ has no *eigenfunction* (an f such that it satisfies the equation appearing in the Corollary 9.4).

Corollary 9.4 *(Non-existence of solutions). Given λ in $\mathbb{F}_{p^n} \setminus \{0\}$, $m \geq 1$. Let $A_{h_1}, \ldots, A_{h_1 \cdots h_m}$ be elements of $\mathbb{F}_{p^n}$, and let $(h_1, \ldots, h_m)$ be a direction vector in $\left(\mathbb{F}^*_{p^n}\right)^m$. The linear differential equation $\sum_{\sigma=1}^{m} A_{h_1 \cdots h_\sigma} \partial^{(\sigma)}_{h_1 \cdots h_\sigma}(f) = \lambda f$*

has no non-trivial (non-zero) solutions on $\mathbb{F}_{p^n}[X]$.

Corollary 9.5 *Given* λ *and* h *in* $\mathbb{F}_{p^n} \setminus \{0\}$, *and the differential equation* $\partial_h(f) = \lambda f$. *For* $\lambda = 1$, *it follows that there are no non-trivial fixed points in the derivative operator.*

Quantum computing and quantum error-correcting codes are another attractive domain. There, Constanza Riera, Matthew G. Parker, and Pantelimon Stănică have generalized the so-called pure graph states—described by simple undirected graphs Gs; G corresponds to a quadratic and homogeneous Boolean function whose coefficients are entries in the adjacency matrix of G—to quantum states via graphs that can consist of edges of both types (directed/undirected), for which they obtain their associated Clifford group operators, see [114]. Other interesting material can be found in [75, 100, 96, 66].

9.1 Algebraic-Differential Analysis of Highly Resistant Functions (Part II)

In this section, we contribute to the powerful problem proposed by Pierrick Méaux and Dibyendu Roy [98], of finding Boolean functions whose derivative also has a high algebraic degree. We can ignore the maximal algebraic degree, since it corresponds to a function of notable vulnerability. Thus, the non-linear Boolean functions we produce have the highest effective algebraic degrees.

Theorem 9.6 *For all* $n, m, u \geq 1$, $u \neq n - m$, *and* $n \geq m + 2 \geq 3$, *it is satisfied that:* $d^0\big((x^{2^u} + x + 1)P_m(x)\big) = m + 1$ *and* $d^0\big(x^{2^u+1} + (x^{2^u} + x + 1)P_m(x)\big) = m + 1$.

Proof. By Theorem 5.1, $\texttt{Ldt}(P_m(x)) = \mathfrak{A}x^{2^{n-1}+\ldots+2^{n-m}}$, where $\mathfrak{A} \neq 0$, $n - 1 \geq m \geq 1$, and $\texttt{Ldt}(g)$ denotes the leading term (of a polynomial, g). Then, $x^{2^u}P_m(x)$ has its polynomial representation with degree no more than $2^n - 1$ given by $\texttt{Ldt}\big(x^{2^u}\big(P_m(x)\big)^{2^{u-(n-m-1)}}\big) = \mathfrak{A}^{2^{u-(n-m-1)}}x^{2^{n-1}+\ldots+2^u+2^{u-(n-m)}+\ldots+2^0}$ if $u \geq n - m$, and $\texttt{Ldt}(x^{2^u}P_m(x)) = \mathfrak{A}x^{2^{n-1}+\ldots+2^{n-m}+2^u}$ if $u \leq n - m - 1$. Furthermore, $\texttt{Ldt}(xP_m(x)) = \mathfrak{A}x^{2^{n-1}+\ldots+2^{n-m}+2^0}$. Which we summarize as: if $u > n-m$, $\texttt{Ldt}(x^{2^u}P_m(x)+xP_m(x)) = \mathfrak{A}x^{2^{n-1}+\ldots+2^{n-m}+2^0}$, while if $u \leq n-m-1$, $\texttt{Ldt}(x^{2^u}P_m(x) + xP_m(x)) = \mathfrak{A}x^{2^{n-1}+\ldots+2^{n-m}+2^u}$. Considering that theorem 5.1 implies that $d^0(P_m(x)) = m$, we accomplish to generalize Theorem 5.2, which we shall preserve because of its demonstration that has been motivating other demonstrations. On the other hand, $\mathfrak{A}x^{2^{n-1}+\ldots+2^{n-m}+2^u}$ prevails as the leading term for $x^{2^u+1} + (x^{2^u} + x + 1)P_m(x)$. □

Theorem 9.7 *Let* $x^{2^u+1} : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ *be Differentially* δ*-Uniform,* $n > 4$, $\frac{n-3}{2} \geq u \geq 1$, *and* $u \neq 2$. *Then, there exists a linear subspace* $\widetilde{\mathcal{S}} \leqslant (\mathbb{F}_2^n, +)$

such that $\forall h \in \mathcal{S}$ *(where* $\mathcal{S} = \mathbb{F}_{2^n} \setminus \widetilde{\mathcal{S}}$ *and* $|\mathcal{S}| = 2^n - \delta$*),* $d^0(\partial_h((x^{2^u} + x + 1)P_{n-2}(x))) = (n-1) - 1 = n - 2$.

Proof. Let $\mathfrak{M}^{(0)}_{Z_u}$ be the max algebraic degree part in Z_u, where $Z_u(x) = (x^{2^u} + x + 1)P_{n-2}(x)$. Next we obtain part $\mathfrak{M}^{(0)}_{Z_u}$, for which we proceed similarly to the proof we made in theorem 5.2, for which we multiply the monomial factors of degrees 2^0 and 2^u by the maximum algebraic degree part in P_{n-2}, considering each $\mathfrak{z}$ in the range $0 \neq \mathfrak{z} \leq \frac{n-1}{2}$, so that all possible terms of algebraic degree $d^0(Z_u)$ are considered. We do this analysis for $n > 4$, and bounded $u \neq 2$, $1 \leq u \leq \frac{n-3}{2}$.

$$\mathfrak{M}^{(0)}_{Z_u}(x) = \Big(\sum_{1 \leq \mathfrak{z} \leq \frac{n-1}{2}} \varkappa_{\mathfrak{z}} x^{-2^{\mathfrak{z}}} + \varkappa_{\mathfrak{z}}^{2^{-\mathfrak{z}}} x^{-2^{-\mathfrak{z}}} + \varkappa_{\mathfrak{z}}^{2^u} x^{-2^{\mathfrak{z}+u}} + \varkappa_{\mathfrak{z}}^{2^{u-\mathfrak{z}}} x^{-2^{u-\mathfrak{z}}} \Big)$$
$$+ \widehat{D}_{2|n} \varkappa_{n/2} x^{-2^{\frac{n}{2}}} (\varkappa_{n/2}^{2^u - 1} x^{(1-2^u)2^{\frac{n}{2}}} + 1) = \Big(\sum_{1 \leq \mathfrak{z} \leq \frac{n-1}{2}} \varkappa_{\mathfrak{z}} x^{-2^{\mathfrak{z}}} +$$
$$\sum_{1 \leq \mathfrak{z} \leq \frac{n-1}{2}} \varkappa_{\mathfrak{z}}^{2^{-\mathfrak{z}}} x^{-2^{-\mathfrak{z}}} + \sum_{u+1 \leq \mathfrak{z} \leq u + \frac{n-1}{2}} \varkappa_{\mathfrak{z}-u}^{2} x^{-2^{\mathfrak{z}}} + \sum_{1-u \leq \mathfrak{z} \leq \frac{n-1}{2} - u} \varkappa_{\mathfrak{z}+u}^{2^{-\mathfrak{z}}} x^{-2^{-\mathfrak{z}}} \Big)$$
$$+ \widehat{D}_{2|n} \varkappa_{n/2} x^{-2^{\frac{n}{2}}} (\varkappa_{n/2}^{2^u - 1} x^{(1-2^u)2^{\frac{n}{2}}} + 1)$$

$$\text{Regrouping, } \mathfrak{M}^{(0)}_{Z_u}(x) = \Big(\sum_{1-u \leq \mathfrak{z} < 0} (\varkappa_{\mathfrak{z}+u}^{2^{-\mathfrak{z}}} + \varkappa_{-\mathfrak{z}}) x^{-2^{-\mathfrak{z}}} + \sum_{\mathfrak{z}=u} \varkappa_{\mathfrak{z}} x^{-2^{\mathfrak{z}}} +$$
$$\sum_{u+1 \leq \mathfrak{z} \leq \frac{n-1}{2}} (\varkappa_{\mathfrak{z}} + \varkappa_{\mathfrak{z}-u}^{2}) x^{-2^{\mathfrak{z}}} + \sum_{\frac{n+1}{2} \leq \mathfrak{z} \leq u + \frac{n-1}{2}} (\varkappa_{\mathfrak{z}-u}^{2} + \varkappa_{-\mathfrak{z}}^{2^{\mathfrak{z}}}) x^{-2^{\mathfrak{z}}} +$$
$$\sum_{1 \leq \mathfrak{z} \leq \frac{n-1}{2} - u} (\varkappa_{\mathfrak{z}}^{2^{-\mathfrak{z}}} + \varkappa_{\mathfrak{z}+u}^{2^{-\mathfrak{z}}}) x^{-2^{-\mathfrak{z}}} + \sum_{\mathfrak{z}=0} \varkappa_{\mathfrak{z}+u}^{2^{-\mathfrak{z}}} x^{-2^{-\mathfrak{z}}} \Big)$$
$$+ \widehat{D}_{2|n} \varkappa_{n/2} x^{-2^{\frac{n}{2}}} (\varkappa_{n/2}^{2^u - 1} x^{(1-2^u)2^{\frac{n}{2}}} + 1)$$

, where the $\varkappa_{\mathfrak{z}}$s belong to $\mathbb{F}_{2^n}$, and $\widehat{D}_{2|n} \stackrel{\text{def}}{=} 1$, if 2 divides n, and is 0 otherwise. In view of Corollary 9.3, $\mathfrak{M}^{(0)}_{Z_u}$ is the derivative of some expression if and only if $d^0(\partial_h(Z_u)) \leq d^0(Z_u) - 2$. In case $\mathfrak{M}^{(0)}_{Z_u}$ is the derivative of some expression, let's name it $\mathfrak{N}_{Z_u}$ (see Eq. I in Theorem 9.2 concerning the derivative of monomials),

then due to size $d^0(\mathfrak{N}_{Z_u})$, the part $\mathfrak{M}^{(0)}_{Z_u}$ can only consist of n nonzero terms belonging to the derivative of a single term. I.e. $h(\neq 0)$ obeys the following nonlinear system of n equations, $\varkappa_{\mathfrak{z}+u}^{2^{-\mathfrak{z}}} + \varkappa_{-\mathfrak{z}} = h^{2^{-\mathfrak{z}}}$ for $1-u \leq \mathfrak{z} < 0$, $\varkappa_{\mathfrak{z}} = h^{2^{\mathfrak{z}}}$ for $\mathfrak{z} = u$, $\varkappa_{\mathfrak{z}} + \varkappa_{\mathfrak{z}-u}^{2} = h^{2^{\mathfrak{z}}}$ for $u+1 \leq \mathfrak{z} \leq \frac{n-1}{2}$, $\varkappa_{\mathfrak{z}-u}^{2} + \varkappa_{-\mathfrak{z}}^{2^{\mathfrak{z}}} = h^{2^{\mathfrak{z}}}$ for $\frac{n+1}{2} \leq \mathfrak{z} \leq u + \frac{n-1}{2}$, $\varkappa_{\mathfrak{z}}^{2^{-\mathfrak{z}}} + \varkappa_{\mathfrak{z}+u}^{2^{-\mathfrak{z}}} = h^{2^{-\mathfrak{z}}}$ for $1 \leq \mathfrak{z} \leq \frac{n-1}{2} - u$, $\varkappa_{\mathfrak{z}+u}^{2^{-\mathfrak{z}}} = h^{2^{-\mathfrak{z}}}$ for $\mathfrak{z} = 0$. Analyzing in the coordinates $\mathfrak{z} = 0$, $\mathfrak{z} = u$, we obtain $h^{2^u} = \varkappa_u = h$. If $\gcd(n,u) = 1$ (i.e. x^{2^u+1} is APN), then $h \in \mathbb{F}_2$. Regarding the APN case, to avoid that the part $\mathfrak{M}^{(0)}_{Z_u}$ coincides with the derivative of some function, it is enough to choose h outside $\mathbb{F}_2$ (in general, if the function is differentially δ-uniform, then h can acquire $2^n - \delta$ values). Which together with Theorem 9.6 give us an exceptionally high value for $d^0(\partial_h(Z_u))$, concluding the theorem. □

Corollary 9.8 *For all $h \in \mathbb{F}_{2^n} \setminus \mathbb{F}_2$, $n > 4$, $\frac{n-3}{2} \geq u \geq 1$, $u \neq 2$, such that $\gcd(n,u) = 1$, we have that $d^0(\partial_h((x^{2^u}+x+1)P_{n-2}(x))) = (n-1)-1 = n-2$.*

Open Problem 17. Investigate the quantity $d^0(\partial^{(2)}_{hh^*}(Z_u))$, for a pair of appropriate directions h, h^*, with $h \neq h^*$, as in the Corollary 9.8 or in Theorem 9.7. **Note.** The properties of $\mathfrak{M}^{(0)}_{Z_u}$ found by Theorem 9.7 together with the linearity of the derivative operator imply the following trade-off (between differentiation and the maximal part), $\mathfrak{M}^{(0)}_{\partial_h(Z_u)} = \partial_h\big(\mathfrak{M}^{(0)}_{Z_u}\big)$. Then, $d^0(\partial^{(2)}_{hh^*}(Z_u)) = d^0(Z_u) - 2$ occurs only if it is shown that $\partial_h\big(\mathfrak{M}^{(0)}_{Z_u}\big)$ is not the derivative in the h^* direction of any function. **Open Problem 18.** What about $d^0(\partial_h((x^{2^u}+x+1)P_m(x)))$ when $n-2 > m$? **Open Problem 19.** Similarly, attack this problem when considering the other family so important in theory and practice, $(x^{2^{2u}-2^u} + x^{2^{2u}-(2)2^u+1} + x^{2^{2u}-(2)2^u} + x^{2^{2u}-(3)2^u+1} + x^{2^{2u}-(3)2^u} + \ldots + x^{2^u+1} + x^{2^u} + x + 1)P_m(x)$ with the factor P_m for $m \geq 1$.

Theorem 9.9 *Given a non-constant function, f from and to $\mathbb{F}_{2^n}$. Then the following trace property holds: there exist at least 2^{n-1} elements $\zeta \in \mathbb{F}^*_{2^n}$ such that $d^0\big(Tr^1_n(\zeta f)\big) = d^0\big(f\big)$.*

Proof. Let $\mathfrak{M}^{(0)}_f$ be the maximum algebraic degree part in f. Since $\mathfrak{M}^{(0)}_f$ is non-constant, $\exists\, \mu, \mu' \in \mathbb{F}_{2^n}$ with $\mu = \mathfrak{M}^{(0)}_f(\alpha)$, $\mu' = \mathfrak{M}^{(0)}_f(\alpha')$, and $\mu - \mu' \in \mathbb{F}^*_{2^n}$, for some $\alpha, \alpha' \in \mathbb{F}_{2^n}$. Let m verifying $m \mid n$, $\mathcal{L} : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$ be a linear function, and the non-empty inverse images, $U' := \big(\mathfrak{M}^{(0)}_f\big)^{-1}(\mu')$ and $U := \big(\mathfrak{M}^{(0)}_f\big)^{-1}(\mu)$. Then $\exists\, \zeta_{\mathcal{L},f,\mu-\mu'} \in \mathbb{F}^*_{2^n}$ such that $\mathcal{L}\big(\zeta_{\mathcal{L},f,\mu-\mu'}\mu - \mu'\big) \in \mathbb{F}^*_{2^m}$. Then $\mathcal{L}\big(\zeta_{\mathcal{L},f,\mu-\mu'}\mathfrak{M}^{(0)}_f(U)\big) - \mathcal{L}\big(\zeta_{\mathcal{L},f,\mu-\mu'}\mathfrak{M}^{(0)}_f(U')\big) = \mathcal{L}\big(\zeta_{\mathcal{L},f,\mu-\mu'}\mu\big) - \mathcal{L}\big(\zeta_{\mathcal{L},f,\mu-\mu'}\mu'\big) = \mathcal{L}\big(\zeta_{\mathcal{L},f,\mu-\mu'}\mu - \mu'\big) \neq 0$. That is, $\mathcal{L}\big(\zeta_{\mathcal{L},f,\mu-\mu'}\mathfrak{M}^{(0)}_f\big)$ does not vanish, or rather, it is not a constant function. Since $d^0\big(\mathcal{L}\big(\zeta_{\mathcal{L},f,\mu-\mu'}x\big)\big) = 1$ (here we are writing the function with its independent variable x), the terms in $\mathcal{L}\big(\zeta_{\mathcal{L},f,\mu-\mu'}\mathfrak{M}^{(0)}_f\big)$ have

the same algebraic degree as $\mathfrak{M}_f^{(0)}$. We can then bound as follows, $d^0\big(\mathfrak{M}_f^{(0)}\big)=\max\big(d^0\big(\mathcal{L}\big(\zeta_{\mathcal{L},f,\mu-\mu'}\mathfrak{M}_f^{(0)}\big)\big),d^0\big(\mathcal{L}\big(\zeta_{\mathcal{L},f,\mu-\mu'}\big(f-\mathfrak{M}_f^{(0)}\big)\big)\big)\big)=d^0\big(\mathcal{L}\big(\zeta_{\mathcal{L},f,\mu-\mu'}f\big)\big)\leq d^0\big(f\big)$. Thus, $d^0\big(\mathcal{L}\big(\zeta_{\mathcal{L},f,\mu-\mu'}f\big)\big)=d^0\big(f\big)$. In particular, if $\mathcal{L}=Tr_n^1$, at least $2^{n-1}=|\{x\in\mathbb{F}_{2^n}^*;\mathcal{L}\big((\mu-\mu')x\big)\in\mathbb{F}_{2^m}^*\}|$ of these $\zeta_{\mathcal{L},f,\mu-\mu'}$ are obtained. □

Specifically, we apply the Theorem 9.9 to the functions $\partial_h(Z_u)$ and Z_u, since they have very high algebraic degrees, $d^0(\partial_h(Z_u))$ and $d^0(Z_u)$, and we immediately obtain the new product $d^0\big(Tr_n^1\big(\zeta_1\partial_h(Z_u)\big)\big)d^0\big(Tr_n^1\big(\zeta_2Z_u\big)\big)$, which is also very high; we will now express this.

Theorem 9.10 *Let $n>4$, $\frac{n-3}{2}\geq u\geq 1$, $u\neq 2$, $\delta=\Delta_{x^{2^u+1}}$, $\widetilde{\mathcal{S}}\leqslant(\mathbb{F}_2^n,+)$ a linear subspace, $\mathcal{S}=\mathbb{F}_{2^n}\setminus\widetilde{\mathcal{S}}$, $|\mathcal{S}|=2^n-\delta$, and Z_u be as in Theorem 9.7. Then $\forall h\in\mathcal{S}$, there are 2^{n-1} elements ζ_1 (also 2^{n-1} elements ζ_2) $\in\mathbb{F}_{2^n}^*$ satisfying,*

$$d^0\big(Tr_n^1\big(\zeta_1\partial_h(Z_u)\big)\big)=n-2 \text{ and } d^0\big(Tr_n^1\big(\zeta_2Z_u\big)\big)=n-1.$$

Corollary 9.11 *Let $n>4$, $\frac{n-3}{2}\geq u\geq 1$, $u\neq 2$, $\gcd(n,u)=1$, and Z_u be as in Theorem 9.7. Then $\forall h\in\mathbb{F}_{2^n}\setminus\mathbb{F}_2$, there are 2^{n-1} elements ζ_1 (and 2^{n-1} elements ζ_2) $\in\mathbb{F}_{2^n}^*$ verifying the following identities,*

$$d^0\big(Tr_n^1\big(\zeta_1\partial_h(Z_u)\big)\big)=n-2 \text{ and } d^0\big(Tr_n^1\big(\zeta_2Z_u\big)\big)=n-1.$$

Open Problem 20: When can $nl(\partial_h(f))$ be bounded in terms of $nl(f)$?

9.2 The Boundary Value Problem for Galois Fields

An important component of the miscellaneous techniques for the design of control laws are based upon the solution of the boundary value problem. Let us consider $F\big(\Theta,\partial_{\mathfrak{s}}(\Theta),\widetilde{\Theta}\big)=0$, where $F\big(\Theta,\partial_{\mathfrak{s}}(\Theta),\widetilde{\Theta}\big)=\widetilde{\Theta}-\partial_{\mathfrak{s}}(\Theta)$, and $\widetilde{\Theta}$ is a signal (function) with values in the field $\mathbb{F}_{p^n}$; in Theorem 9.13 we obtain the desired trajectory Θ (for the first and exclusive time for $\mathbb{F}_{p^n}$) required to pass through the points (x_t,y_t); forming a valuable part of the so-called *trajectory control*, for which some guiding parameters must be embedded in F. In a typical boundary value problem for functions such as those defined on $\mathbb{R}^n$, taking into account the type of smoothness and geometry of the domain pre-assigned to the unknown function are compromised with the structure of the problem-solving method. In the discrete case, the domain may be a subset of points, which will not be relevant here; therefore, we shall consider all of $\mathbb{F}_{p^n}$. We provide new results in this respect in the field of finite fields $\mathbb{F}_{p^n}$. During these years, $\mathbb{F}_{2^n}$, which presents the underlying structure of $\{0,1\}^n$, has been gaining special attention in the field of artificial intelligence. From part of the proof of Theorem 9.13, Theorem 9.12 can be deduced.

Theorem 9.12 *(Existence of solutions of the I.V.P.) Let* $\widetilde{\Theta} : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$, $\mathfrak{s} \in \mathbb{F}_{p^n} \setminus \{0\}$, $\partial_{\mathfrak{s}}(\widetilde{\Theta}) = 0$, $2 \leq d^0(\widetilde{\Theta}) \leq (p-1)(n-1)$, $n \geq 3$, *and* $(x_0, y_0) \in \left(\mathbb{F}_{p^n}\right)^2$, *such that the following initial value problem (I.V.P.) is satisfied,* $\partial_{\mathfrak{s}}(\Theta) = \widetilde{\Theta}$, *and* (x_0, y_0) *belongs to the graph* $\mathcal{G}_{\Theta}$. *Then there exists a solution set, of the form* $\Theta_0 + \partial_{\mathfrak{s}^{p-1}}^{(p-1)}\left(\mathbb{F}_{p^n}[X]\right)$, *for this problem, where* $\Theta_0 : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ *is some function satisfying* $\partial_{\mathfrak{s}}(\Theta_0) = \widetilde{\Theta}$.

