New GAPN Functions with the Lowest Algebraic Degree

Noureddine El-Asri and Valentin Suder

September 17, 2025

Abstract

Most of the known (Almost) Perfect Nonlinear functions over an arbitrary finite field $\mathbb{F}_{p^n}$ have the lowest possible algebraic degree (2) and can be represented by Dembowski-Ostrom (DO) polynomials. We define Generalized DO (GDO) polynomials as homogeneous polynomials of algebraic degree p over finite fields with characteristic p. We illustrate the similarities between DO and GDO polynomials when studied through generalized derivatives. Using this framework, we propose several new classes of Generalized Almost Perfect Nonlinear (GAPN) functions of algebraic degree p, the lowest possible over the finite field $\mathbb{F}_{p^n}$.

1 Introduction

(Almost) Perfect Nonlinear (APN/PN) functions have the best resistance against differential cryptanalysis [19] of block ciphers. Due to their properties, APN/PN functions have applications in other domains such as finite geometry [9] and coding theory [29]. As such exceptional objects, APN/PN functions have attracted the attention of many cryptographers and mathematicians over the years (see [22, 28, 14] to name only a few).

In the recent years, major cryptographic advances have been made regarding zero-knowledge protocols [3] and fully-homomorphic encryption [7] for instance. These recent developments have moved the paradigm from binary fields symmetric cryptography primitives to what is now called arithmetization-oriented cryptography, that is cryptography primitives operating on elements belonging to finite fields with odd characteristics.

Among the many attempts to generalize the concept of Almost Perfect Nonlinearity [1, 4, 11, 5], the one introduced by Kuroda: Generalized Almost Perfect Nonlinear (GAPN) functions [16] fits particularly well in odd characteristic as a direct transposition from APN functions in even characteristic. In this article, we quickly survey the known GAPN functions from the literature [16, 15, 21, 24, 2, 30, 31, 26] that we classify in various tables in the appendix of this article. We display known monomial and non-monomial GAPN functions of algebraic degree p in Table 1 and Table 2 respectively, while Table 3 and Table 4 presents the known monomials and non-monomials GAPN functions respectively, that have an algebraic degree greater than p.

Our main result is to present some new classes of GAPN functions of algebraic degree p, both monomial and multinomial. They are added to Tables 1 and 2. For most of these newly introduced GAPN functions, it is possible to check that they are new up to Generalized Extended Affine Equivalence (see Definition 7) because their Hamming degree (see Definition 2) differs from previously known ones.

The article is structured as follows. Section 2 introduces the mandatory notions concerning the different degrees of functions over a finite field and the derivatives of a functions. In Section 3, we recall the concept of generalized derivatives, some basic properties and the so-called Generalized Extended-Affine (GEA) equivalence. Section 4 contains our main results, that is new classes of GAPN functions of the lowest possible algebraic degree p. Before presenting first some new family of monomial GAPN functions in Subsection 4.2, we introduce the concept of Generalized Dembowski-Ostrom polynomials, that is homogeneous polynomials of algebraic degree p. In Subsection 4.3 we emphasize the relevance of considering such polynomials when studying GAPN functions, mostly because their generalized derivatives are represented by linearized polynomials. Finally, by utilizing this fact, we present new multinomial GAPN functions, and more notably with Hamming degree 3 and 5.

2 Preliminaries

We denote by $\mathbb{F}_q$ the finite fields with q elements, a power of a prime p called the characteristic, and the multiplicative group of its non-zero elements by $\mathbb{F}_q^*$. In this work, we will be using different notions for the degree of a function $F(x) = \sum_{i=0}^{p^n-1} c_i x^i$ over $\mathbb{F}_{p^n}$.

Definition 1 (Polynomial Degree)**.** The polynomial degree of F is defined by:

$$\deg_P(F) := \max\{i \mid 0 \leq i < p^n, \quad c_i \neq 0\}.$$

Definition 2 (Hamming Degree)**.** The Hamming degree of F is defined by:

$$\deg_H(F) := \max\{H_p(i) \mid 0 \leq i < p^n, \quad c_i \neq 0\}$$

where $H_p(i)$ is the p-ary hamming weight of the integer i, that is the number of non-zero coefficients in the p-ary representation of i.

Definition 3 (Algebraic Degree)**.** The algebraic degree of F is defined by:

$$\deg_A(F) := \max\{\sum_{i=0}^{n-1} a_i \mid 0 \leq a_i < p, \quad c_{\sum_{i=0}^{n-1} a_i p^i} \neq 0\}.$$

Remark 1. In binary fields, the concepts of Hamming degree and algebraic degree coincide.

Example 1. Let $p = 5$ and $n > 2$. The monomial function $x \mapsto x^{40} = x^{1\times 25+3\times 5}$ over $\mathbb{F}_{5^n}$ has:

- polynomial degree, $\deg_P(x^{40}) = 40$
- Hamming degree, $\deg_H(x^{40}) = 2$
- Algebraic degree, $\deg_A(x^{40}) = 4$

Although we do not restate the correspondence here, it is worth noting that the algebraic degree of a univariate function over $\mathbb{F}_{p^n}$ corresponds to the maximum multivariate degree of its component functions when seen over the vector space $\mathbb{F}_p^n$.

Definition 4 (Derivative functions)**.** Let $F : \mathbb{F}_q \to \mathbb{F}_q$ and an element $\alpha \in \mathbb{F}_q^*$. The derivative of F in the direction α is defined as:

$$\Delta_\alpha F(x) = F(x+\alpha) - F(x),$$

The derivative of order d along the directions $\alpha_i \in \mathbb{F}_q^*$, for $i = 1, \ldots, d$ is defined by:

$$\Delta_{\alpha_1,\ldots,\alpha_d} F(x) = \Delta_{\alpha_1}\Delta_{\alpha_2,\ldots,\alpha_d} F(x) = \sum_{j=0}^{d} (-1)^{d-j} \sum_{\{i_1,\ldots,i_j\}\subseteq\{1,\ldots,d\}} F(x + \sum_{k=1}^{j} \alpha_{i_k}).$$

We will denote $\Delta_S F(x) := \Delta_{\alpha_1,\ldots,\alpha_d} F(x)$, where $S = \{\alpha_1, \ldots, \alpha_d\}$

Proposition 1. *With the same notation as in Definition 4,*

$$\deg_A(\Delta_S F) \leq \deg_A(F) - \#S.$$

3 Generalized differentials

In 2017, Kuroda and Tsujie [16] introduced a new generalization of APN functions that is particularly convenient in odd characteristic for its similitude with APN functions defined over a binary field. More specifically, they defined generalized almost perfect nonlinear (GAPN) functions to be functions $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ for which the equations

$$\sum_{i\in\mathbb{F}_p} F(x + i\alpha) = \beta, \qquad \forall \alpha \neq 0,\ \beta \in \mathbb{F}_{p^n},$$

has at most p solutions. Actually, this notion can be extended to the concept of generalized differential uniformity.

Definition 5 (Generalized differential uniformity)**.** The generalized differential uniformity of a function $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ is the value:

$$\mathcal{U}(F) = \max_{\alpha\neq 0, \beta\in\mathbb{F}_{p^n}} \#\{x \in \mathbb{F}_{p^n} \mid \sum_{i\in\mathbb{F}_p} F(x + i\alpha) = \beta\} \geq p.$$

When $\mathcal{U}(F) = p$, the function F is called a GAPN function.

It is clear from this definition that the generalized differential uniformity of a function is a multiple of the characteristic of the finite field this function is defined on.

Later, Salagean and Ozbudak [21, 24] used discrete derivatives to interpret GAPN properties. We recall their definition.

Definition 6 (Generalized derivative functions)**.** The Generalized derivative of a function $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ in a direction $\alpha \neq 0 \in \mathbb{F}_{p^n}$ is defined as:

$$\nabla_\alpha F(x) := \sum_{i\in\mathbb{F}_p} F(x + i\alpha).$$

Proposition 2. *Let $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ and $\alpha \in \mathbb{F}_{p^n}$. We have the following identities for all $x \in \mathbb{F}_{p^n}$:*

1. $\nabla_\alpha F(x) = \Delta_{\underbrace{\alpha, \alpha, \ldots, \alpha}_{p-1}} F(x)$
2. $\nabla_\alpha F(x) = -\Delta_{\alpha, 2\alpha, \ldots, (p-1)\alpha} F(x)$
3. $\nabla_\alpha F(x) = \sum_{i \in \mathbb{F}_p^*} \Delta_{i\alpha} F(x)$

Proof. 1. See [21, Lemma 1]

2. See [25] for a detailed proof.

3.

$$\begin{aligned}
\sum_{i \in \mathbb{F}_p^*} \Delta_{i\alpha} F(x) &= \sum_{i \in \mathbb{F}_p^*} (F(x + i\alpha) - F(x)) \\
&= (\sum_{i \in \mathbb{F}_p^*} F(x + i\alpha)) - (p-1)F(x) \\
&= (\sum_{i \in \mathbb{F}_p^*} F(x + i\alpha)) + F(x) \\
&= \sum_{i \in \mathbb{F}_p} F(x + i\alpha) \\
&= \nabla_\alpha F(x)
\end{aligned}$$

□

Similarly to the 'regular' differential operation, the generalized differential operations makes the algebraic degree decrease accordingly.

Proposition 3. *Let $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ and $\alpha \in \mathbb{F}_{p^n}^*$. Then,*

$$\deg_A(\nabla_\alpha F) \leq \deg_A(F) - (p-1)$$

We recall here a result, first established by Xiong et al. [27] in order to identify what is the set of derivative functions over $\mathbb{F}_q$.

Theorem 4 ([27] Theorem 1)**.** *Let G be a function over $\mathbb{F}_q$. There is a function F such that*

$$G(x) = \Delta_\alpha F(x) = F(x + \alpha) - F(x),$$

for some $\alpha \in \mathbb{F}_q$, if and only if

$$\nabla_\alpha G(x) = 0, \forall x \in \mathbb{F}_q.$$

In addition to their introduction of generalized derivatives functions, Ozubdak and Salagean [21] also generalized the so-called Extended Affine (EA) equivalence into the Generalized Extended Affine (GEA) equivalence.

Definition 7 ([21] Definition 2)**.** Two functions $F_1, F_2 : \mathbb{F}_q \to \mathbb{F}_q$ are said to be generalized extended affine equivalent (GEA-equivalent), if there exists bijective affine functions $A_1, A_2 : \mathbb{F}_q \to \mathbb{F}_q$ and a function $B : \mathbb{F}_q \to \mathbb{F}_q$, where $\deg_A(B) \leq p - 1$, such that

$$F_1(x) = A_1 \circ F_2 \circ A_2(x) + B(x).$$

Furthermore, Ozbudak and Salagean noticed that the GAPN property is preserved by the GEA equivalence. This property applies to the generalized differential uniformity, and to the algebraic and Hamming degree. We omit the proof of the following proposition as it is similar to the proof concerning the EA-equivalence.

Proposition 5. *Let $F_1, F_2 : \mathbb{F}_q \to \mathbb{F}_q$. If the functions F_1 and F_2 are GEA-equivalent then*

- $\mathcal{U}(F_1) = \mathcal{U}(F_2)$

Moreover, if the functions F_1 and F_2 have an algebraic degree at least $p-1$, then

- $\deg_A(F_1) = \deg_A(F_2)$
- $\deg_H(F_1) = \deg_H(F_2)$

Up to our knowledge, there is no more general equivalence preserving the generalized differential uniformity. In particular, Kuroda and Tsujie [16] noticed that the CCZ-equivalence [6], which corresponds to the affine equivalence of graphs between two functions, does not preserve the generalized differential uniformity. It is well known that the CCZ-equivalence does not necessarily preserve the algebraic and Hamming degree, which is one of the reason why the CCZ-equivalence is more general than the EA-equivalence. It is therefore natural to ask the following question.

Open problem 1. Is there an equivalence of functions that preserves the generalized differential uniformity but does not necessarily preserve the algebraic and/or Hamming degree?

