A DEGREE BOUND FOR PLANAR FUNCTIONS

Christof Beierle[1] and Tim Beyne*[2]

[1,2]*Faculty of Computer Science, Ruhr University Bochum, Bochum, Germany*
christof.beierle@rub.de
[2]*COSIC, KU Leuven, Leuven, Belgium*
tim.beyne@esat.kuleuven.be

Submitted: Jul 12, 2024; Accepted: Apr 24, 2025; Published: Sep 15, 2025

Abstract. Using Stickelberger's theorem on Gauss sums, we show that if F is a planar function on a finite field $\mathbb{F}_q$, then for all non-zero functions $G : \mathbb{F}_q \to \mathbb{F}_q$, we have

$$d_{\mathsf{alg}}(G \circ F) - d_{\mathsf{alg}}(G) \leqslant \frac{n(p-1)}{2},$$

where $q = p^n$ with p a prime and n a positive integer, and $d_{\mathsf{alg}}(F)$ is the algebraic degree of F, i.e., the maximum degree of the corresponding system of n lowest-degree interpolating polynomials for F considered as a function on $\mathbb{F}_p^n$. This bound implies the (known) classification of planar polynomials over $\mathbb{F}_p$ and planar monomials over $\mathbb{F}_{p^2}$. As a new result, using the same degree bound, we complete the classification of planar monomials for all $n = 2^k$ with $p > 5$ and k a non-negative integer. Finally, we state a conjecture on the sum of the base-p digits of integers modulo $q-1$ that implies the complete classification of planar monomials over finite fields of characteristic $p > 5$.

Keywords. Planar function, algebraic degree, Stickelberger's theorem, digit sum

Mathematics Subject Classifications. 05B25, 11T06, 11T24

1. Introduction

Throughout this work, let p be a prime and n a positive integer. Let $\mathbb{F}_q$ denote a field with $q = p^n$ elements. A function $F\colon \mathbb{F}_q \to \mathbb{F}_q$ is called *planar* if the mappings

$$x \mapsto F(x+\alpha) - F(x) - F(\alpha) \tag{1.1}$$

are permutations on $\mathbb{F}_q$ for all non-zero α in $\mathbb{F}_q$. The notion of planar functions originally comes from finite geometry and goes back to Dembowski and Ostrom [DO68], who studied projective

*Supported by a junior postdoctoral fellowship from the Research Foundation – Flanders (FWO) with reference number 1274724N.

planes of finite order n possessing a collineation group of order n^2. Planar functions have a strong relation to commutative semifields [CH08] and (partial) difference sets [WQWX07], and have applications in coding theory [CDY05]. They can only exist for odd characteristic p, as for $p = 2$ any element in the image of the function defined in (1.1) has at least two preimages x and $x + \alpha$. If p is odd, then there always exists a planar function, the canonical example being $x \mapsto x^2$. A complete classification is only known over prime fields, and was established independently by Gluck [Glu90], Hiramine [Hir89], and Ronyai and Szőnyi [RS89]. More precisely, a function over $\mathbb{F}_p$ with p an odd prime is planar if and only if it is of the form $x \mapsto ax^2 + bx + c$ with $a \neq 0$. For more details on planar functions, their properties and known families, we refer to the survey by Pott [Pot16].

There is a one-to-one correspondence between functions $F\colon \mathbb{F}_q \to \mathbb{F}_q$ and polynomials in the quotient ring $\mathbb{F}_q[X]/(X^q - X)$, as any function over $\mathbb{F}_q$ is the evaluation map of a unique interpolating polynomial of the form

$$\sum_{i=0}^{q-1} a_i X^i, \quad a_i \in \mathbb{F}_q. \tag{1.2}$$

A polynomial is called *planar* if its evaluation map is planar. For odd p, a polynomial of the form

$$\sum_{0 \leqslant i \leqslant j \leqslant n-1} a_{i,j} X^{p^i + p^j}, \quad a_{i,j} \in \mathbb{F}_q$$

is called a *Dembowski–Ostrom polynomial*. Planar Dembowski–Ostrom polynomials are an interesting special case of planar polynomials, as they are in one-to-one correspondence with commutative presemifields of odd order, by defining the presemifield operation $\odot$ corresponding to a planar Dembowski–Ostrom polynomial F as $x \odot \alpha = F(x+\alpha) - F(x) - F(\alpha)$, see [CH08]. In this work, Coulter and Henderson completely classified planar Dembowski–Ostrom polynomials over $\mathbb{F}_{p^2}$ and $\mathbb{F}_{p^3}$.