Theorem 9.13 *(Existence and form of solutions of the B.V.P.). Let* p *be a prime number. Let* $\widetilde{\Theta} : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$, $a_0 = (x_0, y_0)$ *and* $a_t = (x_t, y_t)$ *two points in* $\left(\mathbb{F}_{p^n}\right)^2$, $x_t \neq x_0$, $n \geq 3$, $t \geq 1$, $2 \leq d^0(\widetilde{\Theta}) \leq (p-1)(n-1)$, $\partial_{\mathfrak{s}}(\widetilde{\Theta}) = 0$, *and* $\mathfrak{s} \in \mathbb{F}_{p^n} \setminus \{0\}$, *such that the following boundary value problem (B.V.P.) governs:*

$$\begin{cases} \partial_{\mathfrak{s}}(\Theta) = \widetilde{\Theta}, \\ \Theta(x_0) = y_0, \\ \Theta(x_t) = y_t \end{cases}$$

There exists a function $\Theta_0 : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ *satisfying* $\partial_{\mathfrak{s}}(\Theta_0) = \widetilde{\Theta}$, *and the solutions of the B.V.P. are the functions of the form* $\Theta_0 + \partial_{\mathfrak{s}^{p-1}}^{(p-1)}(\check{\varphi})$, *where* $\check{\varphi} \in \mathbb{F}_{p^n}[X]$. *Specifically, it happens that:*

A1). If $p \neq 2$ *and some odd integer other than 1 divides* n, *there are solutions such that* $\check{\varphi}(x) = \frac{\omega(a_0,a_t)\phi(x)}{\partial_{\mathfrak{s}^{p-1}}^{(p-1)}(\phi)(x_t)} + \frac{y_0 - \Theta_0(x_0)}{(p-1)!\mathfrak{s}^{p-1}} x^{p-1}$, $\phi(x) = (x - x_0)^{p^{\xi}+p-1} - \frac{c_{\xi}(x^{p-1}-x_0)}{(p-1)!\mathfrak{s}^{p-1}}$, $\omega(a_0, a_t) = y_t - y_0 + \partial_{x_0 - x_t}(\Theta_0)(x_t)$, $c_{\xi} = \partial_{\mathfrak{s}^{p-1}}^{(p-1)}\left(x^{p^{\xi}+p-1}\right)(0)$, *and* $\varrho(x - x_0) = (x - x_0)^{p^{\xi}+1}$ *is a Perfect Nonlinear (PN) function.*

A2). If $p = 2$*: for all* $x_t \notin x_0 + \mathfrak{s}\mathbb{F}_2$, *there are solutions such that* $\phi(x) = \check{\phi}(x - x_0) - \frac{\partial_{\mathfrak{s}^{p-1}}^{(p-1)}\check{\phi}(0)(x^{p-1}-x_0)}{(p-1)!\mathfrak{s}^{p-1}}$, *and* $\check{\phi}$ *is any Almost Perfect Nonlinear (APN) function. If* $a_t = (x_0 + \mathfrak{s}, y_t)$, *the B.V.P. has a solution only when* $\widetilde{\Theta}(x_0) + y_0 = y_t$.

Proof. Since $\partial_{\mathfrak{s}}(\widetilde{\Theta}) = 0$, Theorem 9.2 applied to each part of a different algebraic degree in $\widetilde{\Theta}$ implies that there exists a function $\Theta_0 = \partial_{\mathfrak{s}^{p-2}}^{(p-2)}(\varphi)$, for some $\varphi \in \mathbb{F}_{p^n}[X]$, such that $\partial_{\mathfrak{s}}(\Theta_0) = \widetilde{\Theta}$ (i.e. Θ_0 is a particular solution to the associated differential equation of the B.V.P.). Let $\Theta_G = \Theta_0 + \widetilde{\psi}$ be the general solution of $\partial_{\mathfrak{s}}(\Theta) = \widetilde{\Theta}$, then $\partial_{\mathfrak{s}}(\Theta_0) + \partial_{\mathfrak{s}}(\widetilde{\psi}) = \widetilde{\Theta}$. Again, by Theorem 9.2, any solution to the homogeneous equation $\partial_{\mathfrak{s}}(\widetilde{\psi}) = 0$ is given by $\widetilde{\psi} = \partial_{\mathfrak{s}^{p-1}}^{(p-1)}(\check{\varphi})$, for some $\check{\varphi} \in \mathbb{F}_{p^n}[X]$. Then, the $\Theta_G = \Theta_0 + \partial_{\mathfrak{s}^{p-1}}^{(p-1)}(\check{\varphi})$ constitute the solution set of $\partial_{\mathfrak{s}}(\Theta) = \widetilde{\Theta}$ on $\mathbb{F}_{p^n}[X]$. The boundary conditions applied to Θ_G provide constraints on the $(p-1)$-th derivative of $\check{\varphi}$ in the direction $\mathfrak{s}$; decomposing $\check{\varphi}$ as its linear combination over $\mathbb{F}_{p^n}$ of x^{p-1} and a function ϕ, those conditions

become the following system for ϕ:

$$\begin{cases} \frac{\omega(a_0,a_t)}{v_t}\partial^{(p-1)}_{\mathfrak{s}^{p-1}}(\phi)(x_0) + \partial^{(p-1)}_{\mathfrak{s}^{p-1}}\left(\frac{y_0-\Theta_0(x_0)}{(p-1)!\mathfrak{s}^{p-1}}x^{p-1}\right)(x_0) = y_0 - \Theta_0(x_0), \\ \frac{\omega(a_0,a_t)}{v_t}\partial^{(p-1)}_{\mathfrak{s}^{p-1}}(\phi)(x_t) + \partial^{(p-1)}_{\mathfrak{s}^{p-1}}\left(\frac{y_0-\Theta_0(x_0)}{(p-1)!\mathfrak{s}^{p-1}}x^{p-1}\right)(x_t) = y_t - \Theta_0(x_t) \end{cases}$$

where $\omega(a_0, a_t) = y_t - y_0 + \partial_{x_0-x_t}(\Theta_0)(x_t)$, $v_t = \partial^{(p-1)}_{\mathfrak{s}^{p-1}}\phi(x_t)$, with $v_t \neq 0$. Moreover, $\partial^{(p-1)}_{\mathfrak{s}^{p-1}}(x^{p-1}) = (p-1)!\mathfrak{s}^{p-1}$ is obtained by Eq. I in Theorem 9.2; clearly there cannot be parts of lower algebraic degree when the part of *m.a.d.* (maximum algebraic degree) is a constant. Such boundary conditions reduce to finding ϕ that fits: $\partial^{(p-1)}_{\mathfrak{s}^{p-1}}\phi(x_0) = 0$ and $\partial^{(p-1)}_{\mathfrak{s}^{p-1}}\phi(x_t) = v_t$, where $v_t \neq 0$.

Case: p an odd prime. Given $n > \xi \geq 1$, we apply the high-order derivative operator to obtain:

$$\begin{aligned} \partial^{(p-1)}_{\mathfrak{s}^{p-1}}\left(x^{p^\xi+p-1}\right) &= \mathfrak{s}^{p-1}(p-1)!x^{p^\xi} + (p-1)!\mathfrak{s}^{p^\xi+p-2}x + c_\xi \\ &= (p-1)!\mathfrak{s}^{p-2}\partial_{\mathfrak{s}}\left(x^{p^\xi+1}\right) + \hat{c}_\xi \text{ on } \mathbb{F}_{p^n} \end{aligned}$$

Where $c_\xi, \hat{c}_\xi \in \mathbb{F}_{p^n}$. For any $F \in \mathbb{F}_{p^n}[X]$, $A \in \mathbb{F}_{p^n}$, and $k \geq 1$, it is straightforward to show that $\partial^{(k)}_{\mathfrak{s}^k}(F(x+A)) = \partial^{(k)}_{\mathfrak{s}^k}F(x+A)$, where the right-hand side is the function k-th derivative of F evaluated at $x+A$. Then $\partial^{(p-1)}_{\mathfrak{s}^{p-1}}\left((x-x_0)^{p^\xi+p-1}\right) = \partial^{(p-1)}_{\mathfrak{s}^{p-1}}x^{p^\xi+p-1}(\text{at } x-x_0) = (p-1)!\mathfrak{s}^{p-2}\partial_{\mathfrak{s}}\left((x-x_0)^{p^\xi+1}\right) + \hat{c}_\xi$. Then $\phi(x) = (x-x_0)^{p^\xi+p-1} - \frac{c_\xi(x^{p-1}-x_0)}{(p-1)!\mathfrak{s}^{p-1}}$ exists verifying $\partial^{(p-1)}_{\mathfrak{s}^{p-1}}\phi(x_0) = 0$. Suppose $\partial^{(p-1)}_{\mathfrak{s}^{p-1}}\phi(x_t) = \partial^{(p-1)}_{\mathfrak{s}^{p-1}}\phi(x_0)$, then $(p-1)!\mathfrak{s}^{p-2}\partial_{\mathfrak{s}}\left((x-x_0)^{p^\xi+1}\right)(x_t) + \hat{c}_\xi - c_\xi = (p-1)!\mathfrak{s}^{p-2}\partial_{\mathfrak{s}}\left((x-x_0)^{p^\xi+1}\right)(x_0) + \hat{c}_\xi - c_\xi$. Then, $\partial_{\mathfrak{s}}\left((x-x_0)^{p^\xi+1}\right)(x_t) = \partial_{\mathfrak{s}}\left((x-x_0)^{p^\xi+1}\right)(x_0) = \mu$, for some $\mu \in \mathbb{F}_{p^n}$, which contradicts property $\max_{a\in\mathbb{F}_{p^n}\setminus\{0\}, b\in\mathbb{F}_{p^n}} \delta_\varrho(a,b) = 1$ of the *planar* function $\varrho(x-x_0) = (x-x_0)^{p^\xi+1}$ (at this point we are dealing with the planar function defined by Dembowski and Ostrom in [53]; also called *perfect nonlinear*; it always exists for $p \neq 2$), such that some odd integer other than 1 divides n, and $n/\gcd(n,\xi)$ is odd (see [63, 45, 74]). Then the remaining condition is met:

$$\partial^{(p-1)}_{\mathfrak{s}^{p-1}}\phi(x_t) \neq 0 \text{ for all } x_t \text{ in } \mathbb{F}_{p^n} \setminus \{x_0\}.$$

Case: $p = 2$, the even characteristic. $d^0(\widetilde{\Theta})$ can be arbitrary. We choose $\phi(x) = \check{\phi}(x-x_0) - \frac{\partial^{(p-1)}_{\mathfrak{s}^{p-1}}\check{\phi}(0)(x^{p-1}-x_0)}{(p-1)!\mathfrak{s}^{p-1}}$ such that $\check{\phi}$ is any APN (also known as *semi-planar* [46]) function over $\mathbb{F}_{2^n}$ (it always exists; thus $\check{\varphi}$ is APN too; see Table 1), such that $x_t \notin x_0 + \mathfrak{s}\mathbb{F}_2$. If $a_t = (x_0 + \mathfrak{s}, y_t)$: we can deal with this part directly. □

There is a wide variety of functions $\widetilde{\Theta}$ verifying $\partial_{\mathfrak{s}}(\widetilde{\Theta}) = 0$. When looking for the *integral curves* (solutions of I.V.P. or B.V.P.) it is essential to solve

the associated homogeneous equation. Let the $\mathfrak{s}_i$s ($\neq 0$) be mutually distinct directions, where $r \geq 1$. More generally, the function spaces over the field $\mathbb{F}_{p^n}$ given below play a leading role.

The kernel $\mathcal{D}_{\mathbb{F}_{p^n};\mathfrak{s}_1,\ldots,\mathfrak{s}_r} \stackrel{\text{def}}{=} \{f \in \mathbb{F}_{p^n}[X];\ \partial^{(r)}_{\mathfrak{s}_1,\ldots,\mathfrak{s}_r}(f) = 0\}$,
The *Space of R. Carranza* given below
$\overset{\circ}{\mathcal{C}}_{\mathbb{F}_{p^n};\mathfrak{s}_1,\ldots,\mathfrak{s}_r} \stackrel{\text{def}}{=} \{f \in \mathbb{F}_{p^n}[X];\ f = \partial^{(p-1)}_{\mathfrak{s}_1^{p-1}}(\varphi_1) + \ldots + \partial^{(p-1)}_{\mathfrak{s}_r^{p-1}}(\varphi_r) + L^{(d^0\leq r-1)} +$
$\sum_{\ell=1}^{m} L_\ell^{(d^0=r-1)} \partial^{(rp-r)}_{\mathfrak{s}_1^{p-1},\ldots,\mathfrak{s}_r^{p-1}}(\psi_\ell)$, where m is an integer, each φ_ℓ, ψ_ℓ is in $\mathbb{F}_{p^n}[X]$,
$L^{(d^0\leq r-1)} \in \mathbb{F}_{p^n}^{d^0\leq r-1}[X]$, and each $L_\ell^{(d^0=r-1)} \in \mathbb{F}_{p^n}^{d^0=r-1}[X]$ (see Definition 1.13)$\}$.

In the scenario where there is barely a particular solution Θ_0 for the equation of the form $\partial^{(r)}_{\mathfrak{s}_1,\ldots,\mathfrak{s}_r}(\Theta) = \widetilde{\Theta}$, for the case $p = 2$ there automatically exists an f in $\overset{\circ}{\mathcal{C}}_{\mathbb{F}_{p^n};\mathfrak{s}_1,\ldots,\mathfrak{s}_r}$, with an φ_1 APN in its formula, such that the trajectory $\Theta = \Theta_0 + f$ fits the given boundary conditions. For any prime p, these vector spaces respect the subspace relation given below:

$$\overset{\circ}{\mathcal{C}}_{\mathbb{F}_{p^n};\mathfrak{s}_1,\ldots,\mathfrak{s}_r} \leqslant \mathcal{D}_{\mathbb{F}_{p^n};\mathfrak{s}_1,\ldots,\mathfrak{s}_r} \leqslant \mathbb{F}_{p^n}[X]$$

Problem 21. Is subspace $\overset{\circ}{\mathcal{C}}_{\mathbb{F}_{p^n};\mathfrak{s}_1,\ldots,\mathfrak{s}_r}$ equal to $\mathcal{D}_{\mathbb{F}_{p^n};\mathfrak{s}_1,\ldots,\mathfrak{s}_r}$?

Problem 22. Investigate the homogeneous *differential equation* $\mathbb{F}_{p^n}$ associated with each situation given below (especially when the directions $\mathfrak{s}_i(\neq 0)$ are mutually distinct), where $\widetilde{\Theta} : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ is some appropriate function:

P1). $\partial^{(3)}_{\mathfrak{s}_1\mathfrak{s}_2\mathfrak{s}_3}(f) + \partial^{(3)}_{\mathfrak{s}_4\mathfrak{s}_5\mathfrak{s}_6}(f) + \partial^{(3)}_{\mathfrak{s}_7\mathfrak{s}_8\mathfrak{s}_9}(f) = \widetilde{\Theta}$ on $\mathbb{F}_{2^n}$.

P2). For p even or odd, for some pair k, m in $\mathbb{N}$, $\sum_{\ell=1}^{m} \partial^{(k)}_{\mathfrak{s}_{\ell_1}\ldots\mathfrak{s}_{\ell_k}}(f) = \widetilde{\Theta}$ on $\mathbb{F}_{p^n}$.

Note that when there is no ambiguity, we are free to use $\partial^{(3)}_{\mathfrak{s}_1\mathfrak{s}_2\mathfrak{s}_3}(f)$ (without commas) to denote $\partial^{(3)}_{\mathfrak{s}_1,\mathfrak{s}_2,\mathfrak{s}_3}(f)$.

Let $n, m \geq 1$, we say that a function f in $\mathbb{F}_{p^n}[X_1, \cdots, X_m]$ is *harmonic* when it is a solution to Laplace's equation, i.e. $\nabla^2(f) = 0$, where the first member of this equation symbolizes the Laplacian operator of f: $\nabla^2(f) \stackrel{\text{def}}{=} \sum_{i=1}^{m} \partial^{(2)}_{X_i=H_i,X_i=H_i}(f)$, with respect to some vector $(H_1, \ldots, H_m) \in \left(\mathbb{F}_{p^n}^*\right)^m$, also the subfix $X_i = H_i, X_i = H_i$ means that the first order derivative is taken with respect to the variable X_i in the direction H_i, followed by the first order derivative with respect to the variable X_i in the direction H_i, again. As we have seen before, symbols like $\Delta(f)$ are reserved to indicate the uniform

differentiability of f. Let us denote by $\mathbb{F}_{p^n}$-$\mathcal{H}\mathtt{arm}_{(H_1,\ldots,H_m)}$, and in compact notation by $\mathbb{F}_{p^n}$-$\mathcal{H}\mathtt{arm}$, the space of *harmonic* functions on $\mathbb{F}_{p^n}$ relative to the vector $(H_1,\ldots,H_m) \in \left(\mathbb{F}_{p^n}^*\right)^m$. We encourage readers interested in exploring interesting connections in the context of Continuum Mechanics and Finite Elements—in addition to their pertinent differential operators—to consult the work of Lev Steinberg and R. Kvasov [125, 124], as well as research by R. Carranza with Steinberg [110]. In the field of Deep Learning, methods are being developed to deal with BVP (on $\mathbb{R}^n$). E.g., Ziad Aldirany, Régis Cottereau, Marc Laforest, and Serge Prudhomme [1] recently published a method capable of capturing smaller scales of the solution at each level of the process by applying an appropriate neural network in charge of minimizing the resulting residual (and therefore the size of its corresponding numerical error). There is a stream of work in this regard [3, 137]. Let's dive into our next result.

Theorem 9.14 *Let p be a prime number; $n, m \geq 1$, $1 \leq i \leq m$, and $(H_1,\cdots,H_m) \in \left(\mathbb{F}_{p^n}^*\right)^m$. Then: $\mathbb{F}_{p^n}[X_1,\cdots,X_m] \subseteq \ker\left(\partial_{X_i^p}^{(p)}\right)$, where each derivative operator ∂_{X_i} runs along H_i.*

Proof. We will begin by applying the principle of mathematical induction in $\mathbb{Z}^+$. Let's choose a polynomial function with coefficients in the finite field $\mathbb{F}_{p^n}$, i.e. $\zeta \in \mathbb{F}_{p^n}[X_1,\cdots,X_m]$. Let's suppose that for $\sigma \in \mathbb{Z}^+$ we have:

$\widetilde{\partial_{h^\sigma}^{(\sigma)}}(\zeta) = \sum_{\theta=0}^{\sigma} h^{-\sigma}(-1)^\theta \binom{\sigma}{\theta} \zeta((\sigma-\theta)h + \mathtt{id}) = h^{-\sigma}(-1)^\sigma\zeta + \sum_{\theta=0}^{\sigma-1} h^{-\sigma}(-1)^\theta \binom{\sigma}{\theta}$ $(h\widetilde{\partial_{(\sigma-\theta)h}}(\zeta) + \zeta)$, it can be seen that this is true for $\sigma = 1$. We apply the derivations with respect to the variable X_i, and in the direction H_i, which we will denote by h. The other variables are considered constant. Next, we obtain the version of this equation corresponding to $\sigma + 1$.

$\widetilde{\partial}_h(\widetilde{\partial_{h^\sigma}^{(\sigma)}}(\zeta)) = h^{-\sigma}(-1)^\sigma\widetilde{\partial}_h(\zeta) + \sum_{\theta=0}^{\sigma-1} h^{-\sigma}(-1)^\theta \binom{\sigma}{\theta}(\widetilde{\partial_{(\sigma+1-\theta)h}}(\zeta) + h^{-1}\zeta) + \sum_{\theta=0}^{\sigma-1}$ $h^{-\sigma}(-1)^{\theta+1}\binom{\sigma}{\theta}(\widetilde{\partial_{(\sigma-\theta)h}}(\zeta) + h^{-1}\zeta) = h^{-\sigma}\widetilde{\partial_{(\sigma+1)h}}(\zeta) + (1 + (-1)^{\sigma+1})h^{-\sigma-1}\zeta +$ $\sum_{\theta=1}^{\sigma} h^{-\sigma}(-1)^\theta \binom{\sigma}{\theta}(\widetilde{\partial_{(\sigma+1-\theta)h}}(\zeta) + h^{-1}\zeta) + \sum_{\theta=0}^{\sigma-1} h^{-\sigma}(-1)^{\theta+1}\binom{\sigma}{\theta}(\widetilde{\partial_{(\sigma-\theta)h}}(\zeta) + h^{-1}\zeta) =$ $h^{-\sigma}\widetilde{\partial_{(\sigma+1)h}}(\zeta) + (1+(-1)^{\sigma+1})h^{-\sigma-1}\zeta + \sum_{\theta=1}^{\sigma} h^{-\sigma}(-1)^\theta \binom{\sigma}{\theta}(\widetilde{\partial_{(\sigma+1-\theta)h}}(\zeta) + h^{-1}\zeta) +$ $\sum_{\varkappa_1=1}^{\sigma} h^{-\sigma}(-1)^{\varkappa_1}\binom{\sigma}{\varkappa_1-1}(\widetilde{\partial_{(\sigma+1-\varkappa_1)h}}(\zeta) + h^{-1}\zeta) = h^{-\sigma}\widetilde{\partial_{(\sigma+1)h}}(\zeta) + h^{-\sigma-1}\zeta + (-1)^{\sigma+1}$ $h^{-\sigma-1}\zeta + \sum_{\varkappa_2=1}^{\sigma} h^{-\sigma}(-1)^{\varkappa_2}\left(\binom{\sigma}{\varkappa_2} + \binom{\sigma}{\varkappa_2-1}\right)(\widetilde{\partial_{(\sigma+1-\varkappa_2)h}}(\zeta) + h^{-1}\zeta) = \sum_{\varkappa_2=0}^{\sigma+1} h^{-\sigma}(-1)^{\varkappa_2}$ $\binom{\sigma+1}{\varkappa_2}(\widetilde{\partial_{(\sigma+1-\varkappa_2)h}}(\zeta) + h^{-1}\zeta)$. This is the same expression in the inductive hypothesis, but for $\sigma+1$ instead of σ. That is, this formula holds for all $\sigma \in \mathbb{Z}^+$.

If we choose $\sigma = p$ to be a prime number, then $\sigma | \binom{\sigma}{\theta}$ for all $1 \leq \theta \leq \sigma - 1$. Then, the operator $\widetilde{\partial_{h^\sigma}^{(\sigma)}}$ under $\mod (p)$ takes the following form:

$\widetilde{\partial_{h^\sigma}^{(\sigma)}}(\zeta) = h^{-\sigma}(-1)^\sigma \zeta + h^{-\sigma}(h\widetilde{\partial_{\sigma h}}(\zeta) + \zeta) \equiv 0$. Besides, inductively we can obtain that $\partial_{h^\sigma}^{(\sigma)}(\zeta) = h^\sigma \widetilde{\partial_{h^\sigma}^{(\sigma)}}(\zeta)$. Then, $\partial_{h^p}^{(p)}(\zeta) = (0)h^p = 0$ on $\mathbb{F}_{p^n}$, for all $\zeta \in \mathbb{F}_{p^n}[X_1, \cdots, X_m]$, which completes the demonstration. □

So the derivative of order p with respect to the same direction h applied to any function ζ of $\mathbb{F}_{p^n}[X_1, \cdots, X_m]$ is the function 0, for all $n, m \geq 1$.

Corollary 9.15 *Let $n, m \geq 1$, and $(H_1, \cdots, H_m) \in \left(\mathbb{F}_{2^n}^*\right)^m$. Then:* $\mathbb{F}_{2^n}[X_1, \cdots, X_m] \subseteq \mathbb{F}_{2^n}\text{-}\mathcal{H}\mathtt{arm}_{(H_1,\ldots,H_m)}$.

We will leave Theorem 9.16 as an exercise; its proof is quite straightforward. The transformation $\partial_H(.) : \mathbb{F}_{p^n}[X] \to \mathbb{F}_{p^n}[X]$ is a $\mathbb{F}_{p^n}$-Derivation over the algebra $\mathbb{F}_{p^n}[X]$, that is, it is $\mathbb{F}_{p^n}$-linear and satisfies the Leibniz product rule that will be given shortly, even with that form it takes it is still capable of supporting very beautiful implications.