4 Low algebraic degree GAPN functions

Dembowski-Ostrom (DO) polynomials over $\mathbb{F}_{p^n}$ are Hamming Degree 2 polynomials :

$$\sum_{i,j} a_{i,j} x^{p^i+p^j} \in \mathbb{F}_{p^n}[x],$$

which possess numerous algebraic, and combinatorial properties (see [12] for a recent development). Most of the (A)PN functions we know, up to EA-equivalence, are represented by DO polynomials. There exist algorithmic methods to construct quadratic APN functions [28], and only one PN function is not of the DO type [8]. Since the algebraic degree of DO polynomials is also 2, their generalized differentials always vanish in odd characteristic and their study regarding generalized differentials stops there. It is natural to look at the functions of algebraic degree p, the characteristic of the field, which is the lowest algebraic degree for a GAPN function. As expected, a lot of the work regarding the APN properties of DO polynomials in even characteristic extends naturally to the study of the GAPN properties of algebraic degree p functions. In this section we propose to look at some of these connections, and some notable differences.

Definition 8. We call Generalized Dembowski-Ostrom (GDO) polynomials, homogeneous polynomials of algebraic degree p:

$$F(x) = \sum_{i \in I_p} f_i x^i \in \mathbb{F}_{p^n}[x]$$

where

$$I_p = \{\sum_{j=0}^{n-1} i_j p^j \mid 0 \leq i_j \leq p-1 \ \forall 0 \leq j \leq n-1, \ \sum_{j=0}^{p-1} i_j = p\}.$$

From Proposition 3, we can easily see that the generalized derivative functions of a GDO polynomial are affine functions, that is of algebraic degree at most 1. We can actually explicitly give the coefficients of the generalized derivatives of GDO polynomials. We also notice that the generalized derivative functions of GDO polynomials are linearized polynomials.

Lemma 6. *Let p be an odd prime number and $F(x) = \sum_{i=1}^{N} f_i.x^{d_i}$ where $d_i = \sum_{j=0}^{\ell} d_{i,j}p^j$, be a GDO function over $\mathbb{F}_{p^n}$. Then, for every $\alpha \in \mathbb{F}_{p^n}$,*

$$\nabla_\alpha F(x) = \sum_{j=0}^{\ell} g_j^{(F)}(\alpha) x^{p^j}$$

where $g_j^{(F)}(\alpha) = \sum_{i=1}^{N} -d_{i,j} f_i \alpha^{d_i - p^j}$ for every $j \in [0, \ell]$.

Proof. Let $\alpha \in \mathbb{F}_{p^n}^*$, and for $d \in \mathbb{N}$, $M_d : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}, \quad x \mapsto x^d$.
Using the linearity of the derivative :

$$\begin{aligned}
\nabla_\alpha F(x) &= \sum_{i=1}^{N} f_i \nabla_\alpha M_{d_i}(x) \\
&= \sum_{i=1}^{N} f_i (-\sum_{j=0}^{\ell} d_{i,j} \alpha^{d_i - p^j} x^{p^j}) \\
&= \sum_{j=0}^{\ell} (\sum_{i=1}^{N} -f_i d_{i,j} \alpha^{d_i - p^j}) x^{p^j} \\
&= \sum_{j=0}^{\ell} g_j^{(F)}(\alpha) x^{p^j}
\end{aligned}$$

□

4.1 Preliminary results

Before we proceed further into the characterization of GAPN classes of GDO polynomials, we need to introduce a couple of Lemmas that require the concept of modular order of an integer.

Definition 9 (Modular order of an integer)**.** We call the order of an integer i modulo n, the smallest strictly positive integer, denoted $\mathbb{O}_n(i)$, satisfying

$$i^{\mathbb{O}_n(i)} \equiv 1 \pmod{n}.$$

Lemma 7. *Let $n \geq 2$ be an integer, $d \neq 1$ be a divisor of n and p a prime number coprime to n. Then, $\mathbb{O}_d(p) | \mathbb{O}_n(p)$. In particular $\mathbb{O}_d(p) \leq \mathbb{O}_n(p)$.*

Proof. If $n = kd$ for an integer $k \geq 1$, then :

$$\begin{aligned} p^{\mathbb{O}_n(p)} \equiv 1 \pmod{n} &\implies \exists m \in \mathbb{N}^*,\ p^{\mathbb{O}_n(p)} = 1 + nm \\ &\implies p^{\mathbb{O}_n(p)} = 1 + kdm \\ &\implies p^{\mathbb{O}_n(p)} \equiv 1 \pmod{d} \end{aligned}$$

So we have $\mathbb{O}_d(p)|\mathbb{O}_n(p)$, and so $\mathbb{O}_d(p) \leq \mathbb{O}_n(p)$. □

Lemma 8. *Let $n = q_1^{i_1} q_2^{i_2} .. q_s^{i_s}$ be the prime decomposition of an integer n, for some prime numbers $q_1, \ldots, q_s$ and some positive exponents $i_1, \ldots, i_s$. Let also p be a prime number not dividing n. Then,*

$$\min_{i \in \{1,..,s\}} \mathbb{O}_{q_i}(p) = \min_{d>1, d|n} \mathbb{O}_d(p).$$

Proof. If $d|n$, then $\exists i \in \{1, .., s\}$ such that $q_i|d$. From the Lemma 7, we have $\mathbb{O}_{q_i}(p) \leq \mathbb{O}_d(p)$. In particular, $\min\limits_{i \in \{1,..,s\}} \mathbb{O}_{q_i}(p) \leq \mathbb{O}_d(p)$ for every divisor $d > 1$ of n, i.e,

$$\min_{i \in \{1,..,s\}} \mathbb{O}_{q_i}(p) \leq \min_{d>1, d|n} \mathbb{O}_d(p)$$

As $\{\mathbb{O}_{q_1}, .., \mathbb{O}_{q_s}(p)\} \subset \{\mathbb{O}_d(p) \mid d > 1 \text{ divides } n\}$, we have

$$\min_{i \in \{1,..,s\}} \mathbb{O}_{q_i}(p) = \min_{d>1, d|n} \mathbb{O}_d(p)$$

□

Lemma 9. *Let q and p be two different prime numbers. We have, for all integers $n, m \geq 1$,*

$$\mathbb{O}_q(p^n) \leq \mathbb{O}_q(p) \leq \mathbb{O}_{q^m}(p).$$

If $u_{m,n}(q,p) = \mathbb{O}_{q^m}(p^n)$, then $(u_{m,*}(q,p))_m$ is an increasing sequence and $(u_{*,n}(q,p))_n$ is a decreasing one.

Since our study also makes use of cyclotomic polynomials, we recall the following definition from [17].

Definition 10 (**d-th cyclotomic polynomial**)**.** Let d be a positive integer not divisible by a prime p and ζ a primitive d-th root of unity over $\mathbb{F}_{p^n}$. Then the polynomial

$$Q_d(x) := \prod_{\substack{s=1,\ldots,d \\ gcd(s,d)=1}} (x - \zeta^s)$$

is called the d-th cyclotomic polynomial over $\mathbb{F}_{p^n}$.

Later, we will use the following result, inspired directly from [17, Theorem 2.47].

Lemma 10. *Let $Q_d(x) \in \mathbb{F}_p[x]$ be the d-th cyclotomic polynomial such that $d \not\equiv 0 \pmod{p}$. Then $Q_d(x)$ factors into $\phi(d)/\mathbb{O}_d(p)$, where ϕ is the Euler characteristic, distinct monic irreducible polynomials in $\mathbb{F}_p[x]$ of the same polynomial degree $\mathbb{O}_d(p)$.*

We also need the following necessary and sufficient criteria for monomial functions of the GDO type to be GAPN functions due to Kuroda [15]. However, we use the equivalent statement made by Ozbudak and Salagean [21] which is more practical for us to use.

Lemma 11 ([21] Theorem 1)**.** *Let $F(x) = x^e \in \mathbb{F}_{p^n}[x]$ a GDO polynomial, where $e = \sum_{i=0}^{\ell} k_i.p^i$, $k_0 \neq 0$ and $k_\ell \neq 0$. Then, F is a GAPN function over $\mathbb{F}_{p^n}$ if and only if*

$$gcd(\sum_{i=0}^{\ell} k_i.z^i, z^n - 1) = z - 1 \quad in \quad \mathbb{F}_p[z].$$

4.2 About the GDO monomials which are GAPN functions

In [15], Kuroda showed that every monomial GDO over an extension field $\mathbb{F}_{p^n}$ is a GAPN function over some extension of $\mathbb{F}_{p^n}$. He also showed that every monomial GDO is p-exceptional GAPN function, i.e. it is a GAPN function over an infinite amount of extension field $\mathbb{F}_{p^n}$. Table 1 recapitulate all known GDO monomials which are GAPN functions, including our results. In what follows, we give a way to find, for every monomial GDO function, an infinite number of extensions, with an explicit formula for the extension degree, where this function is a GAPN one.

This first result gives sufficient conditions for a GDO monomial to be GAPN.

Theorem 12. *Let an exponent $e = \sum_{i=0}^{\ell} k_i p^i$ such that $F(x) = x^e$ is of the GDO type over $\mathbb{F}_{p^n}$ and let $n = q_1^{i_1}..q_s^{i_s}$ be the prime decomposition of n. We have two cases :*

1. *$n \not\equiv 0 \pmod p$: If $\ell \leq \min_{1 \leq i \leq s} \mathbb{O}_{q_i}(p)$, then F is a GAPN function.*
2. *$n \equiv 0 \pmod p$: If $\ell \leq \min_{1 \leq i \leq s,\ q_i \neq p} \mathbb{O}_{q_i}(p)$ or $n = p^\alpha$, and if the multiplicity of 1 as a root in $\sum_{i=0}^{\ell} k_i x^i \in \mathbb{F}_p[x]$ is equal to 1, then F is a GAPN function.*

Proof. Let $g(x) = \sum_{i=0}^{\ell} k_i x^i \in \mathbb{F}_p[x]$, and let $R(x) := gcd(g(x), x^n - 1) \in \mathbb{F}_p[x]$. We already know from Lemma 11 that F is a GAPN function if and only if $R(x) = x - 1$.

1. When $n \not\equiv 0 \pmod p$, we have that (see [17, Theorem 2.45])

$$x^n - 1 = (x - 1) \prod_{d>1,\ d|n} Q_d(x),$$

where $Q_d(x) \in \mathbb{F}_p[x]$ is the d-th cyclotomic polynomial (see Definition 10).

Since $g(1) = \sum_{i=0}^{\ell} k_i = p \equiv 0 \pmod p$, we can factorize $g(x)$ by $(x-1)^m$ where $m \geq 1$ is the multiplicity of 1 as a root of $g(x)$. In other words, there exists $V(x) \in \mathbb{F}_p[x]$, $V(1) \neq 0$ such that

$$g(x) = (x - 1)^m \times V(x).$$

Hence

$$R(x) = (x - 1) \times gcd(V(x), \prod_{d>1,\ d|n} Q_d(x))$$

A sufficient condition to have the later is to force every irreducible factor of $\prod_{d>1,\ d|n} Q_d(x)$ in $\mathbb{F}_p[x]$ to have degree greater (strictly) than the degree of $V(x)$. We ensure it using Lemma 10, i.e. we must have

$$\mathbb{O}_d(p) > deg(V(x)) = \ell - m$$

for every $d > 1$ dividing n. In particular, if $\mathbb{O}_d(p) \geq \ell$, then we have $\mathbb{O}_d(p) > \ell - m$ because $m > 0$.
So, if $\ell \leq \min(\{\mathbb{O}_d(p) \mid d > 1 \text{ divide } n\})$, then F is a GAPN function over $\mathbb{F}_{p^n}$.
And, by the Lemma 8, we have $\min(\{\mathbb{O}_d(p) \mid d > 1 \text{ divide } n\}) = \min\limits_{1\leq i\leq s} \mathbb{O}_{q_i}(p)$.