In [DO68], Dembowski and Ostrom mentioned the possibility that every planar function can be represented as a Dembowski–Ostrom polynomial.[1] This conjecture was actually proven false by Coulter and Matthews in [CM97] by showing that the monomial $X^{(3^i+1)/2}$ is planar over $\mathbb{F}_{3^n}$ if $\gcd(i, n) = 1$ and i is odd. A special case of this family of counterexamples was independently discovered in [HS97]. However, the conjecture remains open for $p > 3$ and (up to the notion of graph equivalence, i.e., two functions F and G on $\mathbb{F}_q$ are *graph equivalent* if there exists an affine bijection on the $\mathbb{F}_p$-vector space $\mathbb{F}_q^2$ that maps the graph of F to the graph of G) the counterexamples found in [CM97] are the only known counterexamples to the Dembowski–Ostrom conjecture.

There is an ongoing line of research aiming at the classification of planar monomials, i.e., planar polynomials of the form X^d. So far, the complete classification of planar monomials over $\mathbb{F}_{p^n}$ is known only for n in $\{1, 2, 3, 4\}$, see [Joh87, Cou06, BCV22, CL12]. Besides that, planar Dembowski–Ostrom monomials have been fully classified: a monomial $X^{p^i+p^j}$ over $\mathbb{F}_q$ with $0 \leqslant i \leqslant j \leqslant n-1$ is planar if and only if $n/\gcd(j-i, n)$ is odd [CM97]. Hence, the

[1] Adding a polynomial of the form $c + \sum_{i=0}^{n-1} a_i X^{p^i}$ with c and a_i in $\mathbb{F}_q$ does not affect the planar property, so this statement only makes sense for polynomials where the coefficients of X^{p^i} are zero and without constant term.

Dembowski–Ostrom conjecture for monomials over fields of characteristic $p > 3$ can be stated as follows.

Conjecture 1.1. If $\mathbb{F}_q$ has characteristic $p > 3$, then X^d is a planar monomial over $\mathbb{F}_q$ if and only if $d \equiv p^i + p^j \pmod{q-1}$ with $n/\gcd(j-i, n)$ odd.

Apart from the classification results for $n \leqslant 4$, the closest we came to resolving Conjecture 1.1 was a result by Zieve [Zie15], who proved that for a fixed prime p, there does not exists an exponent d other than those mentioned in Conjecture 1.1 (and those of the form $(3^i + 3^j)/2$ in the case of $p = 3$) such that X^d is planar over infinitely many fields $\mathbb{F}_{p^n}$. Mentioning the result of Zieve, it is worth remarking that a result of Menichetti on division algebras implies that for n a prime, all planar Dembowski–Ostrom polynomials with p large enough correspond (up to a notion of equivalence) to planar Dembowski–Ostrom monomials [Men96]. Note that this is in contrast to the case of composite n, as it was shown in [GK23] that the number of (non-equivalent) planar Dembowski–Ostrom polynomials over $\mathbb{F}_{p^{4m}}$ grows exponentially in m.

Our results. The aim of this work is to make progress on the classification of planar functions. We achieve this by proving that the algebraic degree of a planar function F composed with an arbitrary non-zero function G only grows additively with the algebraic degree of G.

For a non-negative integer e, let $s_p(e)$ be the sum of the digits in the base-p representation of e. The *algebraic degree* of a non-zero function $F\colon \mathbb{F}_q \to \mathbb{F}_q$, denoted $d_{\mathsf{alg}}(F)$, is defined as the largest value $s_p(i)$ for which X^i has a non-zero coefficient in the unique interpolating polynomial of degree at most $q-1$ for F. That is, in terms of representation (1.2), $d_{\mathsf{alg}}(F) = \max\{s_p(i) \mid a_i \neq 0\}$. We prove the following result.

Theorem 1.2. *If F is a planar function on $\mathbb{F}_q$, then for all non-zero functions $G : \mathbb{F}_q \to \mathbb{F}_q$, we have*

$$d_{\mathsf{alg}}(G \circ F) - d_{\mathsf{alg}}(G) \leqslant \frac{n(p-1)}{2}.$$