Theorem 9.16 *(A Product Rule) Let F and G be in $\mathbb{F}_{p^n}[X]$, with variable X in $\mathbb{F}_{p^n}$, and $H \in \mathbb{F}_{p^n}^*$. Then $\partial_H(FG) = \partial_H(F)G(\mathtt{id} + H) + F\partial_H(G)$.*

9.3 What Is Beyond the Fractional Derivative?

In article [68], motivated by article [15], the formula ${}_c\partial_a(f) = f(x+a) - cf(x)$ (c-derivative of f with respect to a) was introduced to study the size of the important set $\{x \in \mathbb{F}_{p^n}; {}_c\partial_a(f) = b\}$ associated with a function f, which can go from a $\mathbb{F}_{p^n}$ to a $\mathbb{F}_{p^m}$, for points $(a, (b, c)) \in \mathbb{F}_{p^n} \times \left(\mathbb{F}_{p^m}\right)^2$; the idea is to broaden the landscape that was founded on the basis of Definition 1.19. We recommend visiting Section 1.1 and Table 1. Fortunately, such transformation ${}_c\partial_a$ is linear. The classical product rule is not fulfilled, but a property that can be demonstrated directly is fulfilled, which can be understood as its generalization, covering the case $c \neq 1$: ${}_c\partial_a(fg)(x) = g(x+a){}_c\partial_a(f)(x) + cf(x)\partial_a(g)(x) = g(x+a){}_c\partial_a(f)(x) + cf(x){}_1\partial_a(g)(x)$. **Note.** this formula reveals that the new ${}_c\partial_a$ (seen as a Derivation) "has not yet properly freed itself from its predecessor, ∂_a". It is therefore important to investigate both worlds, for $c \neq 1$ and for $c = 1$. On the other hand, research has been carried out aimed at obtaining properties of differentially (c, δ)-uniform functions using this toy of recent arrival. This section introduces our treatment of the subject from a different perspective. A few centuries have passed since the discovery of the fractional derivative (year 1695). As if we were exploring beyond our solar system, we investigate whether or not there might be other types of derivative order beyond the fractional one. Let E be an operator in general, and $\ell \geq 2$

be an integer. In a rather customary manner, the symbol $E^{(\ell)}$ denotes the corresponding operator of order ℓ, i.e., $E^{(\ell)} = E \circ E^{(\ell-1)}$, where $E^{(1)} = E$.

Our Point of View: Let us introduce the following objects.

Definition 9.17 *Let $a \in \mathbb{F}_{p^n}$ (i.e., direction 0 is included). For each $c \in \mathbb{F}_{p^n} \setminus \{1\}$, the operator $\mathcal{I}_{p-1,a,1-c} := \left(\frac{{}_c\partial_a}{1-c}\right)^{(p-1)}$ will be termed as the* mod (p)*-c-integral operator of R. Carranza-Ellingsen-Felke-Riera-Stănică-Tkachenko-Borisov-Chew-Johnson-Wagner in the direction a. On the other hand, $\frac{{}_c\partial_a}{1-c}$ will be termed as the* mod (p)*-c-derivative operator of R. Carranza et al.*

Theorem 9.18 (Novel Fundamental Theorem of Calculus (FTC)) *Let p be a prime number, $a \in \mathbb{F}_{p^n}$, $c \in \mathbb{F}_{p^n} \setminus \{1\}$, and $\mathtt{id}_{\mathcal{F}\left(\mathbb{F}_{p^n},\mathbb{F}_{p^n}\right)}$ be the identity map over the function space $\mathcal{F}\left(\mathbb{F}_{p^n},\mathbb{F}_{p^n}\right)$. Then,*

$$\mathcal{I}_{p-1,a,1-c} \circ \frac{{}_c\partial_a}{1-c} = \mathtt{id}_{\mathcal{F}\left(\mathbb{F}_{p^n},\mathbb{F}_{p^n}\right)}.$$

Proof. Next we shall apply the principle of mathematical induction. Let us suppose that for an integer, σ, and a function $\zeta \in \mathcal{F}\left(\mathbb{F}_{p^n},\mathbb{F}_{p^n}\right)$ we have that: $\left(\frac{{}_c\partial_a}{1-c}\right)^{(\sigma)}(\zeta) = \left(\underbrace{\frac{{}_c\partial_a}{1-c} \circ \cdots \circ \frac{{}_c\partial_a}{1-c}}_{(\sigma \text{ times})}\right)(\zeta) = \sum_{\theta=0}^{\sigma} \frac{(-c)^\theta \binom{\sigma}{\theta}}{(1-c)^\sigma} \zeta((\sigma-\theta)a + \mathtt{id}_{\mathbb{F}_{p^n}})$. Next, we obtain the version of this equation corresponding to $\sigma+1$.

$\left(\frac{{}_c\partial_a}{1-c}\right)^{(\sigma+1)}(\zeta) = \left(\frac{{}_c\partial_a}{1-c} \circ \left(\frac{{}_c\partial_a}{1-c}\right)^{(\sigma)}\right)(\zeta) = \sum_{\theta=0}^{\sigma} \frac{(-c)^\theta \binom{\sigma}{\theta}}{(1-c)^\sigma} \frac{{}_c\partial_a}{1-c}\left(\zeta((\sigma-\theta)a + \mathtt{id}_{\mathbb{F}_{p^n}})\right) =$
$\frac{\zeta(\mathtt{id}_{\mathbb{F}_{p^n}} + (\sigma+1)a)}{(1-c)^{\sigma+1}} + \left(\sum_{\theta=1}^{\sigma} \frac{(-c)^\theta \binom{\sigma}{\theta}}{(1-c)^{\sigma+1}} \zeta(\mathtt{id}_{\mathbb{F}_{p^n}} + (\sigma+1-\theta)a) + \sum_{\theta_2=0}^{\sigma-1} \frac{(-c)^{\theta_2+1}\binom{\sigma}{\theta_2}}{(1-c)^{\sigma+1}} \zeta(\mathtt{id}_{\mathbb{F}_{p^n}} + (\sigma-\theta_2)a)\right) + \frac{\zeta(\mathtt{id}_{\mathbb{F}_{p^n}})(-c)^{\sigma+1}}{(1-c)^{\sigma+1}} = \frac{\zeta(\mathtt{id}_{\mathbb{F}_{p^n}} + (\sigma+1)a) + \zeta(\mathtt{id}_{\mathbb{F}_{p^n}})(-c)^{\sigma+1}}{(1-c)^{\sigma+1}} + \sum_{\theta=1}^{\sigma} \frac{(-c)^\theta \left(\binom{\sigma}{\theta} + \binom{\sigma}{\theta-1}\right)}{(1-c)^{\sigma+1}} \zeta(\mathtt{id}_{\mathbb{F}_{p^n}}$
$+(\sigma+1-\theta)a) = \sum_{\theta=0}^{\sigma+1} \frac{(-c)^\theta \binom{\sigma+1}{\theta}}{(1-c)^{\sigma+1}} \zeta((\sigma+1-\theta)a + \mathtt{id}_{\mathbb{F}_{p^n}})$. Also, it is not difficult to verify this identity for $\sigma = 1$. Thus the equation is valid for every positive integer σ. In particular, taking $\sigma =$ the field characteristic, it follows that only the first and last term survive. That is, $\left(\frac{{}_c\partial_a}{1-c}\right)^{(\sigma)}(\zeta) = \frac{\zeta(\mathtt{id}_{\mathbb{F}_{p^n}} + 0) + (-c)^p \zeta(\mathtt{id}_{\mathbb{F}_{p^n}})}{(1-c)^p} = \zeta(\mathtt{id}_{\mathbb{F}_{p^n}})$. **Note**: $\mathtt{id}_{\mathbb{F}_{p^n}}$ denotes $\mathtt{id}$ over $\mathbb{F}_{p^n}$. This equation implies FTC. □

Remark. Let us observe that $\Omega(c) = 1-c$ is the only function that makes the operator of form $\frac{{}_c\partial_a}{\Omega(c)}$ satisfy this FTC. It also follows that:

Corollary 9.19 *Let $a \in \mathbb{F}_{p^n}$, $c \in \mathbb{F}_{p^n} \setminus \{1\}$. Then, $\left(\frac{{}_c\partial_a}{1-c}\right)^{(p+1)} = \frac{{}_c\partial_a}{1-c}$.*

In light of Corollary 9.19, the operator $\frac{{}_c\partial_a}{1-c}$ is seen as the $\frac{1}{p+1}$-th derivative (fractional). So we can talk about the $\frac{\ell}{p+1}$-th derivative. **Remark.** It is

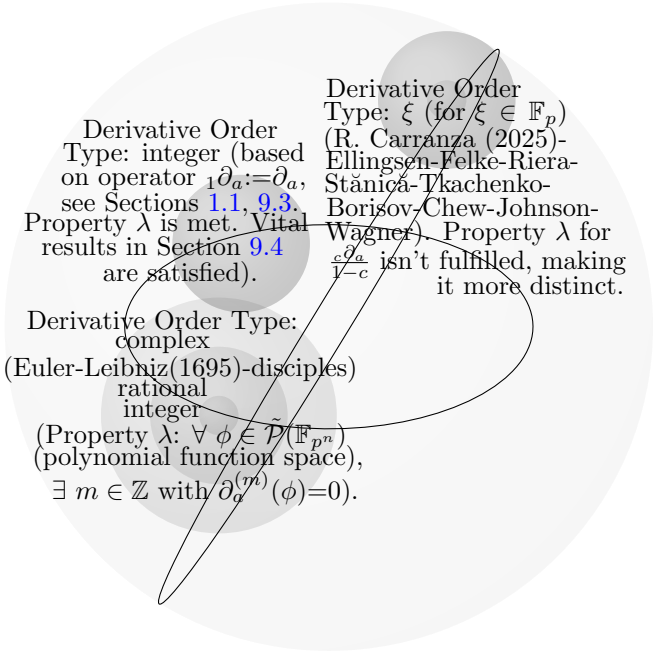

Figure 5: Derivative Order Taxonomy Beyond Fractional Derivatives.

appropriate to refer to this system of derivatives as follows, $\left(\frac{c\partial_a}{1-c}\right)^{(\xi)}$ is the mod (p)-c-derivative of (co-class) order ξ of R. Carranza-Ellingsen-Felke-Riera-Stănică-Tkachenko-Borisov-Chew-Johnson-Wagner, with ξ belonging to the group $\mathbb{Z}_p$, since the following isomorphism is fulfilled (**Eureka!**):

$$\langle \frac{{}_c\partial_a}{1-c} \rangle \cong \mathbb{Z}_p$$

where the operator $\frac{c\partial_a}{1-c}$ is a generator under the composition operation. R. Carranza realizes this magnificent fact, then, now we are aware of this exotic nature of the operators we were dealing with. **Open Problem 23:** will there or will there not be some kind of derivative such that $\xi \in \mathbb{F}_{p^n}$? Does the derivative of order ξ (where $\xi \in \mathbb{F}_{p^n}$, or to a general **Ring**) exist? In general, we have gradually come to understand the derivative order type (integer, rational, real, and complex), which acts on functions $f : S_1 \to S_2$ where $S_1 \bigcup S_2 \subseteq \mathbb{C}$. For our part, we have determined a kind of operator of derivative order type ξ where ξ belongs to field $\mathbb{F}_p$. **Warning** that the scenario established by operator ${}_1\partial_a$ on functions $f : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ has been very different compared to that of mod (p)-c-derivative de R. Carranza-Ellingsen-Felke-Riera-Stănică-Tkachenko-Borisov-Chew-Johnson-Wagner, read Figure 5 and **Remark for** Sec. 9.3.

9.4 An Exotic Chain Complex and an Intriguing Discussion on the Algebra $\mathbb{F}_{p^n}[X_1, ..., X_m]$

Let's get started—deeper—with a powerful result, by exploiting Theorem 9.2.

Theorem 9.20 *(A New Yorker Principle) Let θ be a function from and to $\mathbb{F}_{p^n}$, and $k \geq 1$. Then, $\partial_{X^k}^{(k)}(\theta) = 0$ if and only if $\theta = \partial_{X^{p-k}}^{(p-k)}(\sigma)$, for some σ in the algebra $\mathbb{F}_{p^n}[X]$.*

Proof. As indicated at the beginning of Theorem 9.13, the notable Theorem 9.2 applied to portions with different algebraic degrees in θ, such that $\partial_X^{(1)}(\theta) = 0$, establishes that $\theta = \partial_{X^{p-1}}^{(p-1)}(\sigma)$, for some σ in $\mathbb{F}_{p^n}[X]$. Further, one can follow a procedure analogous to that of Theorem 9.2 by excluding the restriction on $d^0(f)$ corresponding to its protagonist function f, such that if it is fulfilled that $\partial_X^{(1)}(f) = 0$ (where θ is taken as f) with $d^0(f)$ greater than the upper bound $(p-1)(n-1)$, then there exists some σ in $\mathbb{F}_{p^n}[X]$ satisfying $\theta = \partial_{X^{p-1}}^{(p-1)}(\sigma)$ (the case $d^0(f) = 1$ is fundamentally a consequence); while when f is constant, there is no need to talk about the quantity $d^0(f)$ in order to construct a function σ in $\mathbb{F}_{p^n}[X]$ such that f is the $(p-1)$-th derivative of that function. Now let us apply the principle of induction on the (direct) conditional statement, assume that this is true for k, and prove it for $k+1$. We start from $\partial_{X^{k+1}}^{(k+1)}(\theta) = 0$, that is, $\partial_{X^k}^{(k)}\big(\partial_X^{(1)}(\theta)\big) = 0$. By the assumption for k, we have that, $\partial_X^{(1)}(\theta) = \partial_{X^{p-k}}^{(p-k)}(\sigma)$, form some σ in $\mathbb{F}_{p^n}[X]$. Then, $\partial_X^{(1)}\big(\theta - \partial_{X^{p-k-1}}^{(p-k-1)}(\sigma)\big) = 0$. Applying the statement for $k = 1$, we have that $\theta - \partial_{X^{p-k-1}}^{(p-k-1)}(\sigma) = \partial_{X^{p-1}}^{(p-1)}(\bar{\sigma})$, form some $\bar{\sigma}$ in $\mathbb{F}_{p^n}[X]$. That is, $\theta = \partial_{X^{p-k-1}}^{(p-k-1)}(\bar{\bar{\sigma}})$, where $\bar{\bar{\sigma}} = \sigma + \partial_{X^k}^{(k)}(\bar{\sigma})$ belongs to $\mathbb{F}_{p^n}[X]$. The converse statement follows immediately from Theorem 9.14. □

Theorem 9.20 also applies when more than one variable is used. Let $k \geq 1$, we pose the intriguing problem of when one derivative can be converted into another derivative, more precisely, whether there exist functions of several variables, F and G, satisfying $\partial_{X_i}(F) = \partial_{X_j^k}^{(k)}(G)$, such that F does not have the format $\partial_{X_j^k}^{(k)}(\Gamma) + \partial_{X_i^{p-1}}^{(p-1)}(\psi)$ for any pair of functions (Γ, ψ)—note that, when F has that format, the fact $\partial_{X_i}(F) = \partial_{X_j^k}^{(k)}(G)$ becomes obvious—and how large this class of functions can be. More generally, we investigate how much one differential operator, say ∂_{X_i}, can be converted into another, say $\partial_{X_j^k}^{(k)}$. We shall see that over a fairly large function space (for G), $\overline{\mathbb{M}_{p^n,X_j}^{((k),\Xi_k,\cdots,\Xi_{p^n-1})}}[X_1, \cdots, X_m]$, such a conversion is not possible, so in this sense the operators are independent of each other (this independence is measured by the size of $\overline{\mathbb{M}_{p^n,X_j}^{((k),\Xi_k,\cdots,\Xi_{p^n-1})}}[X_1, \cdots, X_m]$; **Open Problem 24:** find another space besides $\overline{\mathbb{M}_{p^n,X_j}^{((k),\Xi_k,\cdots,\Xi_{p^n-1})}}[X_1, \cdots, X_m]$, with a similar role.).

The problem of finding the form of F such that $\partial_{X_i}(F) = \partial^{(k)}_{X_j^k}(G)$ will be answered shortly by our next very sharp theorem. **Remark.** Furthermore, given a function G, for instance, of class as in Theorem 9.21, it can be interpreted that the set of Fs (or that the generic function F) constitutes the integral (indefinite integral with respect to some variable, X_i) of $\partial^{(k)}_{X_j^k}(G)$. For an arbitrary F satisfying the equation $\partial_{X_i}(F) = \partial^{(k)}_{X_j^k}(G)$, it is possible to agree on a slight abuse of the notation, and denote $F = \int \partial^{(k)}_{X_j^k}(G)dX_i$, understanding that, $F \in \int \partial^{(k)}_{X_j^k}(G)dX_i$. In addition, Theorem 9.21 indicates that there is an interchange between the integral operator with respect to X_i and the operator $\partial^{(k)}_{X_j^k}$. Theorem 9.21, for $\beta = 1$, gives us $\int \partial^{(k)}_{X_j^k}(G)dX_i = \partial^{(k)}_{X_j^k}(\Gamma) + \partial^{(p-1)}_{X_i^{p-1}}(\widehat{\Gamma})$; due to the configuration of this formula with the appearance of the part $\partial^{(k)}_{X_j^k}(\Gamma)$ on the right-hand side, we say that: there is an interchange in the weak sense (caused by the necessary presence of the extra function $\partial^{(p-1)}_{X_i^{p-1}}(\widehat{\Gamma})$) between the integral with respect to X_i and the differential operator $\partial^{(k)}_{X_j^k}$.

Theorem 9.21 *(Train or **Centipede Theorem**) Given $m \geq 1$, let F, G be in the multivariate polynomial ring $\mathbb{F}_{p^n}[X_1, \cdots, X_m]$ over the field $\mathbb{F}_{p^n}$, and indices $i, j, k, \beta \geq 1$ (with $j \neq i$), such that $\partial^{(\beta)}_{X_i^\beta}(F) = \partial^{(k)}_{X_j^k}(G)$, while G belongs to the set given below:*

Let Ξ be in $\mathbb{Z}^+$ with $p - 1 \geq \Xi \geq k$, every term of G, except possibly for that of lowest degree, with respect to X_j (i.e. $G_\ell(X_j^*)X_j^\ell$) decomposes such that $d^0(X_j^{\Xi+\ell^{(-)}}) = d^0(X_j^\Xi) + d^0(X_j^{\ell^{(-)}})$, where $\ell^{(-)} := \ell - \Xi$, $G_\ell(X_j^*) \in \mathbb{F}_{p^n}[X_j^*]$, and X_j^* symbolizes the variables list $X_1, \cdots, X_m$, but without the variable X_j. Then:

$$F \in \int \partial^{(k)}_{X_j^k}(G)dX_i^\beta \text{ is given by } F = \partial^{(k)}_{X_j^k}(\Gamma) + \partial^{(p-\beta)}_{X_i^{p-\beta}}(\widehat{\Gamma})$$

for some $(\Gamma, \widehat{\Gamma})$ in $\left(\mathbb{F}_{p^n}[X_1, \cdots, X_m]\right)^2$, where

$\int \partial^{(k)}_{X_j^k}(G)dX_i^\beta := \int \cdots \int \partial^{(k)}_{X_j^k}(G)\, dX_i \ldots dX_i$ (which contains β nested integrals with respect to the single variable X_i).

Proof. Let's define the function $\Lambda_j^{(k)} := \partial^{(k)}_{X_j^k}(G)$. We proceed to decompose G into the form, $G = \sum_{\ell=0}^{p^n-1} G_\ell(X_j^*)X_j^\ell$. Recall that, as $G_0(X_j^*)X_j^0 = G_0(X_j^*)$, an exponent equal to 0 means that the matching indeterminate does not appear in the term. We apply the linear operator $\partial^{(k)}_{X_j^k}$, so $\partial^{(k)}_{X_j^k}(G) = \sum_{\ell=0}^{p^n-1} G_\ell(X_j^*)\partial^{(k)}_{X_j^k}(X_j^\ell)$.

Similarly, we express F as $F = \sum_{\xi=0}^{p^n-1} F_\xi(X_j^*)X_j^\xi$; whose β-th partial derivative with respect to X_i is $\partial_{X_i^\beta}^{(\beta)}(F) = \sum_{\xi=0}^{p^n-1} \partial_{X_i^\beta}^{(\beta)}(F_\xi(X_j^*))X_j^\xi$.