2. In this case, we can write $n = v.p^u$ where $gcd(p, v) = 1$ and $u \in \mathbb{N}^*$.
We have

$$x^n - 1 = (x^v - 1)^{p^u}$$

i.e,

$$x^n - 1 = (x-1)^{p^u}. \prod_{d>1,d|v} Q_d(x)^{p^u}$$

A way to get $R(x) = x - 1$ is that the multiplicity of 1 in $g(x)$ is equal to 1 and that the degree of $Q_d(X)$ for $d > 1$ and $d|n$ is greater (strictly) to $deg(V) \leq \ell - 1$.

□

Remark 2. The result of this theorem remains true when $p = 2$. Notably:
Let $F(x) = x^{2^\ell+1}$. F is APN over $\mathbb{F}_{2^n}$ if and only if $gcd(x^\ell - 1, x^n - 1) = x - 1 \in \mathbb{F}_2[x]$. And we proceed as in the proof.

Proposition 13. *Let p be a prime number and $n = q_1^{i_1}..q_s^{i_s} \not\equiv 0 \pmod p$ an integer with his prime decomposition. For every integer $\ell \leq n - 1$, if $\min\limits_{1\leq i\leq s} \mathbb{O}_{q_i}(p) \geq \ell$, then $gcd(n, \ell) = 1$.*

Proof. We always have :

$$gcd(x^\ell - 1, x^n - 1) = x^{gcd(\ell,n)} - 1 \in \mathbb{F}_p[x].$$

And, with the conditions in the Theorem 12, we have $gcd(x^\ell - 1, x^n - 1) = x - 1 \in \mathbb{F}_p[x]$. □

Remark 3. The proposition above shows that when $p = 2$, some of the Gold functions, i.e. quadratic APN monomial functions [20], are obtained by our method in Theorem 12.

We can illustrate the first point of Theorem 12 by giving some examples. We first fix an odd prime number p and an integer $\ell \geq 2$. We then find some integers $k_0, .., k_\ell$ such that $0 \leq k_i \leq p-1$ for every $0 \leq i \leq \ell$ and $\sum_{i=0}^{\ell} k_i = p$. Let $e = \sum_{i=0}^{\ell} k_i p^i$. From Theorem 12 we can find precisely the extensions where $F(x) = x^e$ is a GAPN function.

Example 2. Let $p = 5$ and $\ell = 2$. The functions $F(x) = x^e$ where

$$e \in \{p^2 + p + 3, p^2 + 2p + 2, 3p^2 + p + 1, 2p^2 + p + 2\}$$

are all GAPN over $\mathbb{F}_{5^n}$ with $n = q_1^{i_1}..q_s^{i_s}$, and where $q_1, .., q_s$ are odd primes different from 5 and such that $\min\limits_{1\leq i\leq s} \mathbb{O}_{q_i}(5) \geq 2$. As a simple case, they are GAPN functions over $\mathbb{F}_{5^3}$ because $\mathbb{O}_3(5) = 2 = \ell$.

We can use the second point of Theorem 12 to construct GAPN functions as well. We first fix a prime number p and an integer $\ell \geq 2$. Then, we find $k_1, .., k_\ell$ such that $0 \leq k_i \leq p-1$ for every $0 \leq i \leq \ell$ and $\sum_{i=0}^{\ell} k_i = p$. We are looking for extensions $\mathbb{F}_{p^n}$ where the monomial GDO $F(x) = x^{\sum_{i=0}^{\ell} k_i p^i}$ is GAPN. Let us denote

$$V(x) := \frac{\sum_{i=0}^{\ell} k_i . x^i}{x-1} \in \mathbb{F}_p[x]$$

and suppose that it verifies $V(1) \neq 0$, i.e. 1 has a multiplicity exactly one as a root of $\sum_{i=0}^{\ell} k_i x^i \in \mathbb{F}_p[x]$. Then, from point 2 of Theorem 12, we can find extensions of $\mathbb{F}_p$ where the GDO function $F(x) = x^{\sum_{i=0}^{\ell} k_i . p^i}$ is GAPN. For example :

Example 3. Let $p = 7$ and $\ell = 4$. Using the same notations as in Theorem 12:

1. Let $g(x) = x^4 + 2x^3 + 3x^2 + 1 \in \mathbb{F}_7[x]$.
   We have :
   - $g(1) = 1 + 2 + 3 + 1 = 7 = 0$,
   - $V(x) = \frac{g(x)}{x-1} = x^3 + 3x^2 + 6x + 6$,
   - $V(1) = 1 + 3 + 6 + 6 = 16 = 2 \neq 0$.
2. Let $g(x) = 2x^4 + 3x^3 + x^2 + 1 \in \mathbb{F}_7[x]$.
   We have :
   - $g(1) = 2 + 3 + 1 + 1 = 7 = 0$,
   - $V(x) = \frac{g(x)}{x-1} = 2x^3 + 5x^2 + 6x + 6$,
   - $V(1) = 2 + 5 + 6 + 6 = 19 = 5 \neq 0$.

We conclude that the functions $F(x) = x^e$, where

$$e \in \{p^4 + 2p^3 + 3p^2 + 1 (= 3235), 2p^4 + 3p^3 + p^2 + 1 (= 5881)\}$$

are GAPN over $\mathbb{F}_{7^{7^\alpha \times N}}$ with $N = q_1^{i_1}..q_s^{i_s}$, where the primes $q_1, .., q_s$ are different from 7, $(i_1, .., i_s) \in \mathbb{N}^s$ and such that $i_1 = .. = i_s = 0$ or $\min\limits_{1 \leq i \leq s} \mathbb{O}_{q_i}(7) \geq 4$.
As a simple case, they are GAPN over $\mathbb{F}_{7^{7 \times 5}}$: $\mathbb{O}_5(7) = 4 = \ell$. From Theorem 12, we can confirm that these functions are GAPN over all the extensions $\mathbb{F}_{7^{7^\alpha \times 5^\beta}}$ for every $(\alpha, \beta) \in \mathbb{N}^* \times \mathbb{N}$.

Now we give some examples in the case $p = 2$. The first one illustrates the first point of Theorem 12 while the second illustrates the second point of the same theorem.

Example 4. Let $\ell = 3$.

- Let $F(x) = x^{2^3+1}$. Then, using the first point of Theorem 12, we only have to find odd primes $q_1, .., q_s$ such that $\min\limits_{1 \leq i \leq s} \mathbb{O}_{q_i}(2) \geq 3$, and we will be sure that F is APN over any extension $\mathbb{F}_{2^n}$ where $n = q_1^{i_1}..q_s^{i_s}$ and $(i_1, .., i_s) \neq (0, .., 0)$. For example, if we take $n = 7$, then F is APN over $\mathbb{F}_{2^7}$ (more generally, over $\mathbb{F}_{2^{7^\alpha}}$, $\alpha \in \mathbb{N}^*$) : In fact, $\mathbb{O}_7(2) = 6 \geq 3$.

- Let $F(x) = x^{2^3+1}$. Then :
  - $g(x) = x^3 + 1$,
  - $g(1) = 2 = 0$,
  - $V(x) = x^2 + x + 1$,
  - $V(1) = 1 + 1 + 1 = 3 = 1 \neq 0$,

  We conclude that F is APN over $\mathbb{F}_{2^{2^\alpha \cdot n}}$ where $\alpha \in \mathbb{N}^*$, $n \in \{1, q_1^{i_1} \times .. \times q_s^{i_s}\}$ and such that $\min\limits_{1 \leq i \leq s} \mathbb{O}_{q_i}(2) \geq 3$

In order to give a sufficient condition for a GDO monomial to be a GAPN function over $\mathbb{F}_{p^n}$ when n is even and p is odd, one sees that the exponent must satisfy some additional criteria. First we state the following lemma and leave the proof as an exercise.

Lemma 14. *Let p be an odd prime number, and consider the polynomial $g(x) = \sum_{i=0}^{\ell} k_i.x^i \in \mathbb{Z}[x]$ where $0 \leq k_i \leq p-1$ for all $0 \leq i \leq \ell$ and $\sum_{i=0}^{\ell} k_i = p$. Then, $g(-1) = 0 \pmod p$ if and only if either $k_{2j} = 0$ for all $j \geq 0$ or $k_{2j+1} = 0$ for all $j \geq 0$.*

The following theorem gives other sufficient conditions for a monomial GDO function to be GAPN, that are not covered by Theorem 12, notably when the extension of the field is even.

Theorem 15. *Let p be an odd prime, and let $n = 2N \not\equiv 0 \pmod p$ where $N \geq 3$ is an odd integer. Let an exponent $e = \sum_{i=0}^{\ell} k_i p^i$ such that $F(x) = x^e$ is of the GDO type, and where it exist $0 \leq i, j \leq \ell$ such that $k_{2i} \neq 0$ and $k_{2j+1} \neq 0$. If*

$$N = q_2^{i_2}..q_m^{i_m} \text{ and } \ell \leq \min_{2 \leq i \leq m} \mathbb{O}_{q_i}(p),$$

then $F(x) = x^e$ is a GAPN function over $\mathbb{F}_{p^n}$.

Proof. Recall that $n = 2N$. Suppose that $\ell \leq \min\limits_{2 \leq i \leq m} \mathbb{O}_{q_i}(p)$.

Let $g(x) = \sum_{i=0}^{\ell} k_i x^i \in \mathbb{F}_p[x]$. We have that

$$x^n - 1 = x^{2N} - 1 = (x-1)(x+1) \prod_{d|N,\ d>1} Q_{2d}(x)$$

Since $g(1) = \sum_{i=0}^{\ell} k_i = p \equiv 0 \pmod p$, we can factorize $g(x)$ by $(x-1)^m$ where $m \geq 1$ is the multiplicity of 1 as a root of $g(x)$. In other words, there exists $V(x) \in \mathbb{F}_p[x]$, $V(1) \neq 0$ such that

$$g(x) = (x-1)^m \times V(x).$$

Hence, as $V(-1) \neq 0$ because of the choice of e (Lemma 14), we have :

$$gcd(g(x), x^{2N} - 1) = (x-1) \times gcd(V(x), \prod_{d|N,\ d>1} Q_{2d}(x)).$$

From the Lemma 7, we have that $\mathbb{O}_{2d}(p) \geq \mathbb{O}_d(p) \geq \ell > deg(V(x))$ for every divisor $d \neq 1$ of N, i.e,

$$\begin{aligned} gcd(g(x), x^{2N} - 1) &= (x-1) \times gcd(V(x), \prod_{d|N,\ d>1} Q_{2d}(x)) \\ &= (x-1). \end{aligned}$$

We end the proof using Lemma 11. □

Remark 4. This approach cannot be generalized to $n = 2^a N$ with $a > 1$. The only result that we can get from this approach is that $F(x) = x^{ip+p-i}$ is always GAPN for every $1 \leq i \leq p-1$, which is already known (special case of [24, Theorem 2]). This is because $\mathbb{O}_2(p) = 1$ for any odd prime number p.

Our results in Theorem 12 and Theorem 15 are independent of the multiplicity m of 1 as a root in $g(x) = \sum_{i=0}^{\ell} k_i x^i \in \mathbb{F}_p[x]$, except for the second point of Theorem 22. But as we showed in the proofs of these two theorems, we can have a way to get more extensions where a monomial GDO is GAPN using the condition $\min_{2 \leq i \leq \ell} \mathbb{O}_{q_i}(p) \geq \ell - m + 1$ whish depends on m. For example we have the following result.