The bound for the case that G is the identity function is relatively high and was already known before in the context of bent functions. Recall that a function $f\colon \mathbb{F}_q \to \mathbb{F}_p$ is called *bent* if $\left|\sum_{x\in\mathbb{F}_q} \theta^{\mathrm{tr}(f(x)-ux)}\right| = \sqrt{q}$ for all u in $\mathbb{F}_q$, where θ is a primitive p-th root of unity in the complex numbers and tr denotes the absolute trace on $\mathbb{F}_q$. Hou [Hou04b] proved that a bent function $f\colon \mathbb{F}_q \to \mathbb{F}_p$ fulfills $d_{\mathsf{alg}}(f) \leqslant n(p-1)/2 + 1$ (a function F on $\mathbb{F}_q$ is planar if and only if all functions $x \mapsto \mathrm{tr}(vF(x))$ with v in $\mathbb{F}_q^\times$ are bent, see [CD01, Pot16]). An analog of Theorem 1.2 for the case of $p = 2$ in terms of divisibility of Walsh coefficients of F was shown in [CV02]. The remarkable part of Theorem 1.2 is the fact that the algebraic degree of $G \circ F$ grows only additively with the algebraic degree of G. This is in contrast with what one expects for functions of low-algebraic degree, namely that the algebraic degree should be around $d_{\mathsf{alg}}(G) \cdot d_{\mathsf{alg}}(F)$ for large enough p and F of constant algebraic degree. Note that the bound $d_{\mathsf{alg}}(G\circ F) \leqslant d_{\mathsf{alg}}(G)\cdot d_{\mathsf{alg}}(F)$ implies that the inequality in Theorem 1.2 is fulfilled for any function F with $d_{\mathsf{alg}}(F) \leqslant 2$, and can therefore only be used to rule out planarity if $d_{\mathsf{alg}}(F) > 2$.

Let us define a binary operation $\star$ on the set $S = \{0, 1, \ldots, q-1\}$ by

$$e \star d = \begin{cases} 0 & \text{if } 0 \in \{e, d\}\,, \\ q-1 & \text{if } 0 \notin \{e, d\} \text{ and } r = 0\,, \\ r & \text{if } 0 \notin \{e, d\} \text{ and } r \neq 0, \end{cases}$$

where r is the unique non-negative integer smaller than $q-1$ such that $r \equiv ed \pmod{q-1}$. This operation makes $(S, \star)$ into a commutative monoid and we have $d_{\mathsf{alg}}(X^{ed}) = s_p(e \star d)$. Theorem 1.2 then has the following corollary for planar monomials.

Corollary 1.3. *If X^d is a planar monomial over $\mathbb{F}_q$ with $0 \leqslant d \leqslant q-1$, then*

$$s_p(e \star d) - s_p(e) \leqslant \frac{n(p-1)}{2},$$

for all e in $\{0, 1, \ldots, q-1\}$.

This provides a method for proving the non-planarity of a monomial X^d, namely by finding an element e with $1 \leqslant e \leqslant q-1$ that violates the degree bound, i.e., $s_p(e \star d) - s_p(e) > n(p-1)/2$. Using this technique, we establish again the classification of planar polynomials over $\mathbb{F}_p$ and planar monomials over $\mathbb{F}_{p^2}$. In addition, for the first time, we completely classify planar monomials over $\mathbb{F}_{p^{2^k}}$ for $p > 5$.

Theorem 1.4. *Let k be a non-negative integer and $p > 5$. The monomial X^d is planar over $\mathbb{F}_{p^{2^k}}$ if and only if $d \equiv 2p^i \pmod{p^{2^k}-1}$ for some non-negative integer i.*

Remark 1.5. A bound similar to the one stated in Corollary 1.3 is known for $p = 2$ in the context of the proof of the Niho conjecture on maximally nonlinear (almost perfect nonlinear, see e.g. [Hou04a] for a definition) monomials. More precisely, for $p = 2$ and $n = 2m+1$, it is known that an almost perfect nonlinear monomial X^d over $\mathbb{F}_q$ is maximally nonlinear if and only if $s_2(e \star d) - s_2(e) \leqslant m$, see [HX01, Hou04a]. In those works, the proof of the maximal nonlinearity of a certain monomial was established by bounding above $s_2(e \star d) - s_2(e)$ for all e with $1 \leqslant e \leqslant 2^n - 1$.

Remark 1.6. A referee pointed us to [LV05] for the first paper that uses Stickelberger's theorem directly to study cryptographic properties of monomials in characteristic two. Previous results of this kind resorted to McEliece's weight divisibility theorems for p-ary cyclic codes [McE71, McE72]. The result in [McE72] states a general congruence relation for weights in a p-ary cyclic code, which can be seen as a generalization of Ax's theorem [Ax64]. Note that both [Ax64] and [McE72] use Stickelberger's result.

Finally, we state and discuss a conjecture on the sum of base p-digits of integers modulo $q-1$ (Conjecture 5.1). A proof of this conjecture implies the complete classification of planar monomials over finite fields of characteristic $p > 5$.