We observe that the $\partial_{X_j^k}^{(k)}(X_j^\ell)$ are linear combinations of the basis vectors X_j^ξ of the $\mathbb{F}_{p^n}$-linear subspace $\mathbb{F}_{p^n}[X_j]$, thanks to the fact that the $\mathbb{F}_{p^n}$-linear subspace relation $\partial_{X_j^k}^{(k)}(\mathbb{F}_{p^n}[X_j]) \leqslant \mathbb{F}_{p^n}[X_j]$ holds. By definition, the kth-order derivative, $G_{\ell_\mu}(X_j^*)\partial_{X_j^k}^{(k)}(X_j^{\ell_\mu})$, contains a term of the form $U^{(k)}(\ell_\mu; H_j)G_{\ell_\mu}(X_j^*)$ $X_j^{\ell_\mu^{(-)}}$, which is not similar to any term in any other $G_{\ell_\varrho}(X_j^*)\partial_{X_j^k}^{(k)}(X_j^{\ell_\varrho})$—the condition on the algebraic degree in the hypothesis is determinative over terms with maximal degrees with respect to X_j in $G_{\ell_\mu}(X_j^*)\partial_{X_j^k}^{(k)}(X_j^{\ell_\mu})$ and $G_{\ell_\varrho}(X_j^*)\partial_{X_j^k}^{(k)}(X_j^{\ell_\varrho})$—for which $\deg_{X_j}(G_{\ell_\varrho}(X_j^*)X_j^{\ell_\varrho}) < \deg_{X_j}(G_{\ell_\mu}(X_j^*)X_j^{\ell_\mu})$, where $U^{(k)}(\ell_\mu; H_j) \neq 0$ denotes a monomial expression for H_j, while $\deg_X$ computes the degree with respect to the (stated) variable X. Hence, $\partial_{X_i^\beta}^{(\beta)}(F_{\ell_\mu^{(-)}}(X_j^*)) = U^{(k)}(\ell_\mu; H_j)G_{\ell_\mu}(X_j^*)$. If we make this choice such that $\deg_{X_j}(G_{\ell_\mu}(X_j^*)X_j^{\ell_\mu}) = \deg_{X_j}(G)$, then $\partial_{X_i^\beta}^{(\beta)}(F) - \frac{1}{U^{(k)}(\ell_\mu;H_j)}\partial_{X_i^\beta}^{(\beta)}(F_{\ell_\mu^{(-)}}(X_j^*))\partial_{X_j^k}^{(k)}(X_j^{\ell_\mu}) = \partial_{X_i^\beta}^{(\beta)}\big(\boxdot_{G,k,X_j}^{(1)}F\big) = \sum_{\ell_\mu \neq \ell=0}^{p^n-1} G_\ell(X_j^*)\partial_{X_j^k}^{(k)}(X_j^\ell)$, where $\boxdot_{G,k,X_j}^{(1)}F = F - \frac{1}{U^{(k)}(\ell_\mu;H_j)}F_{\ell_\mu^{(-)}}(X_j^*)\partial_{X_j^k}^{(k)}(X_j^{\ell_\mu})$; Note that $\partial_{X_j^k}^{(k)}(X_j^{\ell_\mu})$ is also considered a constant function of X_i. We choose $G^{(2)} := \sum_{\ell_\mu \neq \ell=0}^{p^n-1} G_\ell(X_j^*)X_j^\ell$ as our new function G (also, $G^{(1)} := G$), and we repeat the previous procedure over and over again until we have $\partial_{X_i^\beta}^{(\beta)}\big(\boxdot_{G,k,X_j}^{(t_{G,k,X_j})}F\big) = 0$, where t_{G,k,X_j} is the finite number of summands (those non-zeros) of type $G_\ell(X_j^*)\partial_{X_j^k}^{(k)}(X_j^\ell)$ in $\partial_{X_j^k}^{(k)}(G)$; let us denote $G_{\ell_{\mu_1}}(X_j^*)X_j^{\ell_{\mu_1}} = G_{\ell_\mu}(X_j^*)X_j^{\ell_\mu}$, at each step a term of the sequence $G_{\ell_{\mu_1}}(X_j^*)X_j^{\ell_{\mu_1}}$, $G_{\ell_{\mu_2}}(X_j^*)X_j^{\ell_{\mu_2}}, \ldots$ is generated. The powerful Theorem 9.20 applied to the partial differential equation $\partial_{X_i^\beta}^{(\beta)}\big(\boxdot_{G,k,X_j}^{(t_{G,k,X_j})}F\big) = 0$ finally decodes the form of $\boxdot_{G,k,X_j}^{(t_{G,k,X_j})}F$, that is, $\boxdot_{G,k,X_j}^{(t_{G,k,X_j})}F = \partial_{X_i^{p-\beta}}^{(p-\beta)}(\widehat{\Gamma})$ for some $\widehat{\Gamma}$ in $\mathbb{F}_{p^n}[X_1, \cdots, X_m]$. Decoding also the form of F, i.e., $F = \partial_{X_i^{p-\beta}}^{(p-\beta)}(\widehat{\Gamma}) + \sum_{\alpha=1}^{t_{G,k,X_j}} \frac{1}{U^{(k)}(\ell_{\mu_\alpha};H_j)}F_{\ell_{\mu_\alpha}^{(-)}}(X_j^*)\partial_{X_j^k}^{(k)}(X_j^{\ell_{\mu_\alpha}}) = \partial_{X_i^{p-\beta}}^{(p-\beta)}(\widehat{\Gamma}) + \sum_{\alpha=1}^{t_{G,k,X_j}} \partial_{X_j^k}^{(k)}\big(\frac{1}{U^{(k)}(\ell_{\mu_\alpha};H_j)}F_{\ell_{\mu_\alpha}^{(-)}}(X_j^*)X_j^{\ell_{\mu_\alpha}}\big)$. Therefore, $F = \partial_{X_j^k}^{(k)}(\Gamma) + \partial_{X_i^{p-\beta}}^{(p-\beta)}(\widehat{\Gamma})$, for some $(\Gamma, \widehat{\Gamma})$ in $\big(\mathbb{F}_{p^n}[X_1, \cdots, X_m]\big)^2$, $\Gamma = \sum_{\alpha=1}^{t_{G,k,X_j}} \frac{1}{U^{(k)}(\ell_{\mu_\alpha};H_j)}F_{\ell_{\mu_\alpha}^{(-)}}(X_j^*)X_j^{\ell_{\mu_\alpha}}$. Erledigt!. There

is another fundamental fact, since $\Lambda_j^{(k)} = \partial_{X_i^\beta}^{(\beta)}(F)$, we have obtained that for such Γ in $\mathbb{F}_{p^n}[X_1, \cdots, X_m]$ we have that $\Lambda_j^{(k)} = \partial_{X_i^\beta X_j^k}^{(k+\beta)}(\Gamma)$. □

Open Problem 25: Theorem 9.21 should be investigated for other classes of functions G, more precisely, to determine all possible G for which the *partial differential equation* of Theorem 9.21 is solved for F. Moreover, I suggest investigating ***Centipede Theorem*** for the equation with the silhouette $\partial_{X_i^\beta}^{(\beta)}(F) = \partial_{X_j^k}^{(k)}(G) + \partial_{X_{\tilde{j}}^{\tilde{k}}}^{(\tilde{k})}(\widetilde{G})$; we are talking about the conditions on the pair $(G, \widetilde{G})$. Based on the experience acquired with such a wonderful theorem, we define the sets below.

Definition 9.22 *The symbol X_j^* stands for the variables list $X_1, \cdots, X_m$, but without the variable X_j, and be Ξ and k in $\mathbb{Z}^+$ with $p-1 \geq \Xi \geq k$. We define $\overline{\mathbb{M}_{p^n, X_j}^{(k,\Xi)}}[X_1, \cdots, X_m] := \{G \in \mathbb{F}_{p^n}[X_1, \cdots, X_m];$ each term of G with respect to X_j(i.e. $G_\ell(X_j^*)X_j^\ell$) is such that $\ell - \Xi = \ell^{(-)}$ and $d^0(X_j^{\Xi+\ell^{(-)}}) = d^0(X_j^\Xi) + d^0(X_j^{\ell^{(-)}})$, where $G_\ell(X_j^*) \in \mathbb{F}_{p^n}[X_j^*]\}$.*

Theorem 9.23 can handle important problems that Theorem 9.21 cannot, and is obtained by slightly modifying the demonstration of Theorem 9.21; let's summarize how to obtain it. Throughout the proof, we replace the operator $\partial_{X_{j_1}\cdots X_{j_{r-1}}}^{(r-1)}$ by the operator ∂_{X_i}, when $\beta = 1$, we stop at the equation $\partial_{X_{j_1}\cdots X_{j_{r-1}}}^{(r-1)}(F_{\ell_\mu^{(-)}}(X_{j_r}^*)) = U^{(k)}(\ell_\mu; H_{j_r})G_{\ell_\mu}(X_{j_r}^*)$, more precisely, we obtain the following sequence of identities, $\partial_{X_{j_1}\cdots X_{j_{r-1}}}^{(r-1)}(F_{\ell_{\mu_1}^{(-)}}(X_{j_r}^*)) = U^{(k)}(\ell_{\mu_1}; H_{j_r})G_{\ell_{\mu_1}}($ $X_{j_r}^*)$, $\partial_{X_{j_1}\cdots X_{j_{r-1}}}^{(r-1)}\left(\left(\boxdot_{G,k,X_j}^{(1)}F\right)_{\ell_{\mu_2}^{(-)}}(X_{j_r}^*)\right) = U^{(k)}(\ell_{\mu_2}; H_{j_r})G_{\ell_{\mu_2}}(X_{j_r}^*), \ldots, \partial_{X_{j_1}\cdots X_{j_{r-1}}}^{(r-1)}$ $\left(\left(\boxdot_{G,k,X_j}^{(t_{G,k,X_j}-1)}F\right)_{\ell_{\mu_{t_{G,k,X_j}}}^{(-)}}(X_{j_r}^*)\right) = U^{(k)}(\ell_{\mu_{t_{G,k,X_j}}}; H_{j_r})G_{\ell_{\mu_{t_{G,k,X_j}}}}(X_{j_r}^*)$; from which we rewrite $\partial_{X_{j_r}^k}^{(k)}(G)$, i.e. the sum $\sum_{s=1}^{t_{G,k,X_{j_r}}} G_{\ell_{\mu_s}}(X_{j_r}^*)\partial_{X_{j_r}^k}^{(k)}(X_{j_r}^{\ell_{\mu_s}})$, which takes the form $\Lambda_{j_r}^{(k)} = \partial_{X_{j_1}\cdots X_{j_{r-1}}X_{j_r}^k}^{(k+r-1)}(\varphi)$, for some φ in $\mathbb{F}_{p^n}[X_1, \cdots, X_m]$. Travail accompli!

Theorem 9.23 *Let $m, r-1 \geq 1$, let the algebra $\mathbb{F}_{p^n}[X_1, \cdots, X_m]$ in m variables, of which, let $X_{j_1}, \cdots, X_{j_{r-1}}$, and X_{j_r}, be r variables (different from each other, of course). Let F be in the algebra $\mathbb{F}_{p^n}[X_1, \cdots, X_m]$ and $k \geq 1$, such that $\partial_{X_{j_1}\cdots X_{j_{r-1}}}^{(r-1)}(F) = \partial_{X_{j_r}^k}^{(k)}(G)$, where G belongs to the set $\overline{\mathbb{M}_{p^n, X_{j_r}}^{(k,\Xi)}}[X_1, \cdots, X_m]$. Let $\Lambda_{j_r}^{(k)} := \partial_{X_{j_r}^k}^{(k)}(G)$. Then $\exists\ \Gamma$ in $\mathbb{F}_{p^n}[X_1, \cdots, X_m]$ such that the following fundamental fact holds, $\Lambda_{j_r}^{(k)} = \partial_{X_{j_1}\cdots X_{j_{r-1}}X_{j_r}^k}^{(k+r-1)}(\Gamma)$.*

Definition 9.24 *The symbol X_j^* denotes the variables list $X_1, \cdots, X_m$, but without the variable X_j, let k in $\mathbb{Z}^+$, and let $\Xi_k, \cdots, \Xi_{p^n-1}$ be p^n-k elements in $\mathbb{Z}_0^+$ bounded by $p-1 \geq \max_{p^n-1\geq\lambda\geq k} d^0(X_j^{\Xi_\lambda}) \geq \min_{p^n-1\geq\lambda\geq k} d^0(X_j^{\Xi_\lambda}) \geq k$. We define $\overline{\mathbb{M}_{p^n,X_j}^{((k),\Xi_k,\cdots,\Xi_{p^n-1})}}[X_1,\cdots,X_m] := \{G \in \mathbb{F}_{p^n}[X_1,\cdots,X_m];$ if two terms $G_{\ell_1}(X_j^*)X_j^{\ell_1}$ and $G_{\ell_2}(X_j^*)X_j^{\ell_2}$, of G expressed with respect to X_j, satisfy that $d^0(X_j^{\ell_1}) = d^0(X_j^{\ell_2}) = \lambda$ (some) in $\mathbb{Z}^+$, then $d^0(X_j^{\Xi_\lambda+\ell_z^{(-)}}) = d^0(X_j^{\Xi_\lambda}) + d^0(X_j^{\ell_z^{(-)}})$ and $\ell_z - \Xi_\lambda = \ell_z^{(-)}$. Moreover, $\Xi_\lambda = \Xi_\lambda(p)$ viewed as a polynomial in $\mathbb{Z}[P]$ with coefficients in $[0, p-1]$ followed by an evaluation at $P = p$ is such that, $\ell_z^{(-)} = p^{\deg_P(\Xi_\lambda)}\Theta_{\lambda,\ell_z}$, where $\Theta_{\lambda,\ell_z} = \Theta_{\lambda,\ell_z}(p) \in \mathbb{Z}_0^+, G_{\ell_z}(X_j^*) \in \mathbb{F}_{p^n}[X_j^*]$, and $z \in \{1,2\}\}$.*

The identity $\Lambda_{j_r}^{(k)} = \partial^{(k+r-1)}_{X_{j_1}\cdots X_{j_{r-1}}X_{j_r}^k}(\Gamma)$ ensures smoothness gain, i.e., differentiability of a higher class; which in turn is obtained as a sum (not, for example, a product) of the participating differentiability classes. $\overline{\mathbb{M}_{p^n,X_j}^{((k),\Xi_k,\cdots,\Xi_{p^n-1})}}[X_1,\cdots,X_m]$ has a vector space structure over $\mathbb{F}_{p^n}$, $\overline{\mathbb{M}_{p^n,X_j}^{(k,\Xi)}}[X_1,\cdots,X_m]$ is a special case of $\overline{\mathbb{M}_{p^n,X_j}^{((k),\Xi_k,\cdots,\Xi_{p^n-1})}}[X_1,\cdots,X_m]$.

Theorem 9.25 *Theorems 9.21 and 9.23 also hold for G belonging to $\overline{\mathbb{M}_{p^n,X_j}^{((k),\Xi_k,\cdots,\Xi_{p^n-1})}}[X_1,\cdots,X_m]$.*

Theorem 9.26 *Let $m, r-2 \geq 1$, consider the algebra $\mathbb{F}_{p^n}[X_1,\cdots,X_m]$ in m variables, of these, let $X_{j_1},\cdots,X_{j_{r-1}}$, and X_{j_r} be r variables, it is understood that they are different from each other. Let $\Xi_1,\cdots,\Xi_{p^n-1}$, $\breve{\Xi}_{p-1},\cdots,\breve{\Xi}_{p^n-1}$ be in $\mathbb{Z}_0^+$ bounded so that the pair $\left(d^0(X_{j_{r-2}}^{\Xi_\lambda}), d^0(X_{j_r}^{\breve{\Xi}_{\breve{\lambda}}})\right)$ belongs to the segment $[1,p-1]\times\{p-1\}$ as long as $(\lambda,\breve{\lambda})$ is in the rectangle $[1,p^n-1]\times[p-1,p^n-1]$. Let $F \in \overline{\mathbb{M}_{p^n,X_{j_{r-2}}}^{((1),\Xi_1,\cdots,\Xi_{p^n-1})}}[X_1,\cdots,X_m]$ such that $\partial^{(2)}_{X_{j_{r-2}}X_{j_{r-1}}}(F) = \partial^{(p-1)}_{X_{j_r}^{p-1}}(\mathcal{Q}_r)$ for some $\mathcal{Q}_r \in \overline{\mathbb{M}_{p^n,X_{j_r}}^{((p-1),\breve{\Xi}_{p-1},\cdots,\breve{\Xi}_{p^n-1})}}[X_1,\cdots,X_m]$. Furthermore, let $\partial^{(p-1)}_{X_{j_r}^{p-1}}(\varphi_r)$ in $\overline{\mathbb{M}_{p^n,X_{j_{r-2}}}^{((1),\Xi_1,\cdots,\Xi_{p^n-1})}}[X_1,\cdots,X_m]$ be a function with one of its second order derivatives given by $\partial^{(p-1)}_{X_{j_r}^{p-1}}(\mathcal{Q}_r) = \partial^{(2)}_{X_{j_{r-2}}X_{j_{r-1}}}\left(\partial^{(p-1)}_{X_{j_r}^{p-1}}(\varphi_r)\right)$. Then: $\partial^{(3)}_{X_{j_{r-2}}X_{j_{r-1}}X_{j_r}}(F) = 0$ if and only if $F = \sum_{\ell=r-2}^{r}\partial^{(p-1)}_{X_{j_\ell}^{p-1}}(\Gamma_\ell)$, for some $(\Gamma_{r-2},\Gamma_{r-1},\Gamma_r)$ in $\left(\mathbb{F}_{p^n}[X_1,\cdots,X_m]\right)^3$.*

Proof. The converse conditional statement is easy to obtain. Let us demonstrate the direct conditional statement. Given $\partial^{(1)}_{X_{j_r}}(\partial^{(2)}_{X_{j_{r-2}}X_{j_{r-1}}}(F)) = 0$, Theorem 9.20 is responsible for $\partial^{(1)}_{X_{j_{r-1}}}(\partial^{(1)}_{X_{j_{r-2}}}(F)) = \partial^{(p-1)}_{X_{j_r}^{p-1}}(\mathcal{Q}_r)$, for some $\mathcal{Q}_r$, by hy-

pothesis one can locate some $\mathcal{Q}_r$ precisely in $\overline{\mathbb{M}_{p^n,X_{j_r}}^{((p-1),\breve{\Xi}_{p-1},\cdots,\breve{\Xi}_{p^n-1})}}[X_1,\cdots,X_m]$; let $\Lambda_{j_r}^{(p-1)} := \partial_{X_{j_r}^{p-1}}^{(p-1)}(\mathcal{Q}_r)$. Theorem 9.23, version for G (which in this case is $\mathcal{Q}_r$) belonging to $\overline{\mathbb{M}_{p^n,X_{j_r}}^{((p-1),\breve{\Xi}_{p-1},\cdots,\breve{\Xi}_{p^n-1})}}[X_1,\cdots,X_m]$, states that $\Lambda_{j_r}^{(p-1)} = \partial_{X_{j_{r-2}}X_{j_{r-1}}X_{j_r}^{p-1}}^{(p+1)}(\varphi_r)$ for some φ_r in $\mathbb{F}_{p^n}[X_1,\cdots,X_m]$, capturing important information about the equation $\partial_{X_{j_{r-2}}X_{j_{r-1}}}^{(2)}(F) = \partial_{X_{j_r}^{p-1}}^{(p-1)}(\mathcal{Q}_r)$; by hypothesis we shall consider such $\partial_{X_{j_r}^{p-1}}^{(p-1)}(\varphi_r)$ in $\overline{\mathbb{M}_{p^n,X_{j_{r-2}}}^{((1),\Xi_1,\cdots,\Xi_{p^n-1})}}[X_1,\cdots,X_m]$. Thus, the properties of associativity and commutativity between differential operators allow us to conveniently rewrite in an equation with the format, $\partial_{X_{j_{r-1}}}^{(1)}(\beta) = 0$ with β in $\mathbb{F}_{p^n}[X_1,\cdots,X_m]$, Theorem 9.20 tells us that there exists $\widehat{\mathfrak{F}}_{r-1}$ in $\mathbb{F}_{p^n}[X_1,\cdots,X_m]$ such that, $\partial_{X_{j_{r-2}}}^{(1)}(F) = \partial_{X_{j_r}^{p-1}X_{j_{r-2}}}^{(p)}(\varphi_r) + \partial_{X_{j_{r-1}}^{p-1}}^{(p-1)}\big(\widehat{\mathfrak{F}}_{r-1}\big) = \partial_{X_{j_r}^{p-1}X_{j_{r-2}}}^{(p)}(\varphi_r) + \partial_{X_{j_{r-1}}^{p-1}X_{j_{r-2}}}^{(p)}\big(\check{\widehat{\mathfrak{F}}}_{r-1}\big)$. To obtain the summand $\partial_{X_{j_{r-1}}^{p-1}X_{j_{r-2}}}^{(p)}\big(\check{\widehat{\mathfrak{F}}}_{r-1}\big)$ we have followed the following algorithm, by hypothesis $F \in \overline{\mathbb{M}_{p^n,X_{j_{r-2}}}^{((1),\Xi_1,\cdots,\Xi_{p^n-1})}}[X_1,\cdots,X_m]$, also $\partial_{X_{j_r}^{p-1}}^{(p-1)}(\varphi_r) \in \overline{\mathbb{M}_{p^n,X_{j_{r-2}}}^{((1),\Xi_1,\cdots,\Xi_{p^n-1})}}[X_1,\cdots,X_m]$, then the combination $F - \partial_{X_{j_r}^{p-1}}^{(p-1)}(\varphi_r)$ belongs to the $\mathbb{F}_{p^n}$-vector space $\overline{\mathbb{M}_{p^n,X_{j_{r-2}}}^{((1),\Xi_1,\cdots,\Xi_{p^n-1})}}[X_1,\cdots,X_m]$. Then, Theorem 9.21 in its version for G (which in this case is $F - \partial_{X_{j_r}^{p-1}}^{(p-1)}(\varphi_r)$) in $\overline{\mathbb{M}_{p^n,X_{j_{r-2}}}^{((1),\Xi_1,\cdots,\Xi_{p^n-1})}}[X_1,\cdots,X_m]$, applied to the equation $\partial_{X_{j_{r-1}}^{p-1}}^{(p-1)}\big(\widehat{\mathfrak{F}}_{r-1}\big) = \partial_{X_{j_{r-2}}}^{(1)}\big(F - \partial_{X_{j_r}^{p-1}}^{(p-1)}(\varphi_r)\big)$ reveals that $\widehat{\mathfrak{F}}_{r-1}$ has the form $\partial_{X_{j_{r-2}}}^{(1)}\big(\check{\widehat{\mathfrak{F}}}_{r-1}\big)$, inferring that, $\partial_{X_{j_{r-1}}^{p-1}}^{(p-1)}\big(\widehat{\mathfrak{F}}_{r-1}\big)$ is of the form $\partial_{X_{j_{r-1}}^{p-1}X_{j_{r-2}}}^{(p)}\big(\check{\widehat{\mathfrak{F}}}_{r-1}\big)$, for some $\check{\widehat{\mathfrak{F}}}_{r-1}$ in $\mathbb{F}_{p^n}[X_1,\cdots,X_m]$. Then now we can separate the equation $\partial_{X_{j_{r-2}}}^{(1)}(F) = \partial_{X_{j_r}^{p-1}X_{j_{r-2}}}^{(p)}(\varphi_r) + \partial_{X_{j_{r-1}}^{p-1}}^{(p-1)}\big(\widehat{\mathfrak{F}}_{r-1}\big)$, as, $\partial_{X_{j_{r-2}}}^{(1)}(\Phi_1) = \partial_{X_{j_r}^{p-1}X_{j_{r-2}}}^{(p)}(\varphi_r)$ and $\partial_{X_{j_{r-2}}}^{(1)}(\Phi_2) = \partial_{X_{j_{r-1}}^{p-1}X_{j_{r-2}}}^{(p)}\big(\check{\widehat{\mathfrak{F}}}_{r-1}\big)$, with $F = \Phi_1 + \Phi_2$. Then, it is enough to apply Theorem 9.20 in each of these last two equations to arrive at that, $\Phi_1 = \partial_{X_{j_r}^{p-1}}^{(p-1)}(\varphi_r) + \partial_{X_{j_{r-2}}^{p-1}}^{(p-1)}\big(\widehat{\varkappa}_{r-2}\big)$ and $\Phi_2 = \partial_{X_{j_{r-1}}^{p-1}}^{(p-1)}\big(\check{\widehat{\mathfrak{F}}}_{r-1}\big) + \partial_{X_{j_{r-2}}^{p-1}}^{(p-1)}\big(\widehat{\pi}_{r-2}\big)$. We recover F as, $F = \partial_{X_{j_r}^{p-1}}^{(p-1)}(\varphi_r) + \partial_{X_{j_{r-2}}^{p-1}}^{(p-1)}\big(\widehat{\varkappa}_{r-2} + \widehat{\pi}_{r-2}\big) + \partial_{X_{j_{r-1}}^{p-1}}^{(p-1)}\big(\check{\widehat{\mathfrak{F}}}_{r-1}\big)$, for some $(\Gamma_{r-2},\Gamma_{r-1},\Gamma_r)$ in $\big(\mathbb{F}_{p^n}[X_1,\cdots,X_m]\big)^3$, where $\Gamma_{r-2} = \varphi_r$, $\Gamma_{r-1} = \widehat{\varkappa}_{r-2} + \widehat{\pi}_{r-2}$, and $\Gamma_r = \check{\widehat{\mathfrak{F}}}_{r-1}$. □

Open Problem 26: generalize Theorem 9.21 so that it covers *partial differential equations* of the form $\partial_{X_i^\beta}^{(\beta)}(F) = \partial_{X_{j_1}\cdots X_{j_{r-2}}X_{j_{r-1}}^k}^{(r+k-2)}(G)$. **Open Problem 27:** investigate whether Theorem 9.26 holds for $F \in \mathbb{F}_{p^n}[X_1,\cdots,X_m]$ as arbi-

trary as possible (it would be a great achievement), while $m \geq 2$; for $m = 1$ it holds without restrictions. For such a goal, do not rule out the construction of specially molded bases for $\mathbb{F}_{p^n}[X_1, \cdots, X_m]$ and for its derived linear spaces; we perceive that this might require a maximal state of mind.