Corollary 1. *$g(x) = \sum_{i=0}^{\ell} k_i.x^i \in \mathbb{Z}[x]$ such that $\sum_{i=0}^{\ell} k_i = p$ (and $0 \leq k_i \leq p-1$). If the multiplicity of 1 as a root in $g \pmod p$ is ℓ, then $F(x) = x^{g(p)}$ is a GAPN function over $\mathbb{F}_{p^n}$ for $n > \ell$ if and only if $n \not\equiv 0 \pmod p$.*

Proof. Let $F(x) = x^{g(p)}$ and $R(z) = gcd(g(z), z^n - 1) \in \mathbb{F}_p[z]$ where $n > \ell$. F is a GAPN function over $\mathbb{F}_{p^n}$ if and only if

$$R(z) = z - 1.$$

As $g(z) = k_\ell (z-1)^\ell$, we have $R(z) = gcd((z-1)^\ell, z^n - 1)$. And $R(z) = z - 1 \in \mathbb{F}_p[z]$ if and only if the multiplicity of 1 as a root in $z^n - 1$ is exactly 1, i.e. if and only if $n \not\equiv 0 \pmod p$. □

Example 5. The functions $F(x) = x^{ip^2+(p-2i)p+i}$ where $i \in \{1, .., \frac{p-1}{2}\}$ are GAPN over $\mathbb{F}_{p^n}$ for every $n \geq 3$ such that $n \not\equiv 0 \pmod p$.

Example 6. The function $F(x) = x^{1+p+..+p^{p-1}}$ is a GAPN function over $\mathbb{F}_{p^n}$ for every $n \geq p$ such that $n \not\equiv 0 \pmod p$.
In fact, $(x-1)^p = x^p - 1 = (x-1)(1 + x + .. + x^{p-1})$, i.e, $1 + x + .. + x^{p-1} = (x-1)^{p-1}$, i.e, the multiplicity of 1 as a root of $1 + x + .. + x^{p-1}$ is exactly $p - 1$.

Remark 5. An important thing about Theorem 12 and Theorem 15 is that we only care about the primes $q_1, .., q_s$ in the prime decomposition of n. If these prime numbers satisfy the conditions, then the same function will be GAPN over any extension $\mathbb{F}_{p^m}$ where $m = q_1^{i_1}..q_s^{i_s}$ for every $(i_1, .., i_s) \in \mathbb{N}^s \backslash \{(0, .., 0)\}$.

In the next Theorem, we present a specific case of a GDO monomials with a low polynomial degree and their sufficient and necessary conditions to be GAPN functions.

Theorem 16. *Let $F(x) = x^e$ a function over $\mathbb{F}_{p^n}$ where $e = a_2 p^2 + a_1 p + a_0$ and $a_2 + a_1 + a_0 = p$. Let $n = p^\alpha \times N$ where $\alpha \geq 0$ and $gcd(N, p) = 1$.*
Then, F is GAPN over $\mathbb{F}_{p^n}$ if and only if either

- *$a_0^N \neq a_2^N$ or*
- *$a_0 = a_2$ and $\alpha = 0$.*

Proof. The p-polynomial $\nabla_1 F(x)$ has p-associate polynomial

$$\begin{aligned} g(x) &= -(a_2 x^2 - (a_0 + a_2)x + a_0) \\ &= -a_2 (x-1)(x - \frac{a_0}{a_2}) \end{aligned}$$

From [23, Theorem 1], we know that F is a GAPN function over $\mathbb{F}_{p^n}$ if and only if $gcd(x^n - 1, g(x)) = x - 1$ in $\mathbb{F}_p[x]$.

- If $n \not\equiv 0 \pmod{p}$: $x^n - 1 = (x-1).\prod_{d|n \ d>1} Q_d(x)$. So, the condition is verified if and only if $\frac{a_0}{a_2}$ is not an n-th root of unity different from 1.
- If $n \equiv 0 \pmod{p}$, then $x^n - 1 = (x-1)^{p^u}.\prod_{d|v \ d>1} Q_d(x)^{p^u}$ where $n = vp^u$ and $gcd(v,p) = 1$. In this case, the condition in [24, Theorem 1] is verified if and only if 1 is a simple root of g and $\frac{a_0}{a_2}$ is not a v-root of unity.

□

4.3 Some GDO multinomials that are GAPN functions

We are now interested in GAPN functions represented by non monomial GDO polynomials. As already stated, in order to know if a function represented by a GDO polynomial is a GAPN function, one might study the kernel of its generalized derivative functions, which are linearized functions.

Hence, we first recall a result of McGuire and Sheekey [18] on the number of roots of linearized polynomials over extensions of $\mathbb{F}_p$. They give a full description of these roots. From this result, we draw classes of non-monomial GAPN functions with an algebraic degree p.

Theorem 17 ([18] Theorem 5)**.** *Let $L(x) = \sum_{i=0}^{\ell} a_i x^{p^i} \in \mathbb{F}_{p^n}[x]$ be a linearized polynomial where $a_\ell \neq 0$. Let*

$$C^{(p^i)}(L) := \begin{bmatrix} 0 & 0 & \dots & 0 & -\left(\frac{a_0}{a_\ell}\right)^{p^i} \\ 1 & 0 & \dots & 0 & -\left(\frac{a_1}{a_\ell}\right)^{p^i} \\ \vdots & \vdots & \ddots & 0 & \vdots \\ 0 & 0 & \dots & 1 & -\left(\frac{a_{\ell-1}}{a_\ell}\right)^{p^i} \end{bmatrix}, \quad i \in \{0, 1, .., n-1\}$$

And

$$A(L) := \prod_{i=0}^{n-1} C^{(p^i)}(L).$$

Then, the number of roots of L in $\mathbb{F}_{p^n}$ is exactly p^d where $d = dim_{\mathbb{F}_p}(ker(A(L) - I_\ell))$, and I_ℓ is the identity matrix of size ℓ.

Using the results and notation from Lemma 6 about the coefficients of the generalized derivative functions of a GDO polynomial, and Theorem 17 above about the roots of these linearized derivatives functions, we have the following characterization.

Theorem 18. *Let p be an odd prime number and $F(x) = \sum_{i=1}^{N} f_i.x^{d_i}$ be a GDO function over $\mathbb{F}_{p^n}$ where $d_i = \sum_{j=0}^{\ell} d_{i,j} p^j$.*
F is GAPN over $\mathbb{F}_{p^n}$ if and only if the two following conditions hold :

- *$g_1^{(F)}, \dots, g_\ell^{(F)}$ have no nonzero roots in common.*

- $\forall \alpha \in \mathbb{F}_{p^n}^*$, *let* $t_\alpha \in \{0, \dots, \ell\}$ *the greatest integer such that* $g_{t_\alpha}^{(F)}(\alpha) \neq 0$. *The second condition is:*

$$\dim_{\mathbb{F}_p}(\ker(A(\nabla_\alpha F) - I_{t_\alpha})) = 1 \quad \forall \alpha \in \mathbb{F}_{p^n}^*$$

where

$$A(\nabla_\alpha F) := \prod_{i=0}^{n-1} C^{(p^i)}(\nabla_\alpha F)$$

and

$$C^{(p^i)}(\nabla_\alpha F) := \begin{bmatrix} 0 & 0 & \dots & 0 & -\left(\frac{g_0^{(F)}(\alpha)}{g_{t_\alpha}^{(F)}(\alpha)}\right)^{p^i} \\ 1 & 0 & \dots & 0 & -\left(\frac{g_1^{(F)}(\alpha)}{g_{t_\alpha}^{(F)}(\alpha)}\right)^{p^i} \\ & & \ddots & & \vdots \\ 0 & 0 & \dots & 1 & -\left(\frac{g_{t_\alpha-1}^{(F)}(\alpha)}{g_{t_\alpha}^{(F)}(\alpha)}\right)^{p^i} \end{bmatrix} \in \mathbb{F}_{p^n}^{t_\alpha \times t_\alpha}$$

Proof. Let $\alpha \in \mathbb{F}_{p^n}^*$. From Lemma 6 we have

$$\nabla_\alpha F(x) = \sum_{j=0}^{\ell} g_j^{(F)}(\alpha) x^{p^j}.$$

If $g_0^{(F)}$, $g_1^{(F)}$,.., $g_\ell^{(F)}$ have a common root $\alpha \neq 0$, then we have $\nabla_\alpha F(x) = 0$ for every $x \in \mathbb{F}_{p^n}$, i.e. F is not GAPN.
Else, if $g_0^{(F)}$, $g_1^{(F)}$,.., $g_\ell^{(F)}$ have no nonzero common roots, then for any $\alpha \in \mathbb{F}_{p^n}^*$, there exits $t_\alpha \in \{0, 1, .., \ell\}$ such that t_α is the greatest possible value verifying $g_{t_\alpha}^{(F)}(\alpha) \neq 0$.
Therefore we can rewrite

$$\nabla_\alpha F(x) = \sum_{j=0}^{t_\alpha} g_j^{(F)}(\alpha) x^{p^j}.$$

We can apply Theorem 17 for any $\alpha \in \mathbb{F}_{p^n}^*$ to say that $\nabla_\alpha F(x)$ has p roots in $\mathbb{F}_{p^n}$ if and only if $\dim_{\mathbb{F}_p}(\ker(A(\nabla_\alpha F) - I_{t_\alpha})) = 1$. □

Remark that Theorem 18 applies to any GDO polynomial. We can specify this result into another necessary and sufficient conditions for a GDO monomial to be a GAPN function using companion matrices.

Corollary 2. *Let* $F(x) = x^d$ *a monomial GDO function where* $d = \sum_{i=0}^{\ell} k_i.p^i$ *and* $k_\ell \neq 0$.
Let

$$C := \begin{bmatrix} 0 & 0 & \dots & 0 & -\frac{k_0}{k_\ell} \\ 1 & 0 & \dots & 0 & -\frac{k_1}{k_\ell} \\ \vdots & \vdots & \ddots & 0 & \vdots \\ 0 & 0 & \dots & 1 & -\frac{k_{\ell-1}}{k_\ell} \end{bmatrix} \in \mathbb{F}_p^{\ell \times \ell}$$

Then, the function F *is GAPN over* $\mathbb{F}_{p^n}$ *if and only if* $\dim_{\mathbb{F}_p}(\ker(C^n - I_\ell)) = 1$.

Proof. For the monomial case, we have already seen that a GDO function F is GAPN if and only if $\nabla_1 F(x) = 0$ has exactly p solutions. As $\nabla_1 F(x) = -\sum_{i=0}^{\ell} k_i x^{p^i} \in \mathbb{F}_p[x]$, we end the proof using Theorem 18. □

Similarly, we can use the notations previously introduced to re-interpret the following results from McGuire and Sheekey [18].

Lemma 19 ([18] Theorem 7)**.** *Let $L(x) = \sum_{i=0}^{\ell} a_i.x^{p^i}$ a $\mathbb{F}_p$-function over $\mathbb{F}_{p^n}$ where $f_\ell \neq 0$ and $f_0 \neq 0$. L has p^ℓ roots in $\mathbb{F}_{p^n}$ if and only if $C^{(1)}(L) \times C^{(p)}(L) \times \cdots \times C^{(p^{n-1})}(L) = I_\ell$ where :*

$$C^{(p^i)}(L) = \begin{bmatrix} 0 & 0 & \dots & 0 & -\left(\frac{a_0}{a_\ell}\right)^{p^i} \\ 1 & 0 & \dots & 0 & -\left(\frac{a_1}{a_\ell}\right)^{p^i} \\ \vdots & \vdots & \ddots & 0 & \vdots \\ 0 & 0 & \dots & 1 & -\left(\frac{a_{\ell-1}}{a_\ell}\right)^{p^i} \end{bmatrix} \in \mathbb{F}_{p^n}^{\ell \times \ell}$$

Using the above result, we can now give a necessary and sufficient condition for a certain type of multinomial GDO functions with low Hamming degree (i.e. 3) and relatively low polynomial degree, to be GAPN functions.