2. Degree bound

Our proof relies on some ideas that were developed in the context of symmetric-key cryptanalysis, where a variant of Lemma 2.5 was proven for functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$ as an application of ultrametric integral cryptanalysis [Bey23, BV24]. The basic idea is to associate a linear operator to a function on $\mathbb{F}_q$, and to compare the additive and multiplicative Fourier transformations of this operator. Importantly, both Fourier transformations will be defined over a suitable extension of the p-adic numbers.

The motivation for this approach is that the property of being a planar function is inherently related to the additive structure of $\mathbb{F}_q$, and in particular has a simple characterization in terms of the additive Fourier transformation. The notion of algebraic degree is closely related to the multiplicative structure of $\mathbb{F}_q$, because the multiplicative characters of $\mathbb{F}_q$ are (lifted) monomial functions.

2.1. Additive and multiplicative Fourier transformations

We will define additive and multiplicative Fourier transformations over a local field. This requires some background from number theory, see for example [Lan90, Chapter 1] and [Kob84, Chapter 3]. Let p be an odd prime, $\mathbb{Q}_p$ the field of p-adic numbers, and $\mathbb{F}_q$ a field of order $q = p^n$. Let ζ_{q-1} be a primitive $(q-1)^{\text{st}}$ root of unity so that the algebraic extension $\mathbb{Q}_p(\zeta_{q-1})$ of $\mathbb{Q}_p$ has residue field $\mathbb{F}_q$. Throughout this section, we work over the totally ramified extension $\mathbb{K} = \mathbb{Q}_p(\zeta_{q-1}, \zeta_p)$ of $\mathbb{Q}_p(\zeta_{q-1})$, with ζ_p a primitive p^{th} root of unity. The field $\mathbb{K}$ is local with uniformizer π equal to $\zeta_p - 1$. That is, every nonzero element x in $\mathbb{K}$ can be written as $x = u\,\pi^i$ with i a unique integer and u a unit in the ring of integers of $\mathbb{K}$. The valuation of x will be denoted as $\operatorname{ord}_\pi x = i$. Since $(\pi)^{p-1} = (p)$ as ideals of the ring of integers of $\mathbb{K}$, the p-adic valuation extends to $\mathbb{K}$ by

$$\operatorname{ord}_p x = \frac{\operatorname{ord}_\pi x}{\operatorname{ord}_\pi p} = \frac{\operatorname{ord}_\pi x}{p-1}.$$

The corresponding p-adic absolute value of an element x of $\mathbb{K}$ will be denoted by $|x|_p = p^{-\operatorname{ord}_p x}$. By convention, $\operatorname{ord}_p 0 = \infty$ so that $|x|_p = 0$ if and only if $x = 0$. A similar setup was used in [Hou04b] for the proof of the degree bound for bent functions, but can be traced back further and is already found in the work of Ax [Ax64].

Let $\mathbb{K}[X]$ be the free $\mathbb{K}$-vector space on a finite commutative monoid X, and write $\mathbb{K}^X$ for the vector space of functions from X to $\mathbb{K}$. By extending functions on X linearly to all of $\mathbb{K}[X]$, we can think of $\mathbb{K}^X$ as the dual vector space of $\mathbb{K}[X]$. To avoid confusion between X and $\mathbb{K}[X]$, the standard basis vectors of $\mathbb{K}[X]$ will be denoted by δ_x, where $x \in X$. The corresponding dual basis of $\mathbb{K}^X$ consists of the functions $\delta^x : X \to \mathbb{K}$ such that $\delta^x(y) = 1$ if $x = y$ and zero otherwise.

A character is a homomorphism of monoids $X \to \mathbb{K}$. By a well-known result of Dedekind [Ded31], characters are linearly independent. Furthermore, the characters of X form a monoid $\widehat{X}$ under pointwise multiplication. It follows from the representation theory of monoids that if $\mathbb{K}$ contains enough roots of unity, then there exist precisely $|X|$ characters if and only if X

is a commutative *inverse monoid* [Ste16, §5.2]. A monoid X is inverse if for every x in X, there exists a y in X such that $xyx = x$. Hence, if X is an inverse monoid and $\mathbb{K}$ contains enough roots of unity, then its characters form a basis for $\mathbb{K}^X$. This will be true in our setting.

Dually, for a character χ, we can define $\chi^\vee$ as the unique element of $\mathbb{K}[X]$ such that $\psi(\chi^\vee) = 1$ if $\psi = \chi$ and 0 otherwise. Here, we consider ψ as an element of the dual space of $\mathbb{K}[X]$. We define the Fourier transformation as the change-of-basis transformation from the standard basis of $\mathbb{K}[X]$ to the basis $\{\chi^\vee \mid \chi \in \widehat{X}\}$ as follows.