Theorem 9.27 *Let us denote the variables list $X_1, \cdots, X_m$ by the symbol $\overline{X}_{1:m}$. Considering Theorem 9.26, let us consider differential operators, being restrictions of $\partial^{(3)}_{X_{j_{r-2}}X_{j_{r-1}}X_{j_r}}$ and $\partial^{(p-1)}_{X^{p-1}_{j_\ell}}$ respectively, of the following form,* $\widehat{\partial^{(3)}}_{X_{j_{r-2}}X_{j_{r-1}}X_{j_r}} : \partial^{(-3)}_{X^{(-1)}_{j_{r-2}}X^{(-1)}_{j_{r-1}}X^{(-1)}_{j_r}}\Big(\partial^{(1)}_{X_{j_{r-1}}}\Big(\overline{\mathbb{M}^{((1),\Xi_1,\cdots,\Xi_{p^n-1})}_{p^n,X_{j_{r-1}}}}[\overline{X}_{1:m}]\Big)\Big) \bigcap \partial^{(-3)}_{X^{(-1)}_{j_{r-2}}X^{(-1)}_{j_{r-1}}X^{(-1)}_{j_r}}\Big(\partial^{(1)}_{X_{j_r}}\Big(\overline{\mathbb{M}^{((1),\breve{\Xi}_1,\cdots,\breve{\Xi}_{p^n-1})}_{p^n,X_{j_r}}}[\overline{X}_{1:m}]\Big)\Big) \longrightarrow \partial^{(1)}_{X_{j_{r-1}}}\Big(\overline{\mathbb{M}^{((1),\Xi_1,\cdots,\Xi_{p^n-1})}_{p^n,X_{j_{r-1}}}}[\overline{X}_{1:m}]\Big) \bigcap \partial^{(1)}_{X_{j_r}}\Big(\overline{\mathbb{M}^{((1),\breve{\Xi}_1,\cdots,\breve{\Xi}_{p^n-1})}_{p^n,X_{j_r}}}[\overline{X}_{1:m}]\Big)$ *and* $\widehat{\partial^{(p-1)}_{X^{p-1}_{j_\ell}}} : \partial^{(1)}_{X_{j_{r-1}}}\Big(\overline{\mathbb{M}^{((1),\Xi_1,\cdots,\Xi_{p^n-1})}_{p^n,X_{j_{r-1}}}}[\overline{X}_{1:m}]\Big) \bigcap \partial^{(1)}_{X_{j_r}}\Big(\overline{\mathbb{M}^{((1),\breve{\Xi}_1,\cdots,\breve{\Xi}_{p^n-1})}_{p^n,X_{j_r}}}[\overline{X}_{1:m}]\Big) \longrightarrow \partial^{(1)}_{X_{j_{r-1}}}\Big(\overline{\mathbb{M}^{((1),\Xi_1,\cdots,\Xi_{p^n-1})}_{p^n,X_{j_{r-1}}}}[\overline{X}_{1:m}]\Big) \bigcap \partial^{(1)}_{X_{j_r}}\Big(\overline{\mathbb{M}^{((1),\breve{\Xi}_1,\cdots,\breve{\Xi}_{p^n-1})}_{p^n,X_{j_r}}}[\overline{X}_{1:m}]\Big)$, *where $\partial^{(-1)}_{X^{(-1)}_{j_{r-1}}}$ is used to denote the inverse image of a set under the differential operator $\partial^{(1)}_{X_{j_{r-1}}}$, similarly $\partial^{(-3)}_{X^{(-1)}_{j_{r-2}}X^{(-1)}_{j_{r-1}}X^{(-1)}_{j_r}}$ is used to denote the inverse image of a set under $\partial^{(3)}_{X_{j_{r-2}}X_{j_{r-1}}X_{j_r}}$. Then we get an equality,* $Im\big(\widehat{\partial^{(3)}}_{X_{j_{r-2}}X_{j_{r-1}}X_{j_r}}\big) = \bigcap_{\ell=r-2}^{r} \ker\big(\widehat{\partial^{(p-1)}_{X^{p-1}_{j_\ell}}}\big)$.

In addition, the vector subspace relation shown in the chain below holds: $\partial^{(2)}_{X_{j_{r-2}}X_{j_{r-1}}}\Big(\overline{\mathbb{M}^{((1),\breve{\Xi}_1,\cdots,\breve{\Xi}_{p^n-1})}_{p^n,X_{j_r}}}[\overline{X}_{1:m}]\Big) \leqslant \overline{\mathbb{M}^{((1),\breve{\Xi}_1,\cdots,\breve{\Xi}_{p^n-1})}_{p^n,X_{j_r}}}[\overline{X}_{1:m}] \leqslant \partial^{(-2)}_{X^{(-1)}_{j_{r-2}}X^{(-1)}_{j_{r-1}}}\Big(\overline{\mathbb{M}^{((1),\breve{\Xi}_1,\cdots,\breve{\Xi}_{p^n-1})}_{p^n,X_{j_r}}}[\overline{X}_{1:m}]\Big) \leqslant \partial^{(-3)}_{X^{(-1)}_{j_{r-2}}X^{(-1)}_{j_{r-1}}X^{(-1)}_{j_r}}\Big(\partial^{(1)}_{X_{j_r}}\Big(\overline{\mathbb{M}^{((1),\breve{\Xi}_1,\cdots,\breve{\Xi}_{p^n-1})}_{p^n,X_{j_r}}}[\overline{X}_{1:m}]\Big)\Big)$.

Proof. It is not difficult to see that the operators in play are well defined; in passing, let us notice that, the operator $\partial^{(2)}_{X_{j_{r-2}}X_{j_{r-1}}}$—which is mainly constituent of $\widehat{\partial^{(3)}}_{X_{j_{r-2}}X_{j_{r-1}}X_{j_r}}$—respects the following inclusion, $\partial^{(2)}_{X_{j_{r-2}}X_{j_{r-1}}}\Big(\overline{\mathbb{M}^{((1),\breve{\Xi}_1,\cdots,\breve{\Xi}_{p^n-1})}_{p^n,X_{j_r}}}[\overline{X}_{1:m}]\Big) \subseteq \overline{\mathbb{M}^{((1),\breve{\Xi}_1,\cdots,\breve{\Xi}_{p^n-1})}_{p^n,X_{j_r}}}[\overline{X}_{1:m}]$, this is because if we represent an element f of $\overline{\mathbb{M}^{((1),\breve{\Xi}_1,\cdots,\breve{\Xi}_{p^n-1})}_{p^n,X_{j_r}}}[\overline{X}_{1:m}]$ as a polynomial in the variable X_{j_r}, we can see that the operator $\partial^{(2)}_{X_{j_{r-2}}X_{j_{r-1}}}$ will only transform the coefficients of f, being able to cancel some coefficients, and the terms linked to them, which does not affect the membership relationship between $\partial^{(2)}_{X_{j_{r-2}}X_{j_{r-1}}}(f)$ and $\overline{\mathbb{M}^{((1),\breve{\Xi}_1,\cdots,\breve{\Xi}_{p^n-1})}_{p^n,X_{j_r}}}[\overline{X}_{1:m}]$. Obtaining the first vector subspace relation in the chain of spaces, $\partial^{(2)}_{X_{j_{r-2}}X_{j_{r-1}}}\Big(\overline{\mathbb{M}^{((1),\breve{\Xi}_1,\cdots,\breve{\Xi}_{p^n-1})}_{p^n,X_{j_r}}}[\overline{X}_{1:m}]\Big) \leqslant \overline{\mathbb{M}^{((1),\breve{\Xi}_1,\cdots,\breve{\Xi}_{p^n-1})}_{p^n,X_{j_r}}}[\overline{X}_{1:m}]$. From applying a function followed by taking the inverse image of such function, we see that, $\overline{\mathbb{M}^{((1),\breve{\Xi}_1,\cdots,\breve{\Xi}_{p^n-1})}_{p^n,X_{j_r}}}[\overline{X}_{1:m}] \subseteq \partial^{(-1)}_{X^{(-1)}_{j_r}}\Big(\partial^{(1)}_{X_{j_r}}\Big(\overline{\mathbb{M}^{((1),\breve{\Xi}_1,\cdots,\breve{\Xi}_{p^n-1})}_{p^n,X_{j_r}}}[\overline{X}_{1:m}]\Big)\Big)$; then,

to this inclusion we apply $\partial^{(-2)}_{X^{(-1)}_{j_{r-2}}X^{(-1)}_{j_{r-1}}}$, then $\partial^{(-2)}_{X^{(-1)}_{j_{r-2}}X^{(-1)}_{j_{r-1}}}\left(\overline{\mathbb{M}^{((1),\breve{\Xi}_1,\cdots,\breve{\Xi}_{p^n-1})}_{p^n,X_{j_r}}}[\overline{X}_{1:m}]\right)$ $\subseteq$ $\partial^{(-3)}_{X^{(-1)}_{j_{r-2}}X^{(-1)}_{j_{r-1}}X^{(-1)}_{j_r}}\left(\partial^{(1)}_{X_{j_r}}\left(\overline{\mathbb{M}^{((1),\breve{\Xi}_1,\cdots,\breve{\Xi}_{p^n-1})}_{p^n,X_{j_r}}}[\overline{X}_{1:m}]\right)\right)$, due to three things, (1). That the inverse image behaves as an increasing function with respect to the inclusion relation, (2). Applying the inverse image formula of a composition of transformations that are not necessarily invertible, and (3). Commutativity of the composition between these differential operators. We know the first inclusion in the chain, $\partial^{(2)}_{X_{j_{r-2}}X_{j_{r-1}}}\left(\overline{\mathbb{M}^{((1),\breve{\Xi}_1,\cdots,\breve{\Xi}_{p^n-1})}_{p^n,X_{j_r}}}[\overline{X}_{1:m}]\right) \subseteq \overline{\mathbb{M}^{((1),\breve{\Xi}_1,\cdots,\breve{\Xi}_{p^n-1})}_{p^n,X_{j_r}}}[\overline{X}_{1:m}]$; applying $\partial^{(-2)}_{X^{(-1)}_{j_{r-2}}X^{(-1)}_{j_{r-1}}}$ leads us to $\partial^{(-2)}_{X^{(-1)}_{j_{r-2}}X^{(-1)}_{j_{r-1}}}\left(\partial^{(2)}_{X_{j_{r-2}}X_{j_{r-1}}}\left(\overline{\mathbb{M}^{((1),\breve{\Xi}_1,\cdots,\breve{\Xi}_{p^n-1})}_{p^n,X_{j_r}}}[\overline{X}_{1:m}]\right)\right) \subseteq \partial^{(-2)}_{X^{(-1)}_{j_{r-2}}X^{(-1)}_{j_{r-1}}}\left(\overline{\mathbb{M}^{((1),\breve{\Xi}_1,\cdots,\breve{\Xi}_{p^n-1})}_{p^n,X_{j_r}}}[\overline{X}_{1:m}]\right)$, but as before, we observe that $\overline{\mathbb{M}^{((1),\breve{\Xi}_1,\cdots,\breve{\Xi}_{p^n-1})}_{p^n,X_{j_r}}}[\overline{X}_{1:m}] \subseteq \partial^{(-2)}_{X^{(-1)}_{j_{r-2}}X^{(-1)}_{j_{r-1}}}\left(\partial^{(2)}_{X_{j_{r-2}}X_{j_{r-1}}}\left(\overline{\mathbb{M}^{((1),\breve{\Xi}_1,\cdots,\breve{\Xi}_{p^n-1})}_{p^n,X_{j_r}}}[\overline{X}_{1:m}]\right)\right)$, since we have applied the linear operator $\partial^{(2)}_{X_{j_{r-2}}X_{j_{r-1}}}$ and then its inverse image. Therefore, by transitivity, $\overline{\mathbb{M}^{((1),\breve{\Xi}_1,\cdots,\breve{\Xi}_{p^n-1})}_{p^n,X_{j_r}}}[\overline{X}_{1:m}] \leqslant \partial^{(-2)}_{X^{(-1)}_{j_{r-2}}X^{(-1)}_{j_{r-1}}}\left(\overline{\mathbb{M}^{((1),\breve{\Xi}_1,\cdots,\breve{\Xi}_{p^n-1})}_{p^n,X_{j_r}}}[\overline{X}_{1:m}]\right)$.

The inclusion $\mathrm{Im}\big(\widehat{\partial^{(3)}}_{X_{j_{r-2}}X_{j_{r-1}}X_{j_r}}\big) \subseteq \bigcap_{\ell=r-2}^{r} \ker\big(\widehat{\partial^{(p-1)}_{X^{p-1}_{j_\ell}}}\big)$ is simple to verify, where the properties of associativity and commutativity between differential operators with respect to the composition operation are also exploited. We will now focus on complementary inclusion. Given $f \in \bigcap_{\ell=r-2}^{r} \ker\big(\widehat{\partial^{(p-1)}_{X^{p-1}_{j_\ell}}}\big)$, by Theorem 9.20 we infer that $\forall\, r \geq \ell \geq r-2$, $\exists\, \sigma_\ell$ in some subspace of $\mathbb{F}_{p^n}[X_1,\cdots,X_m]$ such that $f = \partial^{(1)}_{X_{j_\ell}}(\sigma_\ell)$. Since $f = \partial^{(1)}_{X_{j_{r-2}}}(\sigma_{r-2}) = \partial^{(1)}_{X_{j_{r-1}}}(\sigma_{r-1})$, for some $\sigma_{r-1} \in \overline{\mathbb{M}^{((1),\Xi_1,\cdots,\Xi_{p^n-1})}_{p^n,X_{j_{r-1}}}}[\overline{X}_{1:m}]$, Theorem 9.25 implies that $\exists\ \widehat{\sigma_{r-1}}$ in $\mathbb{F}_{p^n}[X_1,\cdots,X_m]$ such that $\sigma_{r-2} = \partial^{(1)}_{X_{j_{r-1}}}(\widehat{\sigma_{r-1}})$; then $f = \partial^{(1)}_{X_{j_{r-2}}}(\partial^{(1)}_{X_{j_{r-1}}}(\widehat{\sigma_{r-1}})) = \partial^{(1)}_{X_{j_r}}(\sigma_r)$, for some $\sigma_r \in \overline{\mathbb{M}^{((1),\breve{\Xi}_1,\cdots,\breve{\Xi}_{p^n-1})}_{p^n,X_{j_r}}}[\overline{X}_{1:m}]$. Using Theorem 9.25 on this last equation we infer that $\exists\ \breve{\Omega}$ in $\mathbb{F}_{p^n}[X_1,\cdots,X_m]$ such that $f = \partial^{(3)}_{X_{j_{r-2}}X_{j_{r-1}}X_{j_r}}(\breve{\Omega})$; adding the fact that f is in $\partial^{(1)}_{X_{j_{r-1}}}\left(\overline{\mathbb{M}^{((1),\Xi_1,\cdots,\Xi_{p^n-1})}_{p^n,X_{j_{r-1}}}}[\overline{X}_{1:m}]\right) \bigcap \partial^{(1)}_{X_{j_r}}\left(\overline{\mathbb{M}^{((1),\breve{\Xi}_1,\cdots,\breve{\Xi}_{p^n-1})}_{p^n,X_{j_r}}}[\overline{X}_{1:m}]\right)$, we obtain $f \in \mathrm{Im}\big(\widehat{\partial^{(3)}}_{X_{j_{r-2}}X_{j_{r-1}}X_{j_r}}\big)$. □

Theorem 9.28 *Let $m, r \geq 1$. Consider the restrictions of $\partial^{(r)}_{X_{j_1}\cdots X_{j_r}}$ and*

$\partial^{(p-1)}_{X^{p-1}_{j_\ell}}$ *arranged in the following sequence of differential operators,*

$$\mathbb{F}_{p^n}[X_1,\cdots,X_m] \overset{\partial^{(r)}_{X_{j_1}\cdots X_{j_r}}}{\longrightarrow} \partial^{(r)}_{X_{j_1}\cdots X_{j_r}}\left(\mathbb{F}_{p^n}[X_1,\cdots,X_m]\right) \overset{\widetilde{\partial^{(p-1)}_{X^{p-1}_{j_\ell}}}}{\longrightarrow} \widetilde{\mathcal{D}_{p^n}}$$

where $\widetilde{\mathcal{D}_{p^n}} \leqslant \mathbb{F}_{p^n}[X_1,\cdots,X_m]$ *is an arbitrary* $\mathbb{F}_{p^n}$*-vector subspace. Then,* $Im\left(\partial^{(r)}_{X_{j_1}\cdots X_{j_r}}\right) = \bigcap_{\ell=1}^{r} \ker\left(\widetilde{\partial^{(p-1)}_{X^{p-1}_{j_\ell}}}\right)$.

Proof. With the experience of Theorem 9.27, we simply apply the useful Theorem 9.20. □

We are glad that θ in Theorem 9.20 (fact derived from the powerful Theorem 9.2) has the form it does; this introduces a new symmetry property, a new idea of symmetry over the space of differential operators, such that in a pair, $\left(\partial^{(p-k)}_{X^{p-k}}, \partial^{(k)}_{X^k}\right)$, one component can be said to be p-co-differential of the other.

Definition 9.29 *Let* p *be a prime number, let* $n, m \geq 1$, *and* $m \geq i \geq 1$. *Due to the product differentiation rule and the Theorem 9.14 it follows that, given* $\breve{\zeta}$ *and* ζ *in* $\mathbb{F}_{p^n}[X_1,\cdots,X_m]$, *and* $\gamma \geq 1$, *then* $\partial^{(p-1)}_{X_i^{p-1}}(\zeta)\partial^{(\gamma)}_{X_i^{\gamma}}(\breve{\zeta}) = \partial_{X_i}\left(\partial^{(p-1)}_{X_i^{p-1}}(\zeta)\partial^{(\gamma-1)}_{X_i^{\gamma-1}}(\breve{\zeta})\right) = \cdots = \partial^{(\gamma)}_{X_i^{\gamma}}\left(\partial^{(p-1)}_{X_i^{p-1}}(\zeta)\breve{\zeta}\right) = \partial^{(\gamma)}_{X_i^{\gamma}}(\mathfrak{y})$ *belongs to* $\partial^{(\gamma)}_{X_i^{\gamma}}\left(\mathbb{F}_{p^n}[X_1,\cdots,X_m]\right)$, *where* $\mathfrak{y} = \partial^{(p-1)}_{X_i^{p-1}}(\zeta)\breve{\zeta}$ *is in* $\mathbb{F}_{p^n}[X_1,\cdots,X_m]$. *From this fact it follows that* $\partial^{(p-1)}_{X_i^{p-1}}\left(\mathbb{F}_{p^n}[X_1,\cdots,X_m]\right)\partial^{(\gamma)}_{X_i^{\gamma}}\left(\mathbb{F}_{p^n}[X_1,\cdots,X_m]\right) \subseteq \partial^{(\gamma)}_{X_i^{\gamma}}\left(\mathbb{F}_{p^n}[X_1,\cdots,X_m]\right)$, *in particular, taking* $p-\gamma=1$ *the* $\mathbb{F}_{p^n}$*-vector space* $\partial^{(p-1)}_{X_i^{p-1}}\left(\mathbb{F}_{p^n}[X_1,\cdots,X_m]\right)$ *is closed with respect to multiplication. The subalgebra of* $\mathbb{F}_{p^n}[X_1,\cdots,X_m]$ *over the field* $\mathbb{F}_{p^n}$ *given by* $\partial^{(p-1)}_{X_i^{p-1}}\left(\mathbb{F}_{p^n}[X_1,\cdots,X_m]\right)$ *will be called R. Carranza-Galois Algebra (type 1). In a similar fashion, the subalgebra of* $\mathbb{F}_{p^n}[X_1,\cdots,X_m] \mod (X_1^{p^n}-X_1,\ldots,X_m^{p^n}-X_m)$ *over the field* $\mathbb{F}_{p^n}$, $\partial^{(p-1)}_{X_i^{p-1}}\left(\mathbb{F}_{p^n}[X_1,\cdots,X_m] \mod (X_1^{p^n}-X_1,\ldots,X_m^{p^n}-X_m)\right)$, *will also be appointed as R. Carranza-Galois Algebra (type 2). One of the applications of this stellar algebraic structure, intrinsic to* $\mathbb{F}_{p^n}$, *lies at the heart of the time-dependent Schrödinger equation on* $\mathbb{F}_{p^n}[X,T]$, *serving for the construction of abundant wave functions from a single one.*

Theorem 9.30 *Theorems 9.14, 9.16, and 9.20 also hold if:*

1). $\mathbb{F}_{p^n}[X_1,\ldots,X_m]$ *is substituted by* $\mathbb{F}_{p^n}[X_1,\ldots,X_m] \mod (X_1^{p^n}-X_1,\ldots,X_m^{p^n}-X_m)$,

2). F *and* G *are considered in* $\mathbb{F}_{p^n}[X] \mod (X^{p^n}-X)$,

3). θ *belong to the algebra* $\mathbb{F}_{p^n}[X]$. *Similarly, it happens to the other results throughout this Section.*