Theorem 20. *Let p be an odd prime number, and let $F(x) = \sum_{i=1}^{N} f_i.x^{d_i} \in \mathbb{F}_{p^n}[x]$ be a GDO polynomial where the exponents d_i are of the form:*

$$d_i = d_{i,0} + d_{i,1}.p + d_{i,2}.p^2$$

and such that the polynomials $g_0^{(F)}, g_1^{(F)}$ and $g_2^{(F)}$ have no common roots in $\mathbb{F}_{p^n}^*$.
For any $\alpha \in \mathbb{F}_{p^n}^*$ such that $g_2^{(F)}(\alpha) \neq 0$, we have the matrices:

$$C^{(p^i)}(\nabla_\alpha F) := \begin{bmatrix} 0 & -\left(\frac{g_0^{(F)}(\alpha)}{g_2^{(F)}(\alpha)}\right)^{p^i} \\ 1 & -\left(\frac{g_1^{(F)}(\alpha)}{g_2^{(F)}(\alpha)}\right)^{p^i} \end{bmatrix}.$$

Then, F is a GAPN function over $\mathbb{F}_{p^n}$ if and only if

$$C^{(1)}(\nabla_\alpha F) \times C^{(p)}(\nabla_\alpha F) \times \cdots \times C^{(p^{n-1})}(\nabla_\alpha F) \neq I_2$$

for all such suitable α.

Proof. Let $\alpha \in \mathbb{F}_{p^n}^*$.

If $g_i^{(F)}(\alpha) = 0$ for every $i \in \{0, 1, 2\}$, then, from the formula in the proposition 13, $\nabla_\alpha F(x) = 0$ for every $x \in \mathbb{F}_{p^n}$. Then F is not a GAPN function over $\mathbb{F}_{p^n}$.

Otherwise, we have two cases depending on the value of $g_2^{(F)}(\alpha)$.

1. If $g_2^{(F)}(\alpha) = 0$, then, $\nabla_\alpha F(x)$ is a function of polynomial degree $\deg_P(\nabla_\alpha F) \leq p$, that is it has at most p roots.

2. If $g_2^{(F)}(\alpha) \neq 0$, then applying the result from Lemma 19, $\nabla_\alpha F(x)$ has strictly less than p^2 roots in $\mathbb{F}_{p^n}$ if and only if

$$C^{(1)}(\nabla_\alpha F) \times C^{(p)}(\nabla_\alpha F) \times \cdots \times C^{(p^{n-1})}(\nabla_\alpha F) \neq I_2. \tag{1}$$

Moreover since F is a GDO function, $\nabla_\alpha F(\alpha) = 0$ always. So, $\nabla_\alpha F(x)$ has exactly p roots in $\mathbb{F}_{p^n}$ if and only if Inequality (1) is satisfied.

□

From this Theorem, we can extract a sufficient condition for such functions to be GAPN by using the fact that if the determinant is not 1, then the product of matrices cannot be the identity matrix.

Corollary 3. *Let p be an odd prime number, $n \geq 3$, and let $F(x) = \sum_{i=1}^{N} f_i.x^{d_i} \in \mathbb{F}_{p^n}[x]$ be a GDO polynomial where $d_i = \sum_{j=0}^{2} d_{i,j}p^j$.*
Suppose that the equation:

$$N_n(g_2^{(F)}(X)) - N_n(g_0^{(F)}(X)) = 0$$

has no solutions in $\mathbb{F}_{p^n}^*$, where $N_n(x) = x^{\frac{p^n-1}{p-1}}$ is the absolute norm. Then, F is a GAPN function over $\mathbb{F}_{p^n}$.

Proof. If defined, the determinant of $C^{(p^i)}(\nabla_\alpha F)$ is $\left(g_0^{(F)}(\alpha)/g_2^{(F)}(\alpha)\right)^{p^i}$ and so

$$det\left(C^{(1)}(\nabla_\alpha F) \times C^{(p)}(\nabla_\alpha F) \times \cdots \times C^{(p^{n-1})}(\nabla_\alpha F)\right) = N_n\left(\frac{g_0^{(F)}(\alpha)}{g_2^{(F)}(\alpha)}\right).$$

Now if $N_n(g_2^{(F)}(\alpha)) - N_n(g_0^{(F)}(\alpha)) = 0$, then

$$det\left(C^{(1)}(\nabla_\alpha F) \times C^{(p)}(\nabla_\alpha F) \times \cdots \times C^{(p^{n-1})}(\nabla_\alpha F)\right) \neq 1,$$

and this product of matrices cannot equate the identity matrix. We conclude using Theorem 20.
□

We use this last corollary to give the following criteria about GDO polynomial with only one exponent of Hamming degree 3.

Theorem 21. *Let p be an odd prime number, $n \geq 3$, and let $F(x) \in \mathbb{F}_{p^n}[x]$ be the GDO polynomial*

$$F(x) = x^d + \sum_{i \in \mathbb{F}_p^*} \lambda_i.x^{k_i},$$

where $d = d_2p^2 + (p - (d_0 + d_2))p + d_0$, $d_2 \neq 0$ and $k_i = (p-i)p + i$.
If

$$N_n(\frac{d_0}{d_2} + \sum_{i \in \mathbb{F}_p^*} \lambda_i.\frac{i}{d_2}\alpha^{k_i - d}) \neq 1 \quad \forall \alpha \in \mathbb{F}_{p^n}^*,$$

then F is a GAPN function over $\mathbb{F}_{p^n}$.

Proof. Using Lemma 6, we can compute $g_0^{(F)}(\alpha)$ and $g_2^{(F)}(\alpha)$, and we get:

$$g_0^{(F)}(\alpha) = -d_0\alpha^{d-1} - \sum_{i\in\mathbb{F}_p^*} i.\lambda_i\alpha^{k_i-1}$$
$$g_2^{(F)}(\alpha) = -d_2\alpha^{d-p^2}$$

As $g_2^{(F)}(\alpha)$ is a monomial in α, it has only one root in $\mathbb{F}_{p^n}$, which is 0. Thus $g_0^{(F)}$, $g_1^{(F)}$ and $g_2^{(F)}$ have no common roots in $\mathbb{F}_{p^n}^*$.
From Corollary 3, if $N_n(g_2^{(F)}(\alpha)) - N_n(g_2^{(F)}(\alpha)) \neq 0$ for all $\alpha \in \mathbb{F}_{p^n}^*$, then F is GAPN over $\mathbb{F}_{p^n}$. We have

$$\begin{aligned}
N_n(g_2^{(F)}(\alpha)) - N_n(g_2^{(F)}(\alpha)) \neq 0 &\iff N_n(d_2\alpha^{d-p^2}) \neq N_n(d_0\alpha^{d-1} + \sum_{i\in\mathbb{F}_p^*} i.\lambda_i\alpha^{k_i-1}) \\
&\iff N_n(d_0).N_n(\alpha)^{d-p^2} \neq N_n(\alpha^{d-1})N_n(d_0 + \sum_{i\in\mathbb{F}_p^*} i.\lambda_i\alpha^{k_i-d}) \\
&\iff N_n(d_0)N_n(\alpha)^{1-1} \neq N_n(\alpha)^{d-1}N_n(d_0 + \sum_{i\in\mathbb{F}_p^*} i.\lambda_i\alpha^{k_i-d}) \\
&\iff N_n(d_0) \neq N_n(\alpha)^{1-1}N_n(d_0 + \sum_{i\in\mathbb{F}_p^*} i.\lambda_i\alpha^{k_i-d}) \\
&\iff 1 \neq N_n(\frac{d_0}{d_2} + \sum_{i\in\mathbb{F}_p^*} \frac{i}{d_2}.\lambda_i\alpha^{k_i-d})
\end{aligned}$$

□

As we already see, we can use Theorem 17 and Lemma 19 to have many criteria to find GDO multinomials who are combinations of GDO monomials with exponents of the form $d_2p^2+d_1p+d_0$. As further demonstration, we deduce the following sufficient condition for GDO binomials.

Corollary 4. *Let p be an odd prime number, $n \geq 3$, and let*

$$F(x) = x^{(p-d_0)p^2+d_0p} + \lambda x^{k_0p+(p-k_0)} \in \mathbb{F}_{p^n}[x]$$

be a GDO binomial where $\lambda \in \mathbb{F}_{p^n}^*$. If $N_n(\lambda\frac{k_0}{d_0}) \neq 1$, then F is a GAPN function over $\mathbb{F}_{p^n}$.

Proof. Denote $d = (p-d_0)p^2 + d_0p$ and $k = k_0p + (p-k_0)$. From Lemma 6 we have that

$\nabla_\alpha F(x) = d_0\alpha^{d-p^2}x^{p^2} - g_1^F(\alpha)x^p + \lambda k_0\alpha^{k-1}x$. We also have

$$\begin{aligned}
N_n(g_0^F(\alpha)) = N_n(g_2^F(\alpha)) &\iff N_n(d_0\alpha^{d-p^2}) = N_n(\lambda k_0\alpha^{k-1}) \\
&\iff N_n(\frac{k_0}{d_0}\lambda) = \frac{N_n(\alpha^{d-p^2})}{N_n(\alpha^{k-1})} \\
&\iff N_n(\frac{k_0}{d_0}\lambda) = N_n(\alpha)^{d-k} \\
&\iff N_n(\frac{k_0}{d_0}\lambda) = N_n(\alpha)^{p-d_0+d_0-(k_0+p-k_0)} \\
&\iff N_n(\frac{k_0}{d_0}\lambda) = N_n(\alpha)^0 = 1
\end{aligned}$$

We end the proof using Corollary 3. □

Example 7. Let p be an odd prime number. The following function $F(x) = x^{(p-i)p^2+ip} + \lambda x^{ip+p-i}$ where $i \in \{1, .., p-1\}$ is GAPN over $\mathbb{F}_{p^n}$ for every positive integer $n \geq 3$ such that $\lambda^{\frac{p^n-1}{p-1}} \neq 1$ where $\lambda \in \mathbb{F}_{p^n}$.
For a fixed p and n, we can always find $\lambda \in \mathbb{F}_{p^n}^*$ such that $\lambda^{\frac{p^n-1}{p-1}} \neq 1$. In fact, $\{\lambda \in \mathbb{F}_{p^n} \mid \lambda^{\frac{p^n-1}{p-1}} = 1\}$ has a cardinality at most $\frac{p^n-1}{p-1} < p^n - 1$ because p is odd.

4.3.1 Multinomial GAPN GDO functions of Hamming weight 3

Theorem 22. *Let $p \geq 5$ be a prime number and $n \geq 3$, and let $F(x) = \sum_{i=1}^{\frac{p-1}{2}} f_i x^{ip^2+(p-2i)p+i} \in \mathbb{F}_{p^n}[x]$ be a GDO polynomial. Then F is a GAPN function over $\mathbb{F}_{p^n}$ if and only if $n \not\equiv 0 \pmod p$ and the polynomial $g(X) = \sum_{i=1}^{\frac{p-1}{2}} if_i X^{ip^2+(p-2i)p+i} \in \mathbb{F}_{p^n}[X]$ has no root in $\mathbb{F}_{p^n}^*$.*

Proof. Let $\alpha \in \mathbb{F}_{p^n}^*$. We have

$$\begin{aligned}
\nabla_\alpha F(x) &= \sum_{i=1}^{\frac{p-1}{2}} f_i(-i\alpha^{ip^2+(p-2i)p+i-p^2}x^{p^2} + 2i\alpha^{ip^2+(p-2i)p+i-p}x^p - i\alpha^{ip^2+(p-2i)p+i-1}x) \\
&= \sum_{i=1}^{\frac{p-1}{2}} (-i) \times f_i \times (\alpha^{ip^2+(p-2i)p+i-p^2}x^{p^2} - 2\alpha^{ip^2+(p-2i)p+i-p}x^p + \alpha^{ip^2+(p-2i)p+i-1}x) \\
&= \sum_{i=1}^{\frac{p-1}{2}} (-i) \times f_i \times \alpha^{ip^2+(p-2i)p+i} \times (\alpha^{-p^2}x^{p^2} - 2\alpha^{-p}x^p + \alpha^{-1}x) \\
&= -\left(\sum_{i=1}^{\frac{p-1}{2}} if_i\alpha^{ip^2+(p-2i)p+i}\right) \times \left((\frac{x}{\alpha})^{p^2} - 2(\frac{x}{\alpha})^p + \frac{x}{\alpha}\right).
\end{aligned}$$

Thus, if $\sum_{i=1}^{\frac{p-1}{2}} if_i\alpha^{ip^2+(p-2i)p+i} \neq 0$, then

$$\nabla_\alpha F(x) = 0 \iff (\frac{x}{\alpha})^{p^2} - 2(\frac{x}{\alpha})^p + \frac{x}{\alpha} = 0.$$

From Lemma 11, the polynomial $X^{p^2} - 2X^p + X \in \mathbb{F}_p[X]$ has only p roots in $\mathbb{F}_{p^n}$ if and only if $n \not\equiv 0 \pmod{p}$. Thus, $(\frac{X}{\alpha})^{p^2} - 2(\frac{X}{\alpha})^p + \frac{X}{\alpha}$ has only p roots in $\mathbb{F}_{p^n}$ if and only if $n \not\equiv 0 \pmod{p}$. We conclude that the equation $\nabla_\alpha F(x) = 0$ has p solutions in $\mathbb{F}_{p^n}$ if and only if $n \not\equiv 0 \pmod{p}$. □

We need the following definition for our next results.