Definition 2.1 (Fourier transformation)**.** If X is a finite commutative inverse monoid, then the Fourier transformation on $\mathbb{K}[X]$ is the linear map $\mathscr{F}_X : \mathbb{K}[X] \to \mathbb{K}[\widehat{X}]$ defined by $\chi^\vee \mapsto \delta_\chi$ for all monoid characters χ in $\widehat{X}$.

A common alternative to Definition 2.1 is to define the Fourier transformation as the dual change-of-basis $\mathscr{F}_X^{-\vee} : \mathbb{K}^X \to \mathbb{K}^{\widehat{X}}$ that maps χ to δ^χ, where $\mathscr{F}_X^{-\vee}$ is the inverse of the adjoint of $\mathscr{F}_X$. If X is a group, then it is common practice to identify $\mathbb{K}[X]$ with its dual $\mathbb{K}^X$. Indeed, χ and its dual $\chi^\vee$ are then the same up to conjugation and scaling. However, in the multiplicative case, the distinction will be significant for our purposes.

Throughout this paper, X will either be the additive group or the multiplicative monoid of the field $\mathbb{F}_q$. The characters of the additive group are given by $\chi : x \mapsto \zeta_p^{\mathrm{tr}(ux)}$ for u in $\mathbb{F}_q$, and the corresponding dual basis element is

$$\chi^\vee = \frac{1}{q} \sum_{x \in \mathbb{F}_q} \zeta_p^{-\mathrm{tr}(ux)}\, \delta_x.$$

The additive Fourier transformation will be denoted by $\mathscr{F}$, with the field $\mathbb{F}_q$ assumed to be clear from context. The multiplicative monoid $\mathbb{F}_q$ is inverse, and its characters are given by $\lambda : x \mapsto \tau(x^i)$ for i in $\{0, 1, \ldots, q-1\}$. Here, $\tau : \mathbb{F}_q \to \mathbb{Q}_p(\zeta_{q-1}) \subset \mathbb{K}$ is the Teichmüller character. Recall that $\mathbb{F}_q$ is the residue field of $\mathbb{K}$. By definition $\tau(0) = 0$ and, for $x \neq 0$, $\tau(x)$ is the unique $(q-1)^{\text{st}}$ root of unity such that $\tau(x) \equiv x \pmod{p}$. The existence and uniqueness are ensured by Hensel lifting. Restricting the characters of the monoid $\mathbb{F}_q$ to $\mathbb{F}_q^\times$ yields the characters of the multiplicative group $\mathbb{F}_q^\times$. If $i \neq 0$, then the corresponding dual basis element is

$$\lambda^\vee = \frac{1}{q-1} \sum_{x \in \mathbb{F}_q^\times} \tau\big(x^{-i}\big)\, \delta_x + \begin{cases} -\delta_0 & \text{if } i = q-1, \\ 0 & \text{else.} \end{cases}$$

If $i = 0$, i.e. λ is the trivial character $x \mapsto 1$, then $\lambda^\vee = \delta_0$. The multiplicative Fourier transformation will be denoted by $\mathscr{U}$, with the field $\mathbb{F}_q$ again assumed to be clear from the context.

2.2. Linear maps corresponding to a function on $\mathbb{F}_q$

For a function $F : \mathbb{F}_q \to \mathbb{F}_q$, we define a linear map $T^F : \mathbb{K}[\mathbb{F}_q] \to \mathbb{K}[\mathbb{F}_q]$ by

$$T^F\, \delta_x = \delta_{F(x)}.$$

The adjoint of T^F is the linear map $T^{F^\vee} : \mathbb{K}^{\mathbb{F}_q} \to \mathbb{K}^{\mathbb{F}_q}$ such that $T^{F^\vee} f = f \circ F$. The proof of our main result is based on comparing the additive and multiplicative Fourier transformation of the linear map T^F. For brevity, in the following we identify linear operators with their matrix representation relative to the standard basis. In the cryptanalysis literature, the additive Fourier transformation of T^F is called the *correlation matrix* C^F of F, see [DGV95, Bey21]:

$$C^F = \mathscr{F}\ T^F\ \mathscr{F}^{-1}.$$

It plays a central role in linear cryptanalysis, and its matrix coordinates at additive characters $\chi : x \mapsto \zeta_p^{\mathrm{tr}(ux)}$ and $\psi : x \mapsto \zeta_p^{\mathrm{tr}(vx)}$ are equal to

$$C^F_{\psi,\chi} = \psi\big(T^F \chi^\vee\big) = \frac{1}{q} \sum_{x \in \mathbb{F}_q} \zeta_p^{\mathrm{tr}(vF(x) - ux)}.$$

As a function of u (or $-u$ depending on conventions) and up to scaling, this is also called the Walsh transform of $x \mapsto \mathrm{tr}(vF(x))$. The multiplicative Fourier transformation of T^F is called the *ultrametric integral transition matrix* A^F of F, see [BV24, Bey23]:

$$A^F = \mathscr{U}\ T^F\ \mathscr{U}^{-1}.$$

It fulfills the role of the correlation matrix in (ultrametric) integral cryptanalysis. The coordinates of A^F are directly related to the unique interpolating polynomial of F with degree at most $q-1$.