Proof. We will demonstrate item (3), the other two are done in a similar enough way. Let us consider ξ in $\mathbb{F}_{p^n}[X]$ having $\deg(\xi) \geq p^n$ and $\partial_a(\xi) = 0$, where $a \in \mathbb{F}_{p^n}^*$. In the Integral Domain $\mathbb{F}_{p^n}[X]$, we have $X^{p^n} - X \in \mathbb{F}_{p^n}^*[X]$. Further, $\mathbb{F}_{p^n}[X]$ is a Euclidean Domain, so ξ takes the following form, $\xi(X) = \lambda(X)(X^{p^n} - X) + \mathfrak{S}(X)$, where $\mathfrak{S}(X) = 0$ or $\deg(\mathfrak{S}(X)) < p^n$. The product rule (Theorem 9.16) combined with the facts $\partial_a(X^{p^n} - X) = 0$ and that ∂_a is linear implies $\partial_a(\xi) = (X^{p^n} - X)\partial_a(\lambda(X)) + \partial_a(\mathfrak{S}(X))$. Therefore, $-\partial_a(\mathfrak{S}(X)) = (X^{p^n} - X)\partial_a(\lambda(X))$. Let us separate this into two cases. **Case** $\partial_a(\lambda) \neq 0$**:** $\deg((X^{p^n} - X)\partial_a(\lambda(X))) = \deg(X^{p^n} - X) + \deg(\partial_a(\lambda(X))) \geq \deg(X^{p^n} - X) = p^n$ and $\deg(-\partial_a(\mathfrak{S}(X))) \leq \deg(\mathfrak{S}(X)) - 1 \leq p^n - 2$, this case leads to the contradiction $p^n - 2 \geq \deg(-\partial_a(\mathfrak{S}(X))) \geq p^n$, if $-\partial_a(\mathfrak{S}) \neq 0$. On the contrary, if $-\partial_a(\mathfrak{S}) = 0$, then the facts $(\partial_a(\lambda(X)), X^{p^n} - X) \in (\mathbb{F}_{p^n}^*[X])^2$ and $(X^{p^n} - X)\partial_a(\lambda(X)) = 0$ (independent of the indeterminate) cannot coexist under the integral domain $\mathbb{F}_{p^n}[X]$. Consequently, only case $\partial_a(\lambda) = 0$ can occur; a fact that will be applied systematically in what follows. **Case** $\partial_a(\lambda) = 0$**:** hence $\partial_a(\xi) = \partial_a(\mathfrak{S}(X)) = 0$. Applying Theorem 9.20 to $\mathfrak{S}$ we have, $\mathfrak{S} = \partial_{a^{p-1}}^{(p-1)}(\sigma)$, for some σ in the algebra $\mathbb{F}_{p^n}[X]$. Note that $\lambda \neq 0$; the contrary assumption is trivial. Two subcases are presented. **Sub-case** $\deg(\lambda(X)) < p^n$**:** Theorem 9.20 applied to λ implies $\lambda = \partial_{a^{p-1}}^{(p-1)}(\hat{\sigma})$, where $\hat{\sigma}$ is in $\mathbb{F}_{p^n}[X]$. Theorem 9.16 implies, $\xi(X) = (X^{p^n} - X)\partial_{a^{p-1}}^{(p-1)}(\hat{\sigma}(X)) + \partial_{a^{p-1}}^{(p-1)}(\sigma(X)) = \partial_{a^{p-1}}^{(p-1)}(\mathfrak{Z}(X))$, where $\mathfrak{Z} = (X^{p^n} - X)\hat{\sigma} + \sigma$ belongs to $\mathbb{F}_{p^n}[X]$. **Sub-case** $\deg(\lambda(X)) \geq p^n$**:** let us apply to λ the preceding algorithm that has been applied so far to ξ. By applying to λ the division algorithm with divisor $X^{p^n} - X$, a new quotient is obtained, which we label λ_2. Furthermore, $\lambda_2 \neq 0$, since otherwise we fall into the already solved case $\deg(\lambda(X)) < p^n$. Again, two subcases are presented, $\deg(\lambda_2(X)) < p^n$ and $\deg(\lambda_2(X)) \geq p^n$, only now $\deg(\lambda_2(X)) = \deg(\lambda(X)) - p^n$. If the worst case were to occur, we obtain a sequence $(\lambda_\ell(X))_{\ell=2}^{L}$ such that $\lambda_{\ell-1}(X) = \lambda_\ell(X)(X^{p^n} - X) + \mathfrak{S}_\ell(X)$, $\partial_a(\lambda_{\ell-1}) = 0$, $\partial_a(\lambda_L) = 0$, $\lambda_1 = \lambda$, $\deg(\mathfrak{S}_\ell) < p^n$ or $\mathfrak{S}_\ell = 0$, and $\deg(\lambda_L(X)) < p^n$, for some integer L. Theorems 9.16 and 9.20 imply, $\lambda_{L-1}(X) = \partial_{a^{p-1}}^{(p-1)}(\mathfrak{Z}_{L-1}(X))$ for some $\mathfrak{Z}_{L-1}$ in $\mathbb{F}_{p^n}[X]$. Differentiating $\lambda_{L-2}(X) = \lambda_{L-1}(X)(X^{p^n} - X) + \mathfrak{S}_{L-1}(X)$, we have, $\partial_a(\mathfrak{S}_{L-1}(X)) = 0$. Theorem 9.20 implies, $\mathfrak{S}_{L-1}(X) = \partial_{a^{p-1}}^{(p-1)}(\widehat{\mathfrak{S}}_{L-1})$, for some $\widehat{\mathfrak{S}}_{L-1}$ in the algebra $\mathbb{F}_{p^n}[X]$. Then, $\lambda_{L-2}(X) = (X^{p^n} - X)\partial_{a^{p-1}}^{(p-1)}(\mathfrak{Z}_{L-1}) + \partial_{a^{p-1}}^{(p-1)}(\widehat{\mathfrak{S}}_{L-1})$. Again, by Theorem 9.16, $\lambda_{L-2}(X) \in \partial_{a^{p-1}}^{(p-1)}(\mathfrak{Z}_{L-2}(X))$, where $\mathfrak{Z}_{L-2} = (X^{p^n} - X)\mathfrak{Z}_{L-1} + \widehat{\mathfrak{S}}_{L-1}$ belongs to $\mathbb{F}_{p^n}[X]$. In this way we can also get $\lambda_{L-3}(X) \in \partial_{a^{p-1}}^{(p-1)}(\mathfrak{Z}_{L-3}(X))$ for some $\mathfrak{Z}_{L-3}$ in $\mathbb{F}_{p^n}[X]$, and continue until $\lambda = \partial_{a^{p-1}}^{(p-1)}(\mathfrak{Z}_1)$ for some $\mathfrak{Z}_1$ in $\mathbb{F}_{p^n}[X]$. Using this expression of λ and Theorem 9.16, we obtain that, $\xi = \partial_{a^{p-1}}^{(p-1)}(\mathfrak{G})$, for some $\mathfrak{G}$ in $\mathbb{F}_{p^n}[X]$. Complementarily, if $\xi = \partial_{a^{p-1}}^{(p-1)}(\mathfrak{G})$ for some $\mathfrak{G}$ in $\mathbb{F}_{p^n}[X]$, then, Theorem 9.14 reveals that

$\partial_a(\xi) = 0$. This result can be easily generalized to a derivation order greater than 1. It follows that, Theorem 9.20 is also applicable if we only consider θ in the algebra $\mathbb{F}_{p^n}[X]$. □

Following the notation of Theorem 9.14, the following sequences—which are exact, and will be termed *R. Carranza-Galois Exact Sequences*—of a class of $\mathbb{F}_{p^n}$-linear mappings (chosen as the derivatives, according to Definition I, of order r) between $\mathbb{F}_{p^n}$-vector spaces are established:

$$\begin{array}{ccccccc}
\mathbb{F}_{p^n}[X_1,\cdots,X_m] & \xrightarrow{\partial^{(p)}_{X_j^p}} & \mathbb{F}_{p^n}[X_1,\cdots,X_m] & \xrightarrow{\partial^{(0)}_{X_j^0}} & \mathbb{F}_{p^n}[X_1,\cdots,X_m] & \xrightarrow{\partial^{(p)}_{X_j^p}} & \mathbb{F}_{p^n}[X_1,\cdots,X_m] \\
\mathbb{F}_{p^n}[X_1,\cdots,X_m] & \xrightarrow{\partial^{(p-r)}_{X_j^{p-r}}} & \mathbb{F}_{p^n}[X_1,\cdots,X_m] & \xrightarrow{\partial^{(r)}_{X_j^r}} & \mathbb{F}_{p^n}[X_1,\cdots,X_m] & \xrightarrow{\partial^{(p-r)}_{X_j^{p-r}}} & \mathbb{F}_{p^n}[X_1,\cdots,X_m] \\
\mathbb{F}_{p^n}[X_1,\cdots,X_m] & \xrightarrow{\partial^{(0)}_{X_i^0}} & \mathbb{F}_{p^n}[X_1,\cdots,X_m] & \xrightarrow{\partial^{(p)}_{X_i^p}} & \mathbb{F}_{p^n}[X_1,\cdots,X_m] & \xrightarrow{\partial^{(0)}_{X_i^0}} & \mathbb{F}_{p^n}[X_1,\cdots,X_m]
\end{array}$$

Figure 6: R. Carranza-Galois Exact Sequences.

We obtain the following sequence—similar to an exact one, which will be termed *R. Carranza-Galois Atomic Sequence*—of $\mathbb{F}_{p^n}$-linear mappings (chosen as the derivatives, according to Definition I, of orders 3 and $p-1$): see **Fig. 7**; due to Theorem 9.27 the equality $\mathrm{Im}\big(\widehat{\partial^{(3)}}_{X_{j_{r-2}}X_{j_{r-1}}X_{j_r}}\big) = \bigcap_{\ell=r-2}^{r} \ker\big(\widehat{\partial^{(p-1)}_{X_{j_\ell}^{p-1}}}\big)$ takes place.

Regarding the sequence of $\mathbb{F}_{p^n}$-modules, together with $\mathbb{F}_{p^n}$-module homomorphisms of the following type

$$\mathbf{C}_\bullet := \left(\mathbb{F}_{p^n}[X_1,\cdots,X_m] \xrightarrow{\partial^{(p-\sigma_\mu)}_{X_{j_\mu}^{p-\sigma_\mu}}} \mathbb{F}_{p^n}[X_1,\cdots,X_m] \xrightarrow{\partial^{(\sum_{\ell=1}^r \sigma_\ell)}_{X_{j_1}^{\sigma_1}\cdots X_{j_r}^{\sigma_r}}} \mathbb{F}_{p^n}[X_1,\cdots,X_m] \xrightarrow{\partial^{(p-\sigma_\nu)}_{X_{j_\nu}^{p-\sigma_\nu}}} \mathbb{F}_{p^n}[X_1,\cdots,X_m]\right)$$

where $1 \leq \mu,\nu \leq r$, so that X_{j_μ} and X_{j_ν} belong to the set of variables $X_{j_1}\cdots X_{j_r}$; $H_2(\mathbf{C}_\bullet) = \ker\big(\partial^{(\sum_{\ell=1}^r \sigma_\ell)}_{X_{j_1}^{\sigma_1}\cdots X_{j_r}^{\sigma_r}}\big)/\mathrm{Im}\big(\partial^{(p-\sigma_\mu)}_{X_{j_\mu}^{p-\sigma_\mu}}\big)$ and $H_1(\mathbf{C}_\bullet) = \ker\big(\partial^{(p-\sigma_\nu)}_{X_{j_\nu}^{p-\sigma_\nu}}\big)$ $/\mathrm{Im}\big(\partial^{(\sum_{\ell=1}^r \sigma_\ell)}_{X_{j_1}^{\sigma_1}\cdots X_{j_r}^{\sigma_r}}\big)$ are the 2-th and 1-th homology modules of the chain complex $\mathbf{C}_\bullet$, which measure their deviation from being an exact sequence. *Where*: each derivative operator ∂_{X_i} runs along H_i; $1 \leq \sigma_\ell$, $1 \leq \ell \leq r$, $\sum_{\ell=1}^r \sigma_\ell < p$; $\partial^{(0)}_{X_i^0}$ (acting as the identity function) represents the zeroth derivative with respect to the variable X_i. It is an excellent idea to apply machinery used in Homological Algebra and see what else can be obtained.

The field structure on the Galois ring $\mathbb{F}_{p^n}$ does not accept a total order,

Fig.7 *R.Carranza− Galois Atomic Sequence.*

Verifying the following properties:

$$\sum_{\ell=1}^{r} \operatorname{Im}\big(\partial^{\widetilde{(p-1)}}_{X^{p-1}_{j_\ell}}\big) \subseteq \ker\big(\widehat{\partial^{(3)}}_{X_{j_{r-2}}X_{j_{r-1}}X_{j_r}}\big)$$

$$\operatorname{Im}\big(\widehat{\partial^{(3)}}_{X_{j_{r-2}}X_{j_{r-1}}X_{j_r}}\big) = \bigcap_{\ell=r-2}^{r} \ker\big(\widehat{\partial^{(p-1)}_{X^{p-1}_{j_\ell}}}\big).$$

moreover, it never admits a non-trivial partial order $\preceq$ [4] [5] compatible with the field structure. Since the complex field $\mathbb{C}$ is partially ordered, the investigation on $\mathbb{F}_{p^n}$ complements it in order to obtain a general overview that can cover both fields, $\mathbb{C}$ and $\mathbb{F}_{p^n}$, turning this finite structure (but for infinite pairs (p, n)) into a unique-unparalleled underlying scenario. We abstract in the exploration of the solution of which we shall call $\mathbb{F}_{p^n}$-*Schrödinger-type equation* (abbreviated to $\mathbb{F}_{p^n}$-*Schrödinger equation*), this mathematical model describes the relationship between the derivatives (refer to Subsection 1.1) of the involved functions defined on $\mathbb{F}_{p^n}$—the wave function Ψ and the potential energy function V (remember that the derivatives of V do not usually participate)—its form is given by the equations in Theorem 9.32. As for classical and current references about the conventional Schrödinger equation, we recommend [102, 132, 69, 118, 19, 2, 83, 141] Hermann Weyl, *the theory of groups and quantum mechanics*. In quantum theory, to identify the state of a quantum system we use $\Psi : \mathbb{R}^2 \to \mathbb{C}$ usually assumed in a Hilbert space (being the continuous case, it has basic characteristics to ensure existence, such as: every Cauchy sequence converges), we know that $\mathbb{R} \leqslant \mathbb{C}$; in the perspective we are exploring it corresponds to use $\Psi : \left(\mathbb{F}_{p^n}\right)^2 \to \mathbb{F}_{p^n}$ belonging to its corresponding space of functions. In this mathematical model, μ refers to the reduced Planck's constant $\hbar$ and the mass m, considering them divided by their respective physical units, dimensionless; since, in general $-\frac{\hbar^2}{2m}$ belongs to $\mathbb{R}$, the constant μ is taken in $\mathbb{F}_{p^n}$. In this setting, taking advantage of the preceding machinery, especially Theorem 9.14 and Corollary 9.15, we investigate how rare the new wave function Ψ can be; we summarize these implications shortly.

Definition 9.31 *Let $r \geq 1$, $f : \left(\mathbb{F}_{p^n}\right)^r \to \mathbb{F}_{p^n}$ be a function in the variables $X_1, \ldots, X_r$, and let $(H_1, \ldots, H_r) \in \left(\mathbb{F}^*_{p^n}\right)^r$ be a vector. The r-th derivative (derivative of order r) of f denoted by $\partial^{(r)}_{X_1=H_1,\ldots,X_r=H_r}(f)$, is obtained by applying to f the first order derivative with respect to the variable X_1 in the direction H_1 (see subsection 1.1), followed by the first order derivative with*

[4] *Partial order*: when for an arbitrary pair $(\mathfrak{a}, \mathfrak{b})$ of elements of the set it is not required that $\mathfrak{a}$ is comparable with $\mathfrak{b}$. It is understood that $\mathfrak{a}$ *is comparable* with $\mathfrak{b}$ when at least one of the inequalities is ensured: $\mathfrak{a} \preceq \mathfrak{b}$ or $\mathfrak{b} \preceq \mathfrak{a}$.

[5] ($\preceq$ trivial: $\mathfrak{a} \preceq \mathfrak{b}$ if and only if $\mathfrak{a} = \mathfrak{b}$, where every element of the set is maximal (also minimal))

respect to the variable X_2 in the direction H_2, continuing until the r variables are exhausted. As long as there is no ambiguity, we are free to use the compact notation $\partial^{(r)}_{X_1 \ldots X_r}(f)$. In this, the independent variables can be equal.

Theorem 9.32 (Schrödinger Equation on $\mathcal{F}\big(\big(\mathbb{F}_{p^n}\big)^2, \mathbb{F}_{p^n}\big)$, for the first time for functions whose co-domain is strictly the Galois Field). *Let n be a positive integer, let γ, μ be non-zero constants in the field $\mathbb{F}_{p^n}$, and $(H, \bar{H}) \in \big(\mathbb{F}^*_{p^n}\big)^2$. Let us consider the time-dependent $\mathbb{F}_{p^n}$-Schrödinger equation on the space of functions $\mathcal{F}\big(\big(\mathbb{F}_{p^n}\big)^2, \mathbb{F}_{p^n}\big)$ with coefficients γ, μ, given by:*

$$\mathcal{H}_{\mathbb{F}_{p^n}} f(X,T) = \gamma \partial_{T=\bar{H}}(f(X,T))$$

With the following ingredients: a1). $\mathcal{H}_{\mathbb{F}_{p^n}}$ is called the $\mathbb{F}_{p^n}$-Hamiltonian of the system; we consider systems that behave according to the $\mathbb{F}_{p^n}$-Hamiltonian $\mathcal{H}_{\mathbb{F}_{p^n}} := -\mu\nabla^2 + V$, a2). $\nabla^2(f) := \partial^{(2)}_{X=H, X=H}(f)$, a3). $V \in \mathcal{F}\big(\big(\mathbb{F}_{p^n}\big)^2, \mathbb{F}_{p^n}\big)$ is called the potential energy of the particle, and a4). Ψ, called wavefunction, denotes a function that satisfies the posed equation. In cases where the set $\mathcal{V}_V[X,T] := \{f \in \mathcal{F}\big(\big(\mathbb{F}_{p^n}\big)^2, \mathbb{F}_{p^n}\big); -\mu\nabla^2\big(f\big) + V(X,T)f = \gamma\partial_{T=\bar{H}}(f)\}$ is non-empty, it has a vector space structure. Let $\mathcal{V}_V[X,T] \neq \varnothing$ with $\Psi \in \mathcal{V}_V[X,T]$, for some $\Psi \in \mathcal{F}\big(\big(\mathbb{F}_{p^n}\big)^2, \mathbb{F}_{p^n}\big)$, then we determine subspaces of solutions to the $\mathbb{F}_{p^n}$-Schrödinger equation, also regions consisting of non-solutions, as follows:

1i). $\Psi\mathbb{F}_{p^n} \subseteq \mathcal{V}_V[X,T]$.

2i). $\big(\Psi + \mathbb{F}^*_{p^n}\big)\bigcap \mathcal{V}_V[X,T] = \varnothing$, if $V \neq 0$.

3i). The following vector subspace relation on $\mathbb{F}_{p^n}$ holds:

$\big(\partial^{(p-1)}_{\substack{X=H,\ldots,X=H \\ (p-1 \text{ times})}}(\mathbb{F}_{p^n}[X] \mod (X^{p^n} - X)) + \partial^{(p-1)}_{\substack{T=\bar{H},\ldots,T=\bar{H} \\ (p-1 \text{ times})}}(\mathbb{F}_{p^n}[T] \mod (T^{p^n} - T))\big)\Psi \leqslant \mathcal{V}_V[X,T]$.

3.1i). In particular, for even-characteristic fields:

$\big(\partial_{X=H}(\mathbb{F}_{2^n}[X] \mod (X^{p^n} - X)) + \partial_{T=\bar{H}}(\mathbb{F}_{2^n}[T] \mod (T^{p^n} - T))\big)\Psi \leqslant \mathcal{V}_V[X,T]$.

4i). If $\Gamma(X,T)$ in $\mathcal{F}\big(\big(\mathbb{F}_{p^n}\big)^2, \mathbb{F}_{p^n}\big)$ is such that $\partial_{T=\bar{H}}(\Gamma)$ is a nonzero function, $\deg_X(\Gamma) \leq p^n - \deg_X(\Psi) - 1$ (respectively, $\deg_X\big(\partial_{T=\bar{H}}\big(\Gamma(X,T)\big)\big) \leq p^n - \deg_X(\Psi(X,T)) - 1$), and $\deg_X(\partial_{T=\bar{H}}(\Gamma)) \geq \deg_X(\Gamma) - 1$ (this condition occurs in a large class of functions $\Gamma(X,T)$) (respectively, $\deg_X\big(\partial_{T=\bar{H}}\big(\Gamma(X,T)\big)\big) \geq \deg_X\big(\partial_{X=H}\big(\Gamma(X,T)\big)\big)$), then $\Gamma(X,T)\Psi \notin \mathcal{V}_\Psi[X,T]$. Note that an arbitrary function $\Phi \in \mathcal{F}\big(\big(\mathbb{F}_{p^n}\big)^2, \mathbb{F}_{p^n}\big)$ can be identified as an element of the algebra $\mathbb{F}_{p^n}[X,T] \mod (X^{p^n} - X, T^{p^n} - T)$.

Proof. $\mathcal{V}_V[X,T]$ is a vector space (it can be verified via the characterization for a subspace). The part $(1i)$ is sufficiently visible. $2i)$. It can be immediately seen that a translation $\Psi + k$ belongs to the set $\mathcal{V}_V[X,T]$, for k in $\mathbb{F}^*_{p^n}$, if and only if $kV = 0$, that is, $V = 0$, which is not possible due to the hypothesis $V \neq 0$. $3i)$. Given $\zeta(T) \in \mathcal{F}\big(\mathbb{F}_{p^n}, \mathbb{F}_{p^n}\big)$ with $\partial_{T=\bar{H}}\big(\zeta(T)\big) = 0 \ \forall \ T \in \mathbb{F}_{p^n}$, then

$\zeta(T)\Psi \in \mathcal{V}_V[X,T]$; note that it becomes necessary to indicate on which variable the function ζ depends, so we can use $\zeta(T)$ and ζ without distinction, keeping in mind that $\zeta(T)$ usually means the value of such a function at T. Similarly, $A(X)\Psi \in \mathcal{V}_V[X,T]$ for any $A(X) \in \mathcal{F}\big(\mathbb{F}_{p^n},\mathbb{F}_{p^n}\big)$ such that $\partial_{X=H}\big(A(X)\big)= 0$ $\forall\ X \in \mathbb{F}_{p^n}$. The space $\mathcal{F}\Big(\big(\mathbb{F}_{p^n}\big)^2,\mathbb{F}_{p^n}\Big)$ can be represented as the bivariate algebra $\mathbb{F}_{p^n}[X,T] \mod (X^{p^n}-X) \mod (T^{p^n}-T)$ over $\mathbb{F}_{p^n}$, by means of Lagrange interpolation. By applying Theorem 9.20—which also applies when more than one variable is involved—we construct the set, closed with respect to addition and multiplication by scalars, $\Psi\partial^{(p-1)}_{X=H,\ldots,X=H}(\mathbb{F}_{p^n}[X] \mod (X^{p^n}-X)) + \Psi\partial^{(p-1)}_{T=\bar{H},\ldots,T=\bar{H}}(\mathbb{F}_{p^n}[T] \mod (T^{p^n}-T))(\leqslant \mathcal{V}_V[X,T])$; obtaining that the elements defined as a dilation of Ψ in space plus a dilation of Ψ in time form a subspace of the solution vector space $\mathcal{V}_V[X,T]$, such dilations are delimited by an *Algebra of R. Carranza-Galois*. 4*i*). After replacing $\Gamma(X,T)\Psi$ and applying the product rule, Theorem 9.16 (which also adapts to several variables), in $\mathbb{F}_{p^n}$-*Schrödinger equation*, this is reduced to $-\gamma\partial_{T=\bar{H}}(\Gamma(X,T))\Psi(X,T+\bar{H}) = \mu\nabla^2\big(\Gamma(X,T)\big)\Psi(X+2H,T)+2\mu\partial_{X=H}(\Gamma(X,T))\partial_{X=H}(\Psi(X+H,T))$. We have the fact that the function $-\gamma\partial_{T=\bar{H}}(\Gamma(X,T))\Psi(X,T+\bar{H})$ can be represented in $\mathbb{F}_{p^n}[T][X] \mod (T^{p^n}-T, X^{p^n}-X)$, and that similarly to the algebraic degree it is observed that $\deg_X(\partial_{X=H}(\varkappa(X,T))) \leq \deg_X(\varkappa(X,T))-1$ for $\varkappa$ in $\mathbb{F}_{p^n}[T][X] \mod (T^{p^n}-T, X^{p^n}-X)$, combining these facts we have that: $\deg_X(-\gamma\partial_{T=\bar{H}}(\Gamma(X,T))\Psi(X,T+\bar{H})) = \deg_X(\partial_{T=\bar{H}}(\Gamma)) + \deg_X(\Psi(X,T+\bar{H})) > \max\big\{\deg_X(\Gamma)-2+\deg_X(\Psi),\ \deg_X(\partial_{X=H}(\Gamma))+\deg_X(\Psi)-1\big\} \geq \max\big\{\deg_X\big(\mu\nabla^2\big(\Gamma(X,T)\big)\Psi(X+2H,T)\big),\ \deg_X\big(2\mu\partial_{X=H}(\Gamma(X,T))\partial_{X=H}(\Psi(X+H,T))\big)\big\} \geq \deg_X\big(\mu\nabla^2\big(\Gamma(X,T)\big)\Psi(X+2H,T) + 2\mu\partial_{X=H}(\Gamma(X,T))\partial_{X=H}(\Psi(X+H,T))\big)$; in case that for example $2\mu\partial_{X=H}(\Gamma)\partial_{X=H}(\Psi(X+H,T))$ is function 0, we only use the degrees of part $\mu\nabla^2\big(\Gamma(X,T)\big)\Psi(X+2H,T)$, also by hypothesis both parts cannot vanish at the same time, neither their sum; under the hypothesis that $\deg_X(\Gamma) \leq p^n-\deg_X(\Psi)-1$ the quantity $\deg_X(-\gamma\partial_{T=\bar{H}}(\Gamma(X,T))\Psi(X,T+\bar{H}))$ is bounded; similarly it is carried out for the more general conditions $\deg_X\big(\partial_{T=\bar{H}}\big(\Gamma(X,T)\big)\big) \leq p^n-\deg_X(\Psi(X,T))-1$ and $\deg_X\big(\partial_{T=\bar{H}}\big(\Gamma(X,T)\big)\big) \geq \deg_X\big(\partial_{X=H}\big(\Gamma(X,T)\big)\big)$. Then we have a contradiction with the functions on both sides of the equation $-\gamma\partial_{T=\bar{H}}(\Gamma(X,T))\Psi(X,T+\bar{H}) = \mu\nabla^2\big(\Gamma(X,T)\big)\Psi(X+2H,T)+2\mu\partial_{X=H}(\Gamma(X,T))\partial_{X=H}(\Psi(X+H,T))$ being equal, concluding that such Γ cannot exist. □

The wave function in the $\mathbb{F}_{p^n}$-*Schrödinger equation* bears several similarities as well as some marked differences to the continuous case in *Quantum Mechanics*, as can be seen in Theorem 9.32. Much more can be done regarding the investigation of the *Schrödinger equation* for the universe $\mathbb{F}_{p^n}$. **Open Problem 28.** Generalize the Theorem 9.32 for the *Schrödinger equation* on $\mathcal{F}\Big(\big(\overline{\mathbb{F}_{p^n}}\big)^2,\overline{\mathbb{F}_{p^n}}\Big)$, where $\overline{\mathbb{F}_{p^n}}$ is the algebraic closure of $\mathbb{F}_{p^n}$.