Definition 11. Let $p \geq 3$ be a prime number. For $1 \leq k \leq p-1$, we define $e_3(k)$ as

$$e_3(k) := kp^2 + (p-2k)p + k.$$

We have the following result for GDO binomials.

Corollary 5. *Let $p \geq 5$ be a prime number and $F(x) = x^{e_3(i)} - \lambda x^{e_3(j)}$ be a function over $\mathbb{F}_{p^n}$ where $1 \leq i \neq j \leq \frac{p-1}{2}$ and $\lambda \in \mathbb{F}_{p^n}^*$. Then F is GAPN over $\mathbb{F}_{p^n}$ if and only if $n \not\equiv 0 \pmod{p}$ and $\frac{i}{j}\lambda$ is not a $(e_3(j) - e_3(i))$ power in $\mathbb{F}_{p^n}$.*

Proof. From Theorem 22, if

$$i\alpha^{e_3(i)} - j\lambda\alpha^{e_3(j)} \neq 0 \ \forall \alpha \in \mathbb{F}_{p^n}^*$$

then $F(x) = x^{e_3(i)} - \lambda x^{e_3(j)}$ is GAPN over $\mathbb{F}_{p^n}$ if and only if $n \not\equiv 0 \pmod{p}$. In the other hand, for $\alpha \in \mathbb{F}_{p^n}^*$, we have that

$$i\alpha^{e_3(i)} - j\lambda\alpha^{e_3(j)} \neq 0 \iff \frac{i}{j}\lambda \neq \alpha^{e_3(j)-e_3(i)}.$$

□

Remark 6. Remark that $e_3(j) - e_3(i) = (j-i)(p-1)^2$. So, if there exist $y \in \mathbb{F}_{p^n}$ such that $\frac{i}{j}\lambda = y^{e_3(j)-e_3(i)}$, then $N_n(\frac{i}{j}\lambda) = 1$.
Thus, if $N_n(\frac{i}{j}\lambda) \neq 1$, then $F(x) = x^{e_3(i)} - \lambda x^{e_3(j)}$ is a *GAPN* function over $\mathbb{F}_{p^n}$ if and only if $n \not\equiv 0 \pmod{p}$.
For a fixed i and j, we can always find $\lambda \in \mathbb{F}_{p^n}^*$ such that $N_n(\frac{i}{j}\lambda) \neq 1$, i.e, F is a GAPN function as in Corollary 5.

Example 8. Let $p \geq 5$ be a prime number. By using Theorem 22, we can conclude that the following binomial

$$F(x) = x^{p^2+(p-2)p+1} - \lambda x^{2p^2+(p-4)p+2}$$

where $\frac{\lambda}{2}$ is not a $(p-1)^2$ power in $\mathbb{F}_{p^n}^*$ is GAPN over $\mathbb{F}_{p^n}$ for every $n \geq 3$ such that $n \not\equiv 0 \pmod{p}$. Using Remark 6, the function

$$F(x) = x^{p^2+(p-2)p+1} + 2x^{2p^2+(p-4)p+2}$$

is GAPN over $\mathbb{F}_{p^n}$ for every odd integer $n \geq 3$ such that $n \not\equiv 0 \pmod{p}$. It is a new exceptional binomial GAPN function and it is of Hamming weight 3.

As $e_3(i) - e_3(j) = (i-j)(p-1)^2$ for all $1 \leq i, j \leq \frac{p-1}{2}$, we can use Theorem 22 to extract the following result.

Corollary 6. *Let $p \geq 5$ be a prime number and $F(x) = \sum_{i=1}^{\frac{p-1}{2}} f_i x^{e_3(i)} \in \mathbb{F}_{p^n}[x]$ be a GDO polynomial where $n \geq 3$. Suppose that $f_1 \neq 0$ and that the polynomial $g(X) = \sum_{i=1}^{\frac{p-1}{2}} i f_i X^{i-1} \in \mathbb{F}_{p^n}[X]$ has no roots in $\mathbb{F}_{p^n}^*$, then F is a GAPN function over $\mathbb{F}_{p^n}$ if and only if $n \not\equiv 0 \pmod p$.*

Proof. From Theorem 22, if $G(X) = \sum_{i=1}^{\frac{p-1}{2}} i f_i X^{e_3(i)} \in \mathbb{F}_{p^n}[X]$ has no roots in $\mathbb{F}_{p^n}^*$, then F is GAPN over $\mathbb{F}_{p^n}$ if and only if $n \not\equiv 0 \pmod p$. In the other hand, we have :

$$\begin{aligned} G(X) &:= \sum_{i=1}^{\frac{p-1}{2}} i f_i X^{e_3(i)} \\ &= X^{e_1} \times \sum_{i=1}^{\frac{p-1}{2}} i f_i X^{e_3(i)-e_3(1)} \\ &= X^{e_3(1)} \times \sum_{i=1}^{\frac{p-1}{2}} i f_i X^{(i-1)(p-1)^2} \\ &= X^{e_3(1)} \times g(X^{(p-1)^2}) \end{aligned}$$

As a consequence, $G(X)$ and $g(X^{(p-1)^2})$ share the same nonzero roots.
In particular, if the polynomial $g(Y) = \sum_{i=1}^{\frac{p-1}{2}} i f_i Y^{(i-1)} \in \mathbb{F}_{p^n}[Y]$ has no nonzero roots in $\mathbb{F}_{p^n}$, then the same goes for $G(X)$. □

Example 9. Let $p \geq 7$, $n \geq 3$ is such that $n \not\equiv 0 \pmod p$ and $F(x) = f_1 x^{e_3(1)} + \frac{f_2}{2} x^{e_3(2)} + \frac{f_3}{3} x^{e_3(3)}$ be a function over $\mathbb{F}_{p^n}$. From 6, we know that if the polynomial

$$P(X) = f_3 X^2 + f_2 X + f_1 \in \mathbb{F}_{p^n}[X]$$

has no roots in $\mathbb{F}_{p^n}^*$, then F is GAPN over $\mathbb{F}_{p^n}$.
Suppose that $f_1 \neq 0$, i.e. $P(0) \neq 0$. Then P has roots in $\mathbb{F}_{p^n}^*$ if and only if $f_2^2 - 4 f_1 f_3$ is not a square in $\mathbb{F}_{p^n}$.
As a consequence, if $f_2^2 - 4 f_1 f_3$ is not a square in $\mathbb{F}_{p^n}$, then F is a GAPN function over $\mathbb{F}_{p^n}$.

In the example above, we can always suppose that $f_1 = 1$ (GEA-equivalence), and if $f_2^2 - 4 f_3$ is not a square in $\mathbb{F}_{p^n}$, then the function F is GAPN. As a consequence, we have the following corollary.

Corollary 7. *Let $p \geq 7$ be a prime number, $n \geq 3$ is such that $n \not\equiv 0 \pmod p$ and $\lambda \in \mathbb{F}_{p^n}$ be a non square. Then*

$$F(x) = x^{e_3(1)} + \frac{f}{2} x^{e_3(2)} + \frac{f^2 - \lambda}{12} x^{e_3(3)}$$

is GAPN over $\mathbb{F}_{p^n}$ for all $f \in \mathbb{F}_{p^n}^*$.

Proof. As we said above, if $\lambda := f_2^2 - 4 f_3 \in \mathbb{F}_{p^n}$ is not a square, then F is GAPN over $\mathbb{F}_{p^n}$.
Thus, by giving a non square λ, we have $f_3 = \frac{f_2^2 - \lambda}{4}$. □

4.3.2 Multinomial GAPN GDO functions of Hamming weight 5

We can generalize this construction for a Hamming degree equal to 5. Firs let us define the following notation.

Definition 12. Let $p \geq 5$ be a prime number. For $1 \leq k \leq p-1$ such that

- $1 \leq p - 4k \leq p-1$ and
- $1 \leq 6k - p \leq p-1$,

we define $e_5(k)$ as

$$e_5(k) := kp^4 + (p-4k)p^3 + (6k-p)p^2 + (p-4k)p + k.$$

For a given prime $p \geq 5$, we can show that k in Definition 12 verify $\frac{p+1}{6} \leq k \leq \frac{p-1}{4}$. As we are interested about multinomials, it is crucial to know how many $k \in [1, p-1]$ verify $\frac{p+1}{6} \leq k \leq \frac{p-1}{4}$ when p is given.
This quantity is exactly :

$$I(p) := \lfloor \frac{p-1}{4} \rfloor - \lceil \frac{p+1}{6} \rceil + 1.$$

Example 10. We express $I(p)$ for different prime p :

1. For $p = 17$:

$$\begin{aligned} I(p) &= \lfloor \frac{p-1}{4} \rfloor - \lceil \frac{p+1}{6} \rceil + 1 = 2 \\ &= 4 - 3 + 1 \\ &= 2, \end{aligned}$$

2. For $p = 19$: we find $I(p) = 4 - 4 + 1 = 1$,
3. For $p = 257$: we find $I(p) = 64 - 43 + 1 = 22$.

Remark 7. For $p \geq 17$ and $p \neq 19$, we have $I(p) \geq 2$.

By a simple re-adaptation of the proof of Theorem 22, we have the following result.

Theorem 23. *Let $p \geq 17$ and $p \neq 19$ be a prime number and*

$$F(x) = \sum_{i=\lceil \frac{p+1}{6} \rceil}^{\lfloor \frac{p-1}{4} \rfloor} f_i x^{e_5(i)} \in \mathbb{F}_{p^n}[x]$$

be a function over $\mathbb{F}_{p^n}$ where $n \geq 5$. Then F is GAPN over $\mathbb{F}_{p^n}$ if and only if $n \not\equiv 0 \pmod p$ and the following polynomial has no root in $\mathbb{F}_{p^n}^*$:

$$\sum_{i=\lceil \frac{p+1}{6} \rceil}^{\lfloor \frac{p-1}{4} \rfloor} i f_i X^{e_5(i)}.$$

Similarly, we have the following result on binomials as in Corollary 5.

Corollary 8. *Let $p \geq 17$ and $p \neq 19$. Let $F(x) = x^{e_5(i)} - \lambda x^{e_5(j)}$ be a function over $\mathbb{F}_{p^n}$ where $\lceil \frac{p+1}{6} \rceil \leq i \neq j \leq \lfloor \frac{p-1}{4} \rfloor$ and $\lambda \in \mathbb{F}_{p^n}$ is such that $\frac{i}{j}\lambda$ is not an $e_5(i) - e_5(j)$ power. Then F is a GAPN function over $\mathbb{F}_{p^n}$ if and only if $n \not\equiv 0 \pmod{p}$.*

Remark 8. Here we need $I(p) \geq 2$ (binomial), thus we suppose $p \geq 17$ and $p \neq 19$.

Remark 9. Remark that $e_5(i) - e_5(j) = (i-j)(p-1)^4$. If $\frac{i}{j}\lambda$ is an $e_5(i) - e_5(j)$ power, then $N_n(\frac{i}{j}\lambda) = 1$. As a consequence, if we suppose that $N_n(\frac{i}{j}\lambda) \neq 1$, then $F(x) = x^{e_5(i)} - \lambda x^{e_5(j)}$ is a GAPN function over $\mathbb{F}_{p^n}$ if and only if $n \not\equiv 0 \pmod{p}$.
For a fixed j and i, we can always find $\lambda \in \mathbb{F}_{p^n}^*$ such that $N_n(\frac{i}{j}\lambda) \neq 1$.