Theorem 2.2 ([Bey23, Theorem 5.8])**.** *Let $F : \mathbb{F}_q \to \mathbb{F}_q$ be a function on the residue field $\mathbb{F}_q$ of $\mathbb{Q}_p(\zeta_{q-1}) \subset \mathbb{K}$. For all j in $\{0, 1, \ldots, q-1\}$, let $\sum_{i=0}^{q-1} a_{i,j}\, X^i$ be an interpolating polynomial of F^j over $\mathbb{F}_q$. The coordinates of the matrix A^F are integral elements in $\mathbb{Q}_p(\zeta_{q-1})$ and*

$$A^F_{\lambda,\mu} \equiv a_{i,j} \pmod{p},$$

for $\lambda : x \mapsto \tau(x^j)$ and $\mu : x \mapsto \tau(x^i)$.

Proof. Every coordinate $A^F_{\lambda,\mu} = \lambda\big(T^F \mu^\vee\big)$ is an integral element in $\mathbb{Q}_p(\zeta_{q-1})$ because the coordinates of T^F, $\mu^\vee$ and λ are all in the ring of integers of $\mathbb{Q}_p(\zeta_{q-1})$. By the definition of A^F, the function $\lambda \circ F$ in $\mathbb{K}^{\mathbb{F}_q^n}$ is equal to

$$T^{F^\vee} \lambda = \sum_{\mu} A^F_{\lambda,\mu}\ \mu,$$

where the sum is over all multiplicative characters of $\mathbb{F}_q$. That is, for every μ there exists an i in $\{0, 1, \ldots, q-1\}$ such that $\mu(x) = \tau(x^i)$ for all x in $\mathbb{F}_q$. Evaluating $\lambda \circ F$ at x and reducing modulo the maximal ideal (p) of $\mathbb{Z}_p[\zeta_{q-1}]$ gives

$$F^j(x) \equiv \sum_{\mu\,:\,x \mapsto \tau(x^i)} A^F_{\lambda,\mu}\ x^i \pmod{p}.$$

Since F^j has a unique interpolating polynomial of degree at most $q-1$ over $\mathbb{F}_q$, we can conclude that $A^F_{\lambda,\mu} \equiv a_{i,j} \pmod{p}$. □

The matrices C^F and A^F are both similar to T^F, hence similar to each other. More precisely, let $\mathscr{T} = \mathscr{F}\,\mathscr{U}^{-1}$, then $C^F = \mathscr{T}\ A^F\ \mathscr{T}^{-1}$. In the following section, we analyze the change-of-basis matrices $\mathscr{T}$ and $\mathscr{T}^{-1}$ in detail.

2.3. Bounds for change-of-basis

The Gauss sum corresponding to an additive character χ and a multiplicative character λ of $\mathbb{F}_q$ is defined as (the minus sign is a standard convention)

$$G(\chi, \lambda) = -\sum_{x \in \mathbb{F}_q^\times} \chi(x)\, \lambda(x).$$

Such sums are well-understood. In particular, we have the following classical result on the divisibility of $G(\chi, 1/\lambda)$ by $p = -\pi^{p-1}$, attributed to Stickelberger from the 19th century [Sti90]. By the algebraic degree of a multiplicative character λ, we mean the algebraic degree of the corresponding monomial. That is, if $\lambda(x) = \tau(x^k)$ with $0 \leqslant k \leqslant q-1$, then $d_{\mathsf{alg}}(\lambda) = d_{\mathsf{alg}}(X^k) = s_p(k)$.

Theorem 2.3 (Stickelberger's theorem for Gauss sums [Lan90, Chapter 1, Theorem 2.1])**.** *For all nontrivial additive characters χ of $\mathbb{F}_q$ and all multiplicative characters λ of $\mathbb{F}_q$ except $\lambda : x \mapsto \tau(x^{q-1})$, the Gauss sum $G(\chi, 1/\lambda)$ satisfies*

$$\operatorname{ord}_p G(\chi, 1/\lambda) = \frac{d_{\mathsf{alg}}(\lambda)}{p-1}.$$

Furthermore, if λ is $x \mapsto \tau(x^{q-1})$, then $\operatorname{ord}_p G(\chi, 1/\lambda) = 0$.