In the geometric Brownian motion outlook, the *Black-Scholes equation*

$$0 = \partial_t(V) + \frac{\sigma^2}{2} S^2 \partial^{(2)}_{S^2}(V) + rS\partial_S(V) - rV$$

(where $V = V(S,t)$ is the value of the option as a function of stock price $S \geq 0$ and time $t \in [0,T]$, while σ is the volatility (σ^2: the variance rate of the return on the stock), and r is the risk-free interest rate) is a type of parabolic PDE (since its associated matrix $M = \begin{pmatrix} 0 & 0 \\ 0 & \frac{\sigma^2}{2} S^2 \end{pmatrix}$ satisfies $\det(M) = 0$) which through a change of variables it can be transformed into the *diffusion heat-transfer equation*

$$\partial_{\bar{t}}(U) = c_{\sigma,r} \partial^{(2)}_{\bar{S}^2}(U)$$

where $c_{\sigma,r}$ (the thermal constant of the material) belongs to $\mathbb{R}^+$. The Black-Scholes equation is usually equipped with conditions at the maturity date T, that is, we know $V(S,T)\ \forall S$; which is translated into conditions at the initial time and at the boundary—we know $U(\bar{S}, \bar{t} = 0),\ \forall \bar{S} \in \mathbb{R}$—applied to the heat-transfer equation.

Remark. We explore the newest abstraction corresponding to this mathematical model within the field structure $\mathbb{F}_{p^n}$; this research is supplementary with the purpose of gaining a global view-comprehension that can cover both fields, $\mathbb{R}$ and $\mathbb{F}_{p^n}$. Regarding the equation we investigated above, $\partial^{(\beta)}_{X_i^\beta}(F) = \partial^{(k)}_{X_j^k}(G)$, we find solution subspaces for a relevant case of $G = F$ (refer to Theorem 9.33), for $\beta = 1$ and $k = 2$, observing that in this case, G does not necessarily inhabit $\overline{\mathbb{M}^{((k),\Xi_k,\cdots,\Xi_{p^n-1})}_{p^n,X_j}}[X_1, \cdots, X_m]$.

Theorem 9.33 (Newest Black-Scholes equation). *Let n be a positive integer, $c_{\sigma,r}$ a non-zero constant in the field $\mathbb{F}_{p^n}$, and $(H, \bar{H}) \in \left(\mathbb{F}^*_{p^n}\right)^2$. Let us consider the partial differential equation on the space of functions $\mathcal{F}\left(\left(\mathbb{F}_{p^n}\right)^2, \mathbb{F}_{p^n}\right)$, called $\mathbb{F}_{p^n}$-Black-Scholes-Merton equation (or just $\mathbb{F}_{p^n}$-Black-Scholes eq.), given by:*

$$\partial_{\bar{t}}(U) = c_{\sigma,r} \partial^{(2)}_{\bar{S}^2}(U)$$

Then the following is a subspace of solutions:

$$\mathcal{BS}^{c_{\sigma,r}}_{\mathbb{F}_{p^n}} = \Big\{U \in \mathcal{F}((\mathbb{F}_{p^n})^2, \mathbb{F}_{p^n}); U(\bar{S},\bar{t}) = \sum_{\substack{\mathfrak{A},\mathfrak{S} \text{ are some} \\ \text{maps in } \mathcal{F}(\mathbb{F}_{p^n})}} \partial^{(p-2)}_{\bar{S}^{p-2}}(\mathfrak{A}(\bar{S}))\partial^{(p-2)}_{\bar{t}^{p-2}}(\mathfrak{S}(\bar{t}))$$

$$+ \partial^{(p-4)}_{\bar{S}^{p-4}}(\mathfrak{A}(\bar{S}))\partial^{(p-1)}_{\bar{t}^{p-1}}(\mathfrak{S}(\bar{t})) + \sum_{\substack{\widetilde{\mathfrak{S}},\mathfrak{K} \text{ are some} \\ \text{maps in } \mathcal{F}(\mathbb{F}_{p^n}), \\ \text{and } d^0_{\bar{S}}(\mathfrak{K}) \leq 3}} \partial^{(2)}_{\bar{S}^2}(\mathfrak{K}(\bar{S}))\partial^{(p-2)}_{\bar{t}^{p-2}}(\widetilde{\mathfrak{S}}(\bar{t})) +$$

$$\mathfrak{K}(\bar{S})\partial^{(p-1)}_{\bar{t}^{p-1}}(\widetilde{\mathfrak{S}}(\bar{t}))\Big\}.$$

Proof. The associativity-commutativity properties of these differential operators together with the powerful Theorem 9.20 (consequence of Theorem 9.2) allow us to directly infer that the function $\vartheta(\bar{S},\bar{t}) = \partial^{(2p-3)}_{\bar{t}^{p-1}\bar{S}^{p-2}}(\beta(\bar{S},\bar{t}))$ is a solution to all $\beta \in \mathcal{F}\big((\mathbb{F}_{p^n})^2, \mathbb{F}_{p^n}\big)$, where the derivations with respect to $\bar{S}$ are along the direction H, and those with respect to $\bar{t}$ are along the direction $\bar{H}$. Now, if $\omega_U(\bar{S},\bar{t}) := \partial_{\bar{t}}(U) = c_{\sigma,r}\partial^{(2)}_{\bar{S}^2}(U)$ is identically zero, then by Theorem 9.20—which also applies when more than one variable comes into play—we get $U = \partial^{(p-1)}_{\bar{t}^{p-1}}(\theta(\bar{S},\bar{t}))$, for some function θ. Since U must be selected from the function space $\partial^{(p-1)}_{\bar{t}^{p-1}}\big(\mathcal{F}\big((\mathbb{F}_{p^n})^2,$ $\mathbb{F}_{p^n}\big)\big)$, and expressing U in the form $U = \sum_\ell \phi_\ell(\bar{t})\xi_\ell(\bar{S})$ such that $(\phi_\ell)_\ell$ is a basis of $\partial^{(p-1)}_{\bar{t}^{p-1}}\big(\mathcal{F}\big(\mathbb{F}_{p^n}\big)\big)$, together with the fact that $c_{\sigma,r}\partial^{(2)}_{\bar{S}^2}(U) = \sum_\ell c_{\sigma,r}\phi_\ell(\bar{t})\partial^{(2)}_{\bar{S}^2}(\xi_\ell$ $(\bar{S})) = 0$, then $c_{\sigma,r}\partial^{(2)}_{\bar{S}^2}(\xi_\ell(\bar{S})) = 0$ for all ξ_ℓ within U. Thus, $\xi_\ell(\bar{S}) = \partial^{(p-2)}_{\bar{S}^{p-2}}(\tilde{\theta}_\ell(\bar{S}))$ for some $\tilde{\theta}_\ell \in \mathcal{F}\big(\mathbb{F}_{p^n}\big)$ for all ξ_ℓ. Hence $U = \sum_\ell \phi_\ell(\bar{t})\partial^{(p-2)}_{\bar{S}^{p-2}}(\tilde{\theta}_\ell(\bar{S}))$, and also has the form of some function $\partial^{(2p-3)}_{\bar{t}^{p-1}\bar{S}^{p-2}}(\tilde{\beta}(\bar{S},\bar{t}))$. Therefore we have obtained that, $\{U \in \mathcal{F}((\mathbb{F}_{p^n})^2, \mathbb{F}_{p^n}); \omega_U(\bar{S},\bar{t})$ is identically equal to $0\} = \ker\big(\partial_{\bar{t}} :$ $\mathcal{F}((\mathbb{F}_{p^n})^2, \mathbb{F}_{p^n}) \to \mathcal{F}((\mathbb{F}_{p^n})^2, \mathbb{F}_{p^n})\big) \bigcap \ker\big(c_{\sigma,r}\partial^{(2)}_{\bar{S}^2} : \mathcal{F}((\mathbb{F}_{p^n})^2, \mathbb{F}_{p^n}) \to \mathcal{F}((\mathbb{F}_{p^n})^2,$ $\mathbb{F}_{p^n})\big) = \partial^{(2p-3)}_{\bar{t}^{p-1}\bar{S}^{p-2}}\big(\mathcal{F}\big((\mathbb{F}_{p^n})^2, \mathbb{F}_{p^n}\big)\big)$. On the other hand, we observe that functions of the type $\partial^{(p-2)}_{\bar{S}^{p-2}}(\mathfrak{A}(\bar{S}))\partial^{(p-2)}_{\bar{t}^{p-2}}(\mathfrak{S}(\bar{t}))+\partial^{(p-4)}_{\bar{S}^{p-4}}(\mathfrak{A}(\bar{S}))\partial^{(p-1)}_{\bar{t}^{p-1}}(\mathfrak{S}(\bar{t}))$ satisfy the $\mathbb{F}_{p^n}$-Black-Scholes-Merton equation, as well as some of the type $\partial^{(2)}_{\bar{S}^2}(\mathfrak{K}(\bar{S}))\partial^{(p-2)}_{\bar{t}^{p-2}}$ $(\widetilde{\mathfrak{S}}(\bar{t})) + \mathfrak{K}(\bar{S})\partial^{(p-1)}_{\bar{t}^{p-1}}(\widetilde{\mathfrak{S}}(\bar{t}))$, and therefore also the $\mathbb{F}_{p^n}$-linear combinations of both, where $\mathfrak{A},\mathfrak{S},\widetilde{\mathfrak{S}},\mathfrak{K}$ are maps in $\mathcal{F}(\mathbb{F}_{p^n})$. More precisely, we establish the following class of functions with abundant solutions, Us,

$$U(\bar{S},\bar{t}) = \sum_{\substack{\mathfrak{A},\mathfrak{S} \text{ are some} \\ \text{maps in } \mathcal{F}(\mathbb{F}_{p^n})}} \partial^{(p-2)}_{\bar{S}^{p-2}}(\mathfrak{A}(\bar{S}))\partial^{(p-2)}_{\bar{t}^{p-2}}(\mathfrak{S}(\bar{t}))+\partial^{(p-4)}_{\bar{S}^{p-4}}(\mathfrak{A}(\bar{S}))\partial^{(p-1)}_{\bar{t}^{p-1}}(\mathfrak{S}(\bar{t}))+$$

$$\sum_{\substack{\widetilde{\mathfrak{S}},\mathfrak{K} \text{ are some} \\ \text{maps in } \mathcal{F}(\mathbb{F}_{p^n}), \\ \text{and } d^0_{\bar{S}}(\mathfrak{K}) \leq 3}} \partial^{(2)}_{\bar{S}^2}(\mathfrak{K}(\bar{S}))\partial^{(p-2)}_{\bar{t}^{p-2}}(\widetilde{\mathfrak{S}}(\bar{t}))+\mathfrak{K}(\bar{S})\partial^{(p-1)}_{\bar{t}^{p-1}}(\widetilde{\mathfrak{S}}(\bar{t})).$$ This class forms a $\mathbb{F}_{p^n}$-vector space that also contains the space $\partial^{(2p-3)}_{\bar{t}^{p-1}\bar{S}^{p-2}}\big(\mathcal{F}\big((\mathbb{F}_{p^n})^2, \mathbb{F}_{p^n}\big)\big)$. □

Open Problem 29. Investigate what portion of the solution space of the $\mathbb{F}_{p^n}$-*Black-Scholes equation* is the vector space $\mathcal{BS}^{c_{\sigma,r}}_{\mathbb{F}_{p^n}}$. What about those functions that reside outside $\mathcal{BS}^{c_{\sigma,r}}_{\mathbb{F}_{p^n}}$?

Open Problem 30. Construct bases of different types for the function space $\ker\big(\partial_{\bar{t}} - c_{\sigma,r}\partial^{(2)}_{\bar{S}^2}\big)$. More generally, consider the space with the extra variable $\tilde{\bar{S}}$, $\ker\big(\partial_{\bar{t}} - c_{\sigma,r}\partial^{(2)}_{\bar{S}\tilde{\bar{S}}}\big)$.

Open Problem 31. In [4] the Black-Scholes model of the form $0 = \partial_t(V) + \widetilde{\Theta}S^2\partial^{(2)}_{S^2}(V) + rS\partial_S(V) - rV$ is investigated when $\widetilde{\Theta} = f\big(S, t, \partial_S(V), \partial^{(2)}_{S^2}(V)\big)$ is a function rather than a constant. Obtain a theorem for this Black-Scholes model (treat $\widetilde{\Theta}$ as a function of (S, t)), a result connected to Theorem 9.32 concerning the $\mathbb{F}_{p^n}$-*Schrödinger equation*.

In conclusion we have contributed a series of new methods, techniques contained in theorems, definitions, and conceptualization that solve current challenges in number theory and algebra, combinatorics, differential equations, cryptanalysis, coding theory, information security, etc.

Acknowledgements. The author wishes to express his gratitude for the financial support provided in part by NSF in partnership with UPRM while he was conducting postdoctoral research. He is also grateful to: *New York Institute of Technology*; cCc-California; academic units headquartered at *Johns Hopkins University*; UPRRP, main campus, and its High Performance Computing Facility hpcf.upr.edu; academic bodies of *Fairleigh Dickinson University*; *Felician University*; and UNT, main campus. He thanks all of them for providing the latest in suitable teaching-research environments. Besides, for their valuable words of encouragement, all the support, and kindness, the author extends his permanent gratitude to professors, colleagues, and contacts, both present and past. Adj. Full-rank Prof. Roberto Carlos Reyes Carranza, Ph.D. in Math, is often interested in participating in special projects that do not necessarily have to be within his field (updated address: `roberto.reyescarranza@liu.edu` also `rreyescarranza01@manhattan.edu`). The author is grateful to the anonymous reviewers for their careful reading as well as to the publisher for its expeditious and smart system in disseminating this masterpiece.

References

[1] Z. Aldirany, R. Cottereau, Laforest, M., and S. Prudhomme, Multi-level neural networks for accurate solutions of boundary-value problems, *Computer Methods in Applied Mechanics and Engineering,* **419** (2024), 116666. https://doi.org/10.1016/j.cma.2023.116666

[2] M. Alquran, New interesting optical solutions to the quadratic-cubic Schrodinger equation by using the Kudryashov-expansion method and the updated rational sine-cosine functions, *Optical and Quantum Electronics,* **54** (2022), no. 10, 666. https://doi.org/10.1007/s11082-022-04070-3

[3] C. Anitescu, E. Atroshchenko, N. Alajlan, and T. Rabczuk, Artificial neural network methods for the solution of second order boundary value problems, *Computers, Materials & Continua,* **59** (2019), no. 1, 345-359. https://doi.org/10.32604/cmc.2019.06641

[4] J. Ankudinova, and M. Ehrhardt, On the numerical solution of nonlinear Black-Scholes equations, *Computers & Mathematics with Applications,* **56** (2008), no. 3, 799-812. https://doi.org/10.1016/j.camwa.2008.02.005

[5] Y. Aubry, G. McGuire and F. Rodier, A few more functions that are not APNinnitely often, *Finite Fields: Theory and Applications,* **518** (2010), 23-31. https://doi.org/10.1090/conm/518/10193

[6] J. A. Bárcena-Petisco, M. Cavalcante, G. M. Coclite, N. De Nitti, and E. Zuazua, Control of hyperbolic and parabolic equations on networks and singular limits, *Mathematical Control and Related Fields,* **15** (2025), no. 1, 348-389. https://doi.org/10.3934/mcrf.2024015

[7] D. Bartoli et al., Hasse-Weil type theorems and relevant classes of polynomial functions, *En BCC,* 43-102, 2021. https://doi.org/10.1017/9781009036214.003

[8] T. D. Bending, and D. Fon-Der-Flaass, Crooked functions, bent functions, and distance regular graphs, *the electronic journal of combinatorics,* R34-R34, 1998. https://doi.org/10.37236/1372

[9] E. Bendito, A. Carmona, and A. M. Encinas, Potential theory for Schrödinger operators on finite networks, *Revista matemática iberoamericana,* **21** (2005), no. 3, 771-818. https://doi.org/10.4171/rmi/435

[10] U. Biccari, M. Warma, and E. Zuazua, Boundary observation and control for fractional heat and wave equations, 2025. arXiv preprint arXiv:2504.17413

[11] E. Biham and A. Shamir, Differential cryptanalysis of DES-like cryptosystems, *Journal of CRYPTOLOGY,* **4** (1991), 3-72.

[12] C. Blondeau, A. Canteaut, and P. Charpin, Differential properties of power functions, *International Journal of Information and Coding Theory,* **1** (2010), no. 2, 149-170. https://doi.org/10.1109/isit.2010.5513437

[13] C. Blondeau, A. Canteaut, and P. Charpin, Differential properties of $x \mapsto x^{2^t-1}$, *IEEE Transactions on Information Theory,* **57** (2011), no. 12, 8127-8137. https://doi.org/10.1109/tit.2011.2169129

[14] C. Blondeau, and L. Perrin, More differentially 6-uniform power functions, *Designs, codes and cryptography,* **73** (2014), 487-505. https://doi.org/10.1007/s10623-014-9948-2

[15] N. Borisov, M. Chew, R. Johnson, and D. Wagner, Multiplicative differentials, *In Fast Software Encryption: 9th International Workshop, FSE 2002 Leuven, Belgium, February 4-6, 2002 Revised Papers 9 (pp. 17-33). Springer Berlin Heidelberg.*

[16] C. Bracken, E. Byrne, N. Markin, and G. McGuire, On the Walsh spectrum of a new APN function, *In Cryptography and Coding: 11th IMA International Conference, Cirencester, UK, December 18-20, 2007. Proceedings 11, pp. 92-98. Springer Berlin Heidelberg, 2007.*

[17] C. Bracken, C. H. Tan, and Y. Tan, Binomial differentially 4 uniform permutations with high nonlinearity, *Finite Fields Appl.,* **18** (2012), no. 3, 537-546. https://doi.org/10.1016/j.ffa.2011.11.006

[18] C. Bracken and G. Leander, A highly nonlinear differentially 4 uniform power mapping that permutes fields of even degree, *Finite Fields Appl.,* **16** (2010), no. 4, 231-242. https://doi.org/10.1016/j.ffa.2010.03.001

[19] S. Bravyi, O. Dial, J. M. Gambetta, D. Gil, and Z. Nazario, The future of quantum computing with superconducting qubits, *Journal of Applied Physics,* **132** (2022), no. 16. https://doi.org/10.1063/5.0082975

[20] T. P. Berger, A. Canteaut, P. Charpin, and Y. Laigle-Chapuy, On Almost Perfect Nonlinear Functions Over $\mathbb{F}_2^n$, *IEEE Transactions on Information Theory,* **52** (2006), no. 9, 4160-4170. https://doi.org/10.1109/tit.2006.880036

[21] E. Bergman, and R. S. Coulter, Constructing Functions with Low Differential Uniformity, *Mediterranean Journal of Mathematics,* **19** (2022), no. 2, 94. https://doi.org/10.1007/s00009-022-01980-0

[22] F. Black, and M. Scholes, The pricing of options and corporate liabilities, *Journal of political economy,* **81** (1973), no. 3, 637-654. https://doi.org/10.1086/260062

[23] L. Budaghyan, C. Carlet, and A. Pott, New classes of almost bent and almost perfect nonlinear polynomials, *IEEE Trans. Inform. Theory,* **52** (2006), no. 3, 1141-1152. https://doi.org/10.1109/tit.2005.864481

[24] L. Budaghyan, C. Carlet, and G. Leander, Two classes of quadratic APN binomials inequivalent to power functions, *IEEE Transactions on Information Theory,* **54** (2008), no. 9, 4218-4229. https://doi.org/10.1109/tit.2008.928275

[25] L. Budaghyan, C. Carlet, and G. Leander, On inequivalence between known power APN functions, *Proceedings of the conference BFCA, Copenhagen,* 2008.

[26] L. Budaghyan, C. Carlet, and G. Leander, Constructing new APN functions from known ones, *Finite Fields Appl.,* **15** (2009), no. 2, 150-159. https://doi.org/10.1016/j.ffa.2008.10.001

[27] L. Budaghyan, M. Calderini, C. Carlet, D. Davidova, and N. Kaleyski, A note on the walsh spectrum of Dobbertin apn functions, In *In Proceedings of SETA,* submittedd 2020.

[28] M. Calderini, Differentially low uniform permutations from known 4-uniform functions, *Designs, Codes and Cryptography,* **89** (2021), no. 1, 33-52. https://doi.org/10.1007/s10623-020-00807-x

[29] A. Canteaut, P. Charpin, and H. Dobbertin, Binary m-sequences with three-valued crosscorrelation: a proof of Welch's conjecture, *IEEE Transactions on Information Theory,* **46** (2000), no. 1, 4-8. https://doi.org/10.1109/18.817504

[30] A. Canteaut, and M. Videau, Degree of composition of highly nonlinear functions and applications to higher order differential cryptanalysis, *In Advances in Cryptology—EUROCRYPT 2002: International Conference on the Theory and Applications of Cryptographic Techniques Amsterdam, The Netherlands, April 28-May 2, 2002 Proceedings 21, pp. 518-533. Springer Berlin Heidelberg, 2002.*

[31] C. Carlet, Y. Crama, and P. L. Hammer, Vectorial boolean functions for cryptography, 2010. https://doi.org/10.1017/cbo9780511780448.012

[32] C. Carlet, On known and new differentially uniform functions, In *Australasian Conference on Information Security and Privacy*, Springer, (2011), 1-15.