Example 11. Let $p = 29$ and $n = 5$. We have $n \not\equiv 0 \pmod{p}$, $\lceil \frac{p+1}{6} \rceil = 5$ and $\lfloor \frac{p-1}{4} \rfloor = 7$.
We take :

- $i = 5 : e_5(i) = 5 \times 29^4 + 9 \times 29^3 + 29^2 + 9 \times 29 + 5$,
- $j = 6 : e_5(j) = 6 \times 29^4 + 5 \times 29^3 + 7 \times 29^2 + 5 \times 29 + 6$,
- $k = 7 : e_5(k) = 7 \times 29^4 + 1 \times 29^3 + 13 \times 29^2 + 1 \times 29 + 7$.

We can now look for $f_5,\ f_6$ and f_7 in $\mathbb{F}_{p^5}$ such that the polynomial

$$5f_5X^{e_5(5)} + 6f_6X^{e_5(6)} + 7f_7X^{e_5(7)} \in \mathbb{F}_{p^n}[X]$$

has no roots in $\mathbb{F}_{p^n}^*$.
A concrete example of such GAPN functions is found by taking $f_5 = 16,\ f_6 = 25$ and $f_7 = 13$:

$$F(x) = 16x^{e_5(5)} + 25x^{e_5(6)} + 13x^{e_5(7)}.$$

Similar to Corollary 6, as $e_5(i) - e_5(j) = (i-j)(p-1)^4$, we have the following result.

Corollary 9. *Let $p \geq 17$ and $p \neq 19$ be a prime number and*

$$F(x) = \sum_{i=\lceil \frac{p+1}{6} \rceil}^{\lfloor \frac{p-1}{4} \rfloor} f_i x^{e_5(i)} \in \mathbb{F}_{p^n}[x]$$

be a function over $\mathbb{F}_{p^n}$ where $n \geq 5$. Suppose that $f_{\lceil \frac{p+1}{6} \rceil} \neq 0$ and that the polynomial

$$\sum_{i=\lceil \frac{p+1}{6} \rceil}^{\lfloor \frac{p-1}{4} \rfloor} i f_i X^{i-\lceil \frac{p+1}{6} \rceil} \in \mathbb{F}_{p^n}[X]$$

has no roots in $\mathbb{F}_{p^n}^*$. Then F is a GAPN function over $\mathbb{F}_{p^n}$ if and only if $n \not\equiv 0 \pmod{p}$.

Example 12 (Trinomials)**.** Let $p \geq 29$ such that $p \neq 31$ and

- $i = \lceil \frac{p+1}{6} \rceil$,

- $j = \lceil \frac{p+1}{6} \rceil + 1$ and
- $k = \lceil \frac{p+1}{6} \rceil + 2$.

Let $F(x) = \frac{1}{i}x^{e_5(i)} + \frac{f_2}{j}x^{e_5(j)} + \frac{f_3}{k}x^{e_5(k)} \in \mathbb{F}_{p^n}[x]$ be a function over $\mathbb{F}_{p^n}$ and $n \geq 5$. Suppose that $f_2^2 - 4f_3$ is not a square in $\mathbb{F}_{p^n}$. Then F is a GAPN function if and only if $n \not\equiv 0 \pmod{p}$.
In particular, for any $f \in \mathbb{F}_{p^n}^*$ and any non square $\lambda \in \mathbb{F}_{p^n}$, the function

$$F(x) = \frac{1}{i}x^{e_5(i)} + \frac{f}{j}x^{e_5(j)} + \frac{f^2 - \lambda}{4k}x^{e_k} \in \mathbb{F}_{p^n}[x]$$

is GAPN over $\mathbb{F}_{p^n}$ if and only if $n \not\equiv 0 \pmod{p}$.

Open problem 2. Generalizing this construction for Hamming degree greater to 5 (for a given prime p, find, if it can be defined, the expression of $e_i(k)$ for $i > 5$).

5 Conclusion

In this article, we provide new constructions of GAPN functions with algebraic degree p, both monomials and non-monomials. To do so, we call homogeneous polynomial functions of algebraic degree p Generalized Dembowski-Ostrom (GDO) functions in reference to Dembowski-Ostrom (DO) polynomials and justify this choice by illustrating their links and how it can be applied to look for GAPN functions.

In the new constructions we obtain, we can be confident they are indeed new up to GEA-equivalence when their Hamming degree differs from previously known GAPN functions. Similarly, this Hamming degree argument ensures us that some of the non-monomial GAPN functions we describe are not GEA-equivalent to known power functions, although we have currently not proved their are not GEA-equivalent to any power functions. Similarly to what have been done concerning APN functions on binary fields (see [13, 10] for instance), one research direction is to show GEA-inequivalence between known multinomial GAPN functions to power functions.

Aknowledgements

This work is supported by the French Agence Nationale de la Recherche through the SWAP project under Contract ANR-21-CE39-0012.

References

[1] Riccardo Aragona, Marco Calderini, Daniele Maccauro, and Massimiliano Sala. On weak differential uniformity of vectorial boolean functions as a cryptographic criterion. *Appl. Algebra Eng. Commun. Comput.*, 27(5):359–372, 2016.

[2] Christof Beierle. Generalized almost perfect nonlinear binomials and trinomials over fields of prime-square order. *Finite Fields and Their Applications*, 88:102185, June 2023.

[3] Eli Ben-Sasson, Iddo Bentov, Yinon Horesh, and Michael Riabzev. Scalable zero knowledge with no trusted setup. In Alexandra Boldyreva and Daniele Micciancio, editors, *Advances in Cryptology - CRYPTO 2019 - 39th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2019, Proceedings, Part III*, volume 11694 of *Lecture Notes in Computer Science*, pages 701–732. Springer, 2019.

[4] Lilya Budaghyan, Nikolay S. Kaleyski, Soonhak Kwon, Constanza Riera, and Pantelimon Stanica. Partially APN boolean functions and classes of functions that are not APN infinitely often. *Cryptogr. Commun.*, 12(3):527–545, 2020.

[5] Claude Carlet. Two generalizations of almost perfect nonlinearity. *J. Cryptol.*, 38(2):20, 2025.

[6] Claude Carlet, Pascale Charpin, and Victor A. Zinoviev. Codes, bent functions and permutations suitable for des-like cryptosystems. *Des. Codes Cryptogr.*, 15(2):125–156, 1998.

[7] Ilaria Chillotti, Marc Joye, and Pascal Paillier. Programmable bootstrapping enables efficient homomorphic inference of deep neural networks. In Shlomi Dolev, Oded Margalit, Benny Pinkas, and Alexander A. Schwarzmann, editors, *Cyber Security Cryptography and Machine Learning - 5th International Symposium, CSCML 2021, Be'er Sheva, Israel, July 8-9, 2021, Proceedings*, volume 12716 of *Lecture Notes in Computer Science*, pages 1–19. Springer, 2021.

[8] Robert S. Coulter and Rex W. Matthews. Planar functions and planes of lenz-barlotti class II. *Des. Codes Cryptogr.*, 10(2):167–184, 1997.

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

[10] Yves Edel, Gohar M. Kyureghyan, and Alexander Pott. A new APN function which is not equivalent to a power mapping. *IEEE Trans. Inf. Theory*, 52(2):744–747, 2006.

[11] Pål Ellingsen, Patrick Felke, Constanza Riera, Pantelimon Stanica, and Anton Tkachenko. C-differentials, multiplicative uniformity, and (almost) perfect c-nonlinearity. *IEEE Trans. Inf. Theory*, 66(9):5781–5789, 2020.

[12] Sartaj Ul Hasan and Mohit Pal. Dembowski-ostrom polynomials and dickson polynomials. *Adv. Math. Commun.*, 18(4):1084–1099, 2024.

[13] Fernando Hernando and Gary McGuire. On the classification of perfect nonlinear (PN) and almost perfect nonlinear (APN) monomial functions. In Pascale Charpin, Alexander Pott, and Arne Winterhof, editors, *Finite Fields and Their Applications - Character Sums and Polynomials*, volume 11 of *Radon Series on Computational and Applied Mathematics*, pages 145–168. De Gruyter, 2013.

[14] Lukas Kölsch, Björn Kriepke, and Gohar M. Kyureghyan. Image sets of perfectly nonlinear maps. *Des. Codes Cryptogr.*, 91(1):1–27, 2023.

[15] Masamichi Kuroda. Monomial generalized almost perfect nonlinear functions, 2017.

[16] Masamichi Kuroda and Shuhei Tsujie. A generalization of APN functions for odd characteristic. *Finite Fields Their Appl.*, 47:64–84, 2017.

[17] Rudolf Lidl and Harald Niederreiter. *Finite Fields*. Encyclopedia of Mathematics and its Applications. Cambridge University Press, 2 edition, 1996.

[18] Gary McGuire and John Sheekey. A characterization of the number of roots of linearized and projective polynomials in the field of coefficients. *Finite Fields and Their Applications*, 57:68–91, 2019.

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

[20] Kaisa Nyberg. Differentially uniform mappings for cryptography. In Tor Helleseth, editor, *Advances in Cryptology — EUROCRYPT '93*, pages 55–64, Berlin, Heidelberg, 1994. Springer Berlin Heidelberg.

[21] Ferruh Özbudak and Ana Salagean. New generalized almost perfect nonlinear functions. *Finite Fields Their Appl.*, 70:101796, 2021.

[22] Alexander Pott. Almost perfect and planar functions. *Des. Codes Cryptogr.*, 78(1):141–195, 2016.

[23] Ana Salagean. Discrete antiderivatives for functions over $\mathop {{\mathbb {f}}}_p^n$. *Des. Codes Cryptogr.*, 88(3):471–486, 2020.

[24] Ana Salagean and Ferruh Özbudak. Further constructions and characterizations of generalized almost perfect nonlinear functions. *Cryptogr. Commun.*, 15(6):1117–1127, 2023.

[25] Valentin Suder. An equivalent representation of generalized differentials. *CoRR*, abs/2507.07337, 2025.

[26] Lixia Wang, Libo Wang, and Bicheng Zhang. A new class of generalized almost perfect nonlinear power function. *Finite Fields and Their Applications*, 82:102051, 2022.

[27] Hai Xiong, Longjiang Qu, Chao Li, and Ying Li. Some results on the differential functions over finite fields. *Applicable Algebra in Engineering, Communication and Computing*, 25(3):189–195, 2014.

[28] Yuyin Yu and Léo Perrin. Constructing more quadratic APN functions with the QAM method. *Cryptogr. Commun.*, 14(6):1359–1369, 2022.

[29] Xiangyong Zeng, Jinyong Shan, and Lei Hu. A triple-error-correcting cyclic code from the gold and kasami–welch apn power functions. *Finite Fields and Their Applications*, 18(1):70–92, 2012.

[30] Zhengbang Zha, Lei Hu, and Zhizheng Zhang. Three new classes of generalized almost perfect nonlinear power functions. *Finite Fields and Their Applications*, 53:254–266, 2018.

[31] Lijing Zheng, Haibin Kan, Jie Peng, Yanjun Li, and Yanbin Zheng. A new class of generalized almost perfect nonlinear monomial functions. *Information Processing Letters*, 184:106445, 2024.