The following lemma uses Theorem 2.3 to bound the p-adic absolute values of the coordinates of the change-of-basis matrices $\mathscr{T} = \mathscr{F}\,\mathscr{U}^{-1}$ and $\mathscr{T}^{-1} = \mathscr{U}\,\mathscr{F}^{-1}$.

Lemma 2.4. *For the matrix $\mathscr{T} = \mathscr{F}\,\mathscr{U}^{-1}$ and its inverse $\mathscr{T}^{-1}$, we have*

$$\operatorname{ord}_p \mathscr{T}_{\chi,\lambda} = \frac{d_{\mathsf{alg}}(\lambda)}{p-1}, \quad \text{and} \quad \operatorname{ord}_p \mathscr{T}^{-1}_{\lambda,\chi} = -\frac{d_{\mathsf{alg}}(\lambda)}{p-1},$$

for every nontrivial character χ of the additive group $\mathbb{F}_q$ and every nontrivial character λ of the multiplicative monoid $\mathbb{F}_q$. Furthermore, $\mathscr{T}_{1,\lambda} = 0$ for all nontrivial λ.

Proof. Throughout the proof, the multiplicative character $\lambda^* : x \mapsto \tau(x^{q-1})$ will be a special case. By the definition of $\mathscr{U}$ and $\mathscr{F}$, we have $\mathscr{F}^\vee\, \delta^\chi = \chi$ and $\mathscr{U}^{-1}\, \delta_\lambda = \lambda^\vee$. Hence,

$$\begin{aligned}\mathscr{T}_{\chi,\lambda} = \delta^\chi\Big(\mathscr{F}\ \mathscr{U}^{-1}\, \delta_\lambda\Big) = \chi(\lambda^\vee) &= -\delta_\lambda(\lambda^*) + \frac{1}{q-1}\sum_{x \in \mathbb{F}_q^\times} \chi(x)/\lambda(x) \\ &= -\delta_\lambda(\lambda^*) - \frac{G(\chi, 1/\lambda)}{q-1}.\end{aligned}$$

Note that $\mathscr{T}_{\chi,\lambda^*} = -1 - 1/(q-1) = -q/(q-1)$, so $\operatorname{ord}_p \mathscr{T}_{\chi,\lambda^*} = n = d_{\mathsf{alg}}(\lambda^*)/(p-1)$. If $\lambda \neq \lambda^*$, then Theorem 2.3 yields

$$\operatorname{ord}_p \mathscr{T}_{\chi,\lambda} = \frac{d_{\mathsf{alg}}(\lambda)}{p-1}.$$

The result for $\chi = 1$ follows by a similar case distinction between $\lambda = \lambda^*$ and $\lambda \neq \lambda^*$. The proof for $\mathscr{T}^{-1}$ follows the same argument as above. Since $\mathscr{U}^\vee \delta^\lambda = \lambda$ and $\mathscr{F}^{-1} \delta_\chi = \chi^\vee$, we have

$$\mathscr{T}^{-1}_{\lambda,\chi} = \delta^\lambda \Big(\mathscr{U}\ \mathscr{F}^{-1}\ \delta_\chi \Big) = \lambda(\chi^\vee) = \frac{1}{q} \sum_{x \in \mathbb{F}_q^\times} \lambda(x)/\chi(x) = -\frac{G(1/\chi, \lambda)}{q}.$$

If $\lambda = \lambda^*$, then $\operatorname{ord}_p \mathscr{T}^{-1}_{\lambda^*,\chi} = 0 - n = -d_{\mathsf{alg}}(\lambda)/(p-1)$. Otherwise, using Theorem 2.3 we get

$$\operatorname{ord}_p \mathscr{T}^{-1}_{\lambda,\chi} = \frac{d_{\mathsf{alg}}(1/\lambda)}{p-1} - n = \frac{n(p-1) - d_{\mathsf{alg}}(\lambda)}{p-1} - n = -\frac{d_{\mathsf{alg}}(\lambda)}{p-1}.$$

In the second equality, we use the fact that $d_{\mathsf{alg}}(1/\lambda) = n(p-1) - d_{\mathsf{alg}}(\lambda)$ for nontrivial $\lambda \neq \lambda^*$. □

Lemma 2.4 implies the following theorem that bounds above the p-adic absolute value of the coordinates of A^F in terms of those of C^F. In Section 2.4, it will be shown that the degree bound for planar functions is a special case of Lemma 2.5.