[33] C. Carlet, On the higher order nonlinearities of algebraic immune functions, In *Advances in cryptology—CRYPTO 2006*, volume 4117 of *Lecture Notes in Comput. Sci.,* pages 584-601. Springer, Berlin, 2006.

[34] C. Carlet, P. Charpin, and V. Zinoviev, Codes, bent functions and permutations suitable for DES-like cryptosystems, *Designs, Codes and Cryptography,* **15** (1998), no. 2, 125-156. https://doi.org/10.1023/a:1008344232130

[35] C. Carlet, *Boolean functions for cryptography and coding theory,* 2021. https://doi.org/10.1017/9781108606806

[36] L. Carlitz, and S. Uchiyama, Bounds for exponential sums, *Duke Math. Journal,* **24** (1957) no. 1, 37-41. https://doi.org/10.1215/s0012-7094-57-02406-7

[37] L. Carlitz, Kloosterman sums and finite field extensions, *Acta Arithmetica,* **16** (1969), no. 2, 179-194. https://doi.org/10.4064/aa-16-2-179-194

[38] P. Charpin and G. M. Kyureghyan, and V. Suder, Sparse permutations with low differential uniformity, *Finite Fields and Their Applications,* **28** (2014), 214-243. https://doi.org/10.1016/j.ffa.2014.02.003

[39] P. Charpin and G. M. Kyureghyan, On sets determining the differential spectrum of mappings, *Int. J. Inf. Coding Theory,* **4** (2017), no. (2-3), 170-184. https://doi.org/10.1504/ijicot.2017.083844

[40] C. Li, C. Riera, and P. Stănică, Dillon's switching method generalized to c-differentials. Manuscript; preliminary version in, *Boolean Functions & Applic.(BFA)*, Paper# 1, 2022.

[41] C. Li, C. Riera, and P. Stănică, Low c-differentially uniform functions via an extension of Dillon's switching method, (2022). arXiv preprint arXiv:2204.08760

[42] G. Cohen, M. Karpovsky, H. Mattson, and J. Schatz, Covering radius—survey and recent results, *IEEE Transactions on Information Theory,* **31** (1985), no. 3, 328-343. https://doi.org/10.1109/tit.1985.1057043

[43] G. Cohen, I. Honkala, S. Litsyn, and A. Lobstein, *Covering codes,* volume 54 of *North-Holland Mathematical Library*, North-Holland Publishing Co., Amsterdam, 1997. https://doi.org/10.1016/s0924-6509(97)x8001-8

[44] J. B. Conway, Functions of One Complex Variable I, *Springer Verlag,* 1986.

[45] R. S. Coulter, and R. W. Matthews, Planar functions and planes of Lenz-Barlotti class II, *Designs, Codes and Cryptography,* **10** (1997), no. 2, 167-184.

[46] R. S. Coulter and M. Henderson, A class of functions and their application in constructing semi-biplanes and association schemes, *Discrete mathematics,* **202** (1999), no. (1-3), 21-31. https://doi.org/10.1016/s0012-365x(98)00345-8

[47] N. T. Courtois, and J. Pieprzyk, Cryptanalysis of block ciphers with overdefined systems of equations, *In Advances in Cryptology—ASIACRYPT 2002: 8th International Conference on the Theory and Application of Cryptology and Information Security Queenstown, New Zealand, December 1-5, 2002 Proceedings 8, pp. 267-287. Springer Berlin Heidelberg, 2002.*

[48] S. Y. Chung, Y. S. Chung, and J. H. Kim, Diffusion and elastic equations on networks, *Publications of the Research Institute for Mathematical Sciences,* **43** (2007), no. 3, 699-726.
https://doi.org/10.2977/prims/1201012039

[49] E. B. Curtis and J. A. Morrow, The Dirichlet to Neumann map for a resistor network, *SIAM Journal on Applied Mathematics,* **51** (1991), no. 4, 1011-1029. https://doi.org/10.1137/0151051

[50] J. Daemen and V. Rijmen, *The design of Rijndael,* Information Security and Cryptography, Springer-Verlag, Berlin, AES—the advanced encryption standard, 2002. https://doi.org/10.1007/978-3-662-04722-4

[51] J. Daemen, and V. Rijmen, Aes proposal: Rijndael, 1999.

[52] M. Delgado, R. Reyes Carranza, and C. Agrinsoni, DES-like Ciphers, Differential Attacks and APN Functions, *Journal of Mathematical Sciences: Advances and Applications,* **49** (2018), no. 1, 29-50.

[53] P. Dembowski, and T. G. Ostrom, Planes of order n with collineation groups of order n 2, *Mathematische Zeitschrift,* **103** (1968), no. 3, 239-258. https://doi.org/10.1007/bf01111042

[54] U. Dempwolff, CCZ equivalence of power functions, *Des. Codes Cryptogr.,* **86** (2018), 665-692. https://doi.org/10.1007/s10623-017-0350-8

[55] J. F. Dillon, Multiplicative difference sets via additive characters, *Designs, Codes and Cryptography,* **17** (1999), no. 1, 225-235.

[56] J. F. Dillon and H. Dobbertin, New cyclic difference sets with Singer parameters, *Finite Fields and Their Applications,* **10** (2004), no. 3, 342-389. https://doi.org/10.1016/j.ffa.2003.09.003

[57] J. F. Dillon, Apn polynomials and related codes, In *Banff Conference, Nov. 2006,* 2006.

[58] J. F. Dillon, Apn polynomials: an update, In *International Conference on Finite fields and applications-Fq9,* 2009.

[59] H. Dobbertin, One-to-one highly nonlinear power functions on GF(2n), *Applicable Algebra in Engineering, Communication and Computing,* **9** (1998), no. 2, 139-152. https://doi.org/10.1007/s002000050099

[60] H. Dobbertin, Almost perfect nonlinear power functions on GF(2/sup n/): the welch case, *IEEE Transactions on Information Theory,* **45** (1999), no. 4, 1271-1275. https://doi.org/10.1109/18.761283

[61] H. Dobbertin, Almost perfect nonlinear power functions on GF(2n): the niho case, *Information and Computation,* **151** (1999), no. 1-2, 57-72. https://doi.org/10.1006/inco.1998.2764

[62] H. Dobbertin, Almost perfect nonlinear power functions on GF(2 n): a new case for n divisible by 5, *Finite Fields and Applications,* **151** (1999), no. 1-2, 113-121.

[63] H. Dobbertin, D. Mills, E. N. Müller, A. Pott, and W. Willems, APN functions in odd characteristic, *Discrete mathematics,* **267** (2003), no. 1-3, 95-112. https://doi.org/10.1016/s0012-365x(02)00606-4

[64] R. J. Duffin, Potential theory on a rhombic lattice, *Journal of Combinatorial Theory,* **5** (1968), no. 3, 258-272. https://doi.org/10.1016/s0021-9800(68)80072-9

[65] D. S. Dummit, and R. M. Foote, Abstract algebra, *Vol. 3. Hoboken: Wiley,* 2004.

[66] S. Dutta, R. Sarkar, and P. K. Panigrahi, Permutation symmetric hypergraph states and multipartite quantum entanglement, *International Journal of Theoretical Physics,* **58** (2019), 3927-3944. https://doi.org/10.1007/s10773-019-04259-5

[67] Y. Edel and A. Pott, A new almost perfect nonlinear function which is not quadratic, *Adv. Math. Commun.,* **3** (2009), no. 1, 59-81. https://doi.org/10.3934/amc.2009.3.59

[68] P. Ellingsen, P. Felke, C. Riera, P. Stănică, and A. Tkachenko, C-differentials, multiplicative uniformity, and (almost) perfect c-nonlinearity, *IEEE Transactions on Information Theory,* **66** (2020), no. 9, 5781-5789. https://doi.org/10.1109/tit.2020.2971988

[69] M. D. Feit, J. A. Fleck, and A. Steiger, Solution of the Schrödinger equation by a spectral method, *Journal of Computational Physics.,* **47** (1982), no. 3, 412-433. https://doi.org/10.1016/0021-9991(82)90091-2

[70] J. B. Fraleigh, A First Course in Abstract Algebra, *Pearson Education,* 2003.

[71] D. Garton, Periodic points of rational functions of large degree over finite fields, 2022. arXiv preprint arXiv:2208.13281

[72] R. Gold, Maximal recursive sequences with 3-valued recursive cross-correlation functions (corresp.), *IEEE transactions on Information Theory,* **14** (1968), no. 1, 154-156. https://doi.org/10.1109/tit.1968.1054106

[73] Paul Richard Halmos, Naive set theory, *van Nostrand,* 1960.

[74] Y. Hiramine, On planar functions, In *Journal of Algebra, Springer* **133** (1990), no. 1, 103-110. https://doi.org/10.1016/0021-8693(90)90071-u

[75] M. Hein, W. Dür, J. Eisert, R. Raussendorf, M. Van den Nest, and H. J. Briegel, Entanglement in graph states and its applications, In *Quantum computers, algorithms and chaos, IOS Press,* (2006), 115-218.

[76] Henk D. L. Hollmann, and Q. Xiang, A proof of the Welch and Niho conjectures on cross-correlations of binary m-sequences, In *Finite Fields and Their Applications,* **7** (2001), no. 2, 253-286. https://doi.org/10.1006/ffta.2000.0281

[77] F. Hernando, and G. McGuire, Proof of a conjecture on the sequence of exceptional numbers, classifying cyclic codes and APN functions, *Journal of Algebra,* **343** (2011), no. 1, 78-92. https://doi.org/10.1016/j.jalgebra.2011.06.019

[78] H. Janwa and R. M. Wilson, Hyperplane sections of Fermat varieties in $\mathbf{P}^3$ in char. 2 and some applications to cyclic codes, In *Applied algebra, algebraic algorithms and error-correcting codes (San Juan, PR, 1993),* volume 673 of *Lecture Notes in Comput. Sci.*, pages 180-194. Springer, Berlin, 1993.

[79] J. Jeong, N. Koo, and S. Kwon, Constructing differentially 4-uniform involutions over F22k by using carlitz form, *Finite Fields and Their Applications,* **78** (2022), no. 3, 101957. https://doi.org/10.1016/j.ffa.2021.101957

[80] J. Jeong, N. Koo, and S. Kwon, New differentially 4-uniform permutations from modifications of the inverse function, *Finite Fields and Their Applications,* **77** (2022), 101931. https://doi.org/10.1016/j.ffa.2021.101931

[81] T. Kasami, The weight enumerators for several classes of subcodes of the 2nd order binary Reed-Muller codes, *Information and Control,* **18** (1971), 369-394. https://doi.org/10.1016/s0019-9958(71)90473-6

[82] J. Klappert, F. Lange, P. Maierhöfer, and J. Usovitsch, Integral reduction with Kira 2.0 and finite field methods, *Computer Physics Communications,* **266** (2021), 108024. https://doi.org/10.1016/j.cpc.2021.108024

[83] N. A. Kudryashov, Implicit solitary waves for one of the generalized nonlinear Schrödinger equations, *Mathematics,* **9** (2021), no. 23, 3024. https://doi.org/10.3390/math9233024

[84] G. Kyureghyan, Crooked maps in F2n, *Finite Fields and their applications,* **13** (2007), no. 3, 713-726. https://doi.org/10.46298/dmtcs.3392

[85] G. M. Kyureghyan; V. Suder, On inversion in Z2n-1, *Finite Fields and their applications,* **25** (2014), 234-254. https://doi.org/10.1016/j.ffa.2013.10.002

[86] G. Lachaud, and J. Wolfmann, The weights of the orthogonals of the extended quadratic binary Goppa codes, *IEEE transactions on information theory,* **36** (1990), no. 3, 686-692. https://doi.org/10.1109/18.54892

[87] X. Lai, Higher order derivatives and differential cryptanalysis, *Communications and Cryptography: Two Sides of One Tapestry,* (1994), 227-233.

[88] X. Lai, J. L. Massey, and S. Murphy, Markov ciphers and differential cryptanalysis, *In Advances in Cryptology—EUROCRYPT'91: Workshop on the Theory and Application of Cryptographic Techniques Brighton, UK, April 8-11, 1991 Proceedings 10, pp. 17-38. Springer Berlin Heidelberg, 1991.*

[89] Serge Lang, Algebra, 3rd Edition, *Springer Verlag, New York,* 2002.

[90] T. Leinster, Basic category theory, *Cambridge University Press,* **143** (2014). https://doi.org/10.1017/cbo9781107360068

[91] A. Lenstra, E. Tromer, A. Shamir, W.l Kortsmit, B. Dodson, J. Hughes, and P. Leyland, Factoring estimates for a 1024-bit RSA modulus, In *Advances in cryptology—ASIACRYPT 2003*, volume 2894 of *Lecture Notes in Comput. Sci.,* pages 55-74. Springer, Berlin, 2003.

[92] Y. Li, M. Wang, and Y. Yu, Constructing differentially 4-uniform permutations over GF (22k) from the inverse function revisited, *IACR Cryptol. ePrint Arch,* **2013** (2013), 731.

[93] Y. Li and M. Wang , Constructing differentially 4-uniform permutations over GF(2 2m) from quadratic apn permutations over GF(2 2m+ 1), *Designs, codes and cryptography,* **72** (2014), no. 2, 249-264. https://doi.org/10.1007/s10623-012-9760-9

[94] R. Lidl, and H. Niederreiter, Finite fields, *Cambridge university press,* no. 20, 1997. https://doi.org/10.1017/cbo9780511525926

[95] J. B. Lima, R. M. Campello de Souza, and D. Panario, The eigenstructure of finite field trigonometric transforms, *Linear Algebra and its Applications,* **435** (2011), no. 8, 1956-1971. https://doi.org/10.1016/j.laa.2011.03.031

[96] D. W. Lyons, D. J. Upchurch, S. N. Walck, and C. D. Yetter, Local unitary symmetries of hypergraph states, *Journal of Physics A: Mathematical and Theoretical,* **48** (2015), no. 9, 095301. https://doi.org/10.1088/1751-8113/48/9/095301

[97] F. J. MacWilliams and N. J. A. Sloane, *The theory of error-correcting codes. II*, North-Holland Publishing Co., Amsterdam-New York-Oxford, North-Holland Mathematical Library, **16**, 1977. https://doi.org/10.1016/s0924-6509(08)x7030-8

[98] P. Méaux, and D. Roy, Theoretical differential fault attacks on FLIP and FiLIP, *Cryptography and Communications,* (2024), 1-24. https://doi.org/10.1007/s12095-024-00698-y

[99] M. Pal, and P. Stănică, A connection between the boomerang uniformity and the extended differential in odd characteristic and applications, *arXiv preprint,* 2023. arXiv:2312.01434. https://doi.org/10.3934/amc.2024059

[100] D. W. Moore, Quantum hypergraph states in continuous variables, *Physical Review A,* **100** (2019), no. 6, 062301. https://doi.org/10.1103/physreva.100.062301

[101] G. L. Mullen, and D. Panario, Handbook of finite fields, *Boca Raton: CRC press,* **17**, 2013. https://doi.org/10.1201/b15006

[102] J. Von Neumann, Mathematical foundations of quantum mechanics: New edition. Princeton university press, 2018. https://doi.org/10.23943/princeton/9780691178561.001.0001

[103] K. Nyberg, On the construction of highly nonlinear permutations, *Workshop on the Theory and Application of of Cryptographic Techniques,* pages 92-98. Berlin, Heidelberg: Springer Berlin Heidelberg, 1992.

[104] K. Nyberg, Differentially uniform mappings for cryptography, In *Workshop on the Theory and Application of of Cryptographic Techniques,* pages 55-64, Springer, 1993.

[105] K. Nyberg, S-boxes and round functions with controllable linearity and differential uniformity, In *In International Workshop on Fast Software Encryption,* pages 111-130. Berlin, Heidelberg: Springer Berlin Heidelberg, 1994.

[106] D. Panario, and L. Reis, The functional graph of linear maps over finite fields and applications, *Designs, Codes and Cryptography,* **87** (2019), 437-453. https://doi.org/10.1007/s10623-018-0547-5

[107] J. Peng, C. H. Tan, and Q. Wang, A new family of differentially 4-uniform permutations over $\mathbb{F}_{2^{2k}}$ for odd k, *Sci. China Math.,* **59** (2016), no. 6, 1221-1234. https://doi.org/10.1007/s11425-016-5122-9

[108] T. Peraro, FiniteFlow: multivariate functional reconstruction using finite fields and dataflow graphs, *Journal of High Energy Physics,* **7** (2019). https://doi.org/10.1007/jhep07(2019)031

[109] L. Qu, Y. Tan, C. H. Tan, and C. Li, Constructing differentially 4-uniform permutations over $\mathbb{F}_{2^{2k}}$ via the switching method, *IEEE Trans. Inform. Theory,* **59** (2013), no. 7, 4675-4686. https://doi.org/10.1109/tit.2013.2252420

[110] Roberto Reyes, Comparison of elastic plate theories for micropolar materials. *Diss. MS Thesis, University of Puerto Rico, Mayaguez,* 2010.

[111] Roberto C. Reyes Carranza, Construction of new differentially delta-uniform families, *Ph.D. Dissertation, University of Puerto Rico, Rio Piedras,* 2020.

[112] R. C. Reyes Carranza, Construction of the First Nonmonomial Exceptional APN and Solution of a Conjecture Plus the Core Cases of a Second, *International Journal of Algebra,* **18** (2024), no. 1, 15-30. https://doi.org/10.12988/ija.2024.91851

[113] Roberto C. Reyes Carranza, On a Type of Optimization Problem, *To appear in International Journal of Algebra,*

[114] C. Riera, M. G. Parker, and P. Stanica, Quantum states associated to mixed graphs and their algebraic characterization, *Adv. Math. Commun.,* **17** (2023), no. 3, 660-680. https://doi.org/10.3934/amc.2021015

[115] F. Rodier, Borne sur le degré des polynômes presque parfaitement nonlinéaires, *Contemporary Mathematics,* **487** (2009), 169. https://doi.org/10.1090/conm/487/09531

[116] H. L. Royden, Real Analysis. Third Edition, *Macmillan Publishig Company,* 1988.

[117] A. Sarma, T. W. Watts, M. Moosa, Y. Liu, and P. L. McMahon, Quantum variational solving of nonlinear and multidimensional partial differential equations, *Physical Review A,* **109** (2024), no. 6, 062616. https://doi.org/10.1103/physreva.109.062616

[118] E. Schrödinger, Discussion of probability relations between separated systems, *Mathematical Proceedings of the Cambridge Philosophical Society,* **31** (1935), no. 4, 555-563, Cambridge University Press. https://doi.org/10.1017/s0305004100013554

[119] B. Segre, Ovals in a finite projective plane, *Canadian Journal of Mathematics,* **7** (1955), 414-416. https://doi.org/10.4153/cjm-1955-045-x

[120] C. E. Shannon, Communication theory of secrecy systems, *The Bell system technical journal,* **28** (1949), no. 4, 656-715. https://doi.org/10.1002/j.1538-7305.1949.tb00928.x

[121] J.H. Silverman, The arithmetic of dynamical systems, *Springer Science & Business Media,* 241, 2010. https://doi.org/10.1007/978-0-387-69904-2

[122] A. Skolik, M. Cattelan, S. Yarkoni, T. Bäck, and V. Dunjko, Equivariant quantum circuits for learning on weighted graphs, *npj Quantum Information,* **9** (2023), no. 1, 47. https://doi.org/10.1038/s41534-023-00710-y

[123] B. Steinbach, and C. Posthoff, Boolean differential equations. In *Boolean Differential Equations. Cham: Springer International Publishing,* 49-127, 2013.

[124] L. Steinberg and R. Kvasov, Cosserat plate theory, *CRC Press,* 2022. https://doi.org/10.1201/9781003190264

[125] L. Steinberg and R. Kvasov, Numerical modeling of bending of Cosserat elastic plates, *Proceedings of the 5th Computing Alliance of Hispanic-Serving Institutions,* pages 67-70, 2011.

[126] A. Sălăgean, R. Winter, M. Mandache-Sălăgean, and R. C.-W. Phan, Higher order differentiation over finite fields with applications to generalising the cube attack, *Designs, codes and cryptography,* **84** (2017), 425-449. https://doi.org/10.1007/s10623-016-0277-5

[127] D. Tang, C. Carlet, and X. Tang, Differentially 4-uniform bijections by permuting the inverse function, *Des. Codes Cryptogr.,* **77** (2015), no. 1, 117-141. https://doi.org/10.1007/s10623-014-9992-y

[128] Z. Tu, X. Zeng, and Z. Zhang, More permutation polynomials with differential uniformity six, *Sci. China Inf. Sci.,* **61** (2018), no. 3, 038104-1. https://doi.org/10.1007/s11432-017-9118-5

[129] T. Vasiga, and J. Shallit. On the iteration of certain quadratic maps over GF(p), *Discrete Mathematics,* **277** (2004), no. (1-3), 219-240. https://doi.org/10.1016/s0012-365x(03)00158-4

[130] Y.-P. Wang, W. G. Zhang, and Z. Zha, Low differentially uniform permutations from the Dobbertin APN function over F2n, *Discrete Mathematics,* **344** (2021), no. 12, 112616. https://doi.org/10.1016/j.disc.2021.112616

[131] A. Weil, On some exponential sums, *Proceedings of the National Academy of Sciences,* **34** (1948), no. 5, 204-207. https://doi.org/10.1073/pnas.34.5.204

[132] H. Weyl, The theory of groups and quantum mechanics, *Courier Corporation,* 1950.

[133] G. Xu and L. Qu., Two classes of differentially 4-uniform permutations over f 2n with n even, *Advances in Mathematics of Communications,* **14** (2020), no. 1. https://doi.org/10.3934/amc.2020008

[134] Y. Xu, Y. Li, C. Wu, and F. Liu, On the construction of differentially 4-uniform involutions, *Finite Fields and Their Applications,* **47** (2017), 309-329. https://doi.org/10.1016/j.ffa.2017.06.004

[135] S. Yoshiara, Equivalences of power APN functions with power or quadratic APN functions, *J Algebr Comb,* **44** (2016), 561-585. https://doi.org/10.1007/s10801-016-0680-z

[136] Y. Yu, M. Wang, and Y. Li, Constructing differentially 4 uniform permutations from known ones, *Chinese Journal of Electronics,* **22** (2013), no. 3, 495-499.

[137] Y. Zang, G. Bao, X. Ye, and H. Zhou, Weak adversarial networks for high-dimensional partial differential equations, *Journal of Computational Physic,* (2020), 411, 109409. https://doi.org/10.1016/j.jcp.2020.109409

[138] Z. Zha, L. Hu, and S. Sun, Constructing new differentially 4-uniform permutations from the inverse function, *Finite Fields Appl.,* (2014), 25, 64-78. https://doi.org/10.1016/j.ffa.2013.08.003

[139] Z. Zha, L. Hu, and J. Shan, Differentially 6-uniform permutations by modifying the Gold function, *2014 IEEE International Conference on Information and Automation (ICIA),* (2014), 961-965. https://doi.org/10.1109/icinfa.2014.6932790

[140] Z. Zha, and L. Hu, and S. Sun, and J. Shan, Further Results on Differentially 4-Uniform Permutations over $\mathbb{F}_{2^{2m}}$, *Science China Mathematics,* **58** (2015), no. 7, 1577-1588. https://doi.org/10.1007/s11425-015-4996-2

[141] E. Zuazua, Remarks on the controllability of the Schrödinger equation, *En CRM Workshop,* 193-211, 2002. https://doi.org/10.1090/crmp/033/12

Received: May 25, 2025; Published: June 20, 2025