Exponents e	**Conditions**	**Hamming degree**	**References**
$1+p^{i_2}+\cdots+p^{i_p}$	$i_2,\ldots,i_p>0$, $\{z\in\mathbb{F}_{p^n} \mid z+z^{p^{i_2}}+\cdots+z^{p^{i_p}}=0\}=\mathbb{F}_p$	p	[16, Lemma 3.3]
$k_2p^{l_2}+k_1p^{l_1}$	$l_1<l_2,\ 0<k_1,k_2\leq p-1$, $k_1+k_2=p$, $\gcd(l_2-l_1,n)=1$, $\gcd(k_1+k_2-(p-1),p^n-1)=1$	2	[24, Theorem 2]
$\sum_{i=0}^{\ell}k_i.p^i$	$0\leq k_i\leq p-1$, $n=q_1^{i_1}..q_s^{i_s}\geq 3$, $q_i\notin\{2,p\}$ primes, $\mathbb{O}_{q_i}(p)\geq\ell$ for every $1\leq i\leq s$.	$\in[2,\ell+1]$	Theorem 12
$\sum_{i=0}^{\ell}k_i.p^i$,	$0\leq k_i\leq p-1$, $n=2N$, $N=q_2^{i_2}..q_s^{i_s}\geq 3$, $q_i\notin\{2,p\}$ primes, $\mathbb{O}_{q_i}(p)\geq\ell$ for every $2\leq i\leq s$, $\exists 0\leq i,j\leq\ell,\ k_{2i}\neq 0$ and $k_{2j+1}\neq 0$	$\in[2,\ell+1]$	Theorem 15
$k_2p^2+k_1p+k_0$	$n=p^{\alpha}.N$ where $N\not\equiv 0 \pmod p$ and $\alpha\geq 0$ $k_0^N\neq k_2^N$ or ($k_0=k_1$ and $\alpha=0$)	$\in[2,3]$	Theorem 16

Table 1: Known GDO GAPN monomial functions over $\mathbb{F}_{p^n}$ for an odd prime p up to GEA-equivalence.

Polynomial Representation	Conditions	Hamming degree	References
$x^{p^i+p-1} - x^{p^{n-i}+p-1}$	$i > 0$ and $gcd(i,n) = 1$	2	[16, Proposition 3.5]
$\sum_{i=1}^{p-1} c^{p-1-i} x^{ip^{l_2}+(p-i)p^{l_1}}$	$l_2 > l_1,\ gcd(l_2 - l_1, n) = 1$ $c = \alpha^v,\ \alpha$ primitive element of $\mathbb{F}_{p^n}$ $v \mid p-1$ and $v < p-1$	2	[24, Theorem 7]
$cx^{i_1 p^{l_2}+(p-i_1)p^{l_1}} + x^{i_2 p^{l_2}+(p-i_2)p^{l_1}}$	$l_2 > l_1,\ gcd(l_2 - l_1, n) = 1,$ $1 \le i_1 < i_2 \le p-1,$ $c = (-1)^{i_2-i_1+1} \frac{\binom{p-2}{i_2-1}}{\binom{p-2}{i_1-1}} \beta,$ $\beta \in \mathbb{F}_{p^n}$ of order not dividing $\frac{p^n-1}{i_3(p-1)}$ $i_3 = gcd(i_2 - i_1, \frac{p^n-1}{p-1}) = 1$	2	[24, Theorem 8]
$x^{p-s}(ax^{p^k} + x^{p^{n-k}} + bx)^s$	$n \ge 3,\ 1 \le k \le n-1,$ $gcd(n,k) = 1$ $2 \le s \le p-1,$ $a^{\frac{p^n-1}{p-1}} \ne 1,$ $b \notin \{0, \frac{ax^{p^k}+x^{p^{n-k}}}{x} \mid x \in \mathbb{F}_{p^n}^*\}$	$\in [2, s+1]$	[24, Example 3]
$x^{p-s}(ax^{p^k} + x^{p^{n-k}} + bx)^s$	$n \ge 3,\ 1 \le k \le n-1,$ $gcd(n,k) = 1$ $2 \le s \le p-1,$ $a^{\frac{p^n-1}{p-1}} = 1,\ n$ odd $b \notin \{0, \frac{ax^{p^k}+x^{p^{n-k}}}{x} \mid x \in \mathbb{F}_{p^n}^*\}$	$\in [2, s+1]$	[24, Example 3]
$x^{p-s}(ax^{p^k} + x^{p^{n-k}})^s$	$n \ge 3$ odd, $1 \le k \le n-1,$ $gcd(n,k) = 1$ $2 \le s \le p-1,$ $a^{\frac{p^n-1}{p-1}} \notin \{-1, 1\},$	$\in [2, s+1]$	[24, Corollary 3]
$x^{d_1} + ux^{d_2}$ (over $\mathbb{F}_{p^2}$)	$d_1, d_2 \in [1, p^2-1],\ d_2$odd and u not a square in$\mathbb{F}_{p^2}$ $x \mapsto x^{d_1}$ GAPN over $\mathbb{F}_{p^2}$	2	[2, Theorem 1]
$x^{d_1} + ux^{d_2}$ (over $\mathbb{F}_{p^2}$)	$d_1, d_2 \in [1, p^2-1],\ d_2$ even and $\exists N$ odd such that $N \mid p+1$ and $N \mid d_2 - d_1$ and u not an N-th power in $\mathbb{F}_{p^2}$ $x \mapsto x^{d_1}$ GAPN over $\mathbb{F}_{p^2}$	2	[2, Theorem 1]
$x^{2p-1} + ux^{kp+l}$ (over $\mathbb{F}_{p^2}$)	$u \in \mathbb{F}_{p^2}$ a primitive element, $k, l \in [0, p-1]$ with $l + k$ odd	2	[2, Corollary 1]
$x^{(p-d_0)p^2+d_0 p} + \lambda x^{k_0 p+p-k0}$	$(\frac{k_0}{d_0})^n \lambda^{\frac{p^n-1}{p-1}} \ne 1$	2	Corollary 4
$x^{e_3(i)} - \lambda x^{e_3(j)}$	$p > 3,\ e_3(k)$ as in Definition 11 $\frac{i}{j}\lambda$ not an $e_3(i) - e_3(j)$ power in $\mathbb{F}_{p^n}^*,\ n \ge 3.$	3	Corollary 5
$x^{e_5(i)} - \lambda x^{e_5(j)}$	$p \ge 17$ such that $p \ne 19,$ $e_5(k)$ as in Definition 12, $\lceil \frac{p+1}{6} \rceil \le i \ne j \le \lfloor \frac{p-1}{4} \rfloor,$ $\frac{i}{j}\lambda$ not an $e_5(i) - e_5(j)$ power in $\mathbb{F}_{p^n}^*,\ n \ge 5.$	5	Corollary 8
$x^{e_3(1)} + \frac{f}{2}x^{e_3(2)} + \frac{f^2-\lambda}{12}x^{e_3(3)}$	$p \ge 7,\ n \ge 3$ such that $n \not\equiv 0 \pmod p,$ $e_3(k)$ as in Definition 11, $f \in \mathbb{F}_{p^n},$ $\lambda \in \mathbb{F}_{p^n}$ not a square.	3	Corollary 7
$\frac{1}{i}x^{e_5(i)} + \frac{f}{j}x^{e_5(j)} + \frac{f^2-\lambda}{4k}x^{e_5(k)}$	$p \ge 17$ such that $p \ne 19,\ n \ge 5$ such that $n \not\equiv 0 \pmod p,$ $e_5(k)$ as in Definition 12, $i = \lceil \frac{p+1}{6} \rceil,\ j = i+1,\ k = i+2$ $f \in \mathbb{F}_{p^n},$ $\lambda \in \mathbb{F}_{p^n}$ not a square.	5	Corollary 8

Table 2: Known non monomial GAPN functions which are GDO polynomials over $\mathbb{F}_{p^n}$ for an odd prime p.

Exponents e	**Conditions**	**Hamming degree**	**Algebraic degree**	**References**
p^n-2		n	$n(p-1)-1$	[16, Proposition 3.2]
$k_2p^{l_2}+k_1p^{l_1}$	$l_1<l_2,\ 0<k_1,k_2\le p-1$, $p\le k_1+k_2\le 2p-2\gcd(l_2-l_1,n)=1$, $\gcd(k_1+k_2-(p-1),p^n-1)=1$	2	$\in[p,2p-3]$	[24, Theorem 2]
$kp+p-j$	$p>3,\ 1\le j<k<p$, $gcd(k-j+1,p^n-1)=1$	2	$p+k-j$	[30, Theorem 2.4]
$tp^\ell+p-1$	$p>3,\ 1<\ell<n-1,\ gcd(\ell,n)=1$, t odd,$1<t<p,\ gcd(t,p^n-1)=1$	2	$p+t-1$	[30, Theorem 3.1]
$tp^{n-1}-1$	$p>3,\ 0<t<p\ gcd(p-t,p^n-1)=1$, t even	unknown	$n(p-1)-p+t$	[30, Theorem 4.1]
$k_2p^{l_2}+k_1p^{l_1}+p-1$	$p>3, l_1+l_2=n$, $1<k_1+k_2\le p-1$, $gcd(k_2p^{l_2}+k_1,p^n-1)=1$, $gcd(l_2,n)=1$	3	$\in[p+1,2(p-1)-1]$	[26, Theorem 3.1]
$p^{2\ell}+(p-1)p^{\ell l}+p-3$	$p>3,\ gcd(\ell,n)=1,\ gcd(p^\ell+p-3,p^n-1)=1$	3	$2p-3$	[31, Theorem 3.1]

Table 3: Known monomial GAPN functions which are not GDO polynomials over $\mathbb{F}_{p^n}$ for an odd prime p up to GEA-equivalence.

Polynomial Representation	**Conditions**	**Algebraic degree**	**References**
$\sum_{i=u}^{p-1}c^{p-1-i}x^{ip^{l_2}+(p-1+u-i)p^{l_1}}$	$l_2>l_1,\ gcd(l_2-l_1,n)=1$, $1\le u<p-1,\ gcd(u,p^n-1)=1$ $c=\alpha^v,\ \alpha$ primitive element of $\mathbb{F}_{p^n}$ $v\mid p-1$ and $v<p-1$	$p-1+u$	[24, Theorem 7]
$cx^{i_1p^{l_2}+(p-1+u-i_1)p^{l_1}}+x^{i_2p^{l_2}+(p-1+u-i_2)p^{l_1}}$	$l_2>l_1,\ gcd(l_2-l_1,n)=1$, $1\le u\le i_1<i_2\le p-1$, $gcd(u,p^n-1)=1$ $c=(-1)^{i_2-i_1+1}\frac{\binom{p-1-u}{i_2-u}}{\binom{p-1-u}{i_1-u}}\beta$, $\beta\in\mathbb{F}_{p^n}$ of order not dividing $\frac{p^n-1}{i_3(p-1)}$ $i_3=gcd(i_2-i,\frac{p^n-1}{p-1})=1$	$p-1+u$	[24, Theorem 8]
$x^{d_1}+ux^{d_2}$	$d_1,d_2\in[1,p^2-1],\ d_2$ odd and u not a square in $\mathbb{F}_{p^2}$	$\in[p,2(p-1)]$	[2, Theorem 1]
$x^{d_1}+ux^{d_2}$	$d_1,d_2\in[1,p^2-1],\ d_2$ even and $\exists N$ odd such that $N\mid p+1$ and $N\mid d_2-d_1$ and u not an N-th power in $\mathbb{F}_{p^2}$	$\in[p,2(p-1)]$	[2, Theorem 1]
$x^{2p-1}+ux^{kp+l}$	$u\in\mathbb{F}_{p^2}$ a primitive element, $k,l\in[0,p-1]$ with $l+k$ odd	$\in[p,2(p-1)]$	[2, Corollary 1]
$x^{kp+p-j}+x^{(k+1)p+p-j-1}$	$p>3,\ gcd(n,p-1)\in\{1,2\}$ $1\le j<k<p-1$ $gcd(k-j+1,p^n-1)=1$	$k-j+p$	[30, Proposition 2.7]
$x^{(p-5)p^{n-1}-1}+\beta x^{(p-3)p^{n-1}-1}+5^{-1}\beta^2x^{(p-1)p^{n-1}-1}$	$p\ge7,\ gcd(5,p^{2n}-1)=1$	$(n-1)(p-1)+p-2$	[30, Proposition 4.3]

Table 4: Known non monomial GAPN functions which are not GDO polynomials over $\mathbb{F}_{p^n}$ for an odd prime p.