Lemma 2.5. *Let F be a function on $\mathbb{F}_q$. For all nontrivial multiplicative characters λ and μ of $\mathbb{F}_q$, we have*

$$\operatorname{ord}_p A^F_{\mu,\lambda} \geqslant \frac{d_{\mathsf{alg}}(\lambda) - d_{\mathsf{alg}}(\mu)}{p-1} + \min_{\chi \neq 1, \psi \neq 1} \operatorname{ord}_p C^F_{\psi,\chi},$$

where the minimum is over all nontrivial additive characters of $\mathbb{F}_q$.

Proof. The result follows from the ultrametric triangle inequality. More precisely,

$$\operatorname{ord}_p A^F_{\mu,\lambda} = \operatorname{ord}_p \left(\mathscr{T}^{-1}\ C^F\ \mathscr{T} \right)_{\mu,\lambda} \geqslant \min_{\chi,\psi} \left(\operatorname{ord}_p \mathscr{T}^{-1}_{\mu,\psi} + \operatorname{ord}_p C^F_{\psi,\chi} + \operatorname{ord}_p \mathscr{T}_{\chi,\lambda} \right).$$

It can be assumed that $\chi \neq 1$ since $\mathscr{T}_{1,\lambda} = 0$ for nontrivial λ. Furthermore, $C^F_{1,\chi} = 0$ for $\chi \neq 1$. Hence, it can also be assumed that $\psi \neq 1$. Applying Lemma 2.4 to the first and last term in the sum concludes the proof. □

2.4. Degree bound

The field $\mathbb{K}$ has an automorphism $x \mapsto \overline{x}$ defined by $\zeta_p \mapsto 1/\zeta_p$. Given an embedding of $\mathbb{K}$ into $\mathbb{C}$, it corresponds to complex conjugation. Note that x and $\overline{x}$ always have the same p-adic valuation. Recall that F is a planar function on $\mathbb{F}_q$ if and only if $x \mapsto \operatorname{tr}(vF(x))$ is bent for all nonzero v in $\mathbb{F}_q$ (see [CD01, Pot16]). Equivalently, for all nontrivial additive characters χ and ψ of $\mathbb{F}_q$,

$$\overline{C^F_{\psi,\chi}} C^F_{\psi,\chi} = 1/q.$$

It terms of p-adic valuations, we have $\operatorname{ord}_p C^F_{\psi,\chi} = -n/2$. Lemma 2.5 can now be applied to bound above the p-adic absolute value of the coordinates of A^F. This upper bound leads to Theorem 1.2 below.

Theorem 1.2. *If F is a planar function on $\mathbb{F}_q$, then for all non-zero functions $G : \mathbb{F}_q \to \mathbb{F}_q$, we have*

$$d_{\mathsf{alg}}(G \circ F) - d_{\mathsf{alg}}(G) \leqslant \frac{n(p-1)}{2}.$$

Proof. Let $\mu(x) = \tau(x^i)$ and $\lambda(x) = \tau(x^j)$. From Lemma 2.5, we find that

$$\operatorname{ord}_p A^F_{\mu,\lambda} \geqslant \frac{s_p(j) - s_p(i)}{p-1} - n/2 = \frac{s_p(j) - s_p(i) - (p-1)n/2}{p-1}.$$

By Theorem 2.2, $A^F_{\mu,\lambda}$ is an element of $\mathbb{Z}_p[\zeta_{q-1}]$. Hence, it reduces to zero in the residue field $\mathbb{F}_q$ whenever $\operatorname{ord}_p A^F_{\mu,\lambda} > 0$. This implies that x^j can only be a monomial in the unique interpolating polynomial of degree at most $q-1$ for $x \mapsto F(x)^i$ if

$$s_p(j) - s_p(i) - (p-1)n/2 \leqslant 0.$$

Hence, the algebraic degree of any monomial with nonzero coefficients in the unique interpolating polynomial of degree at most $q-1$ for $x \mapsto F(x)^i$ is at most $(p-1)n/2 + s_p(i)$. If $G(x) = \sum_{i=0}^{q-1} a_i\, x^i$, then $G(F(x)) = \sum_{i=0}^{q-1} a_i\, F^i(x)$. Since the algebraic degree of $x \mapsto F^i(x)$ is at most $(p-1)n/2 + s_p(i)$, the algebraic degree of $G \circ F$ is bounded above by

$$d_{\mathsf{alg}}(G \circ F) \leqslant (p-1)n/2 + \max_{a_i \neq 0} s_p(i) = (p-1)n/2 + d_{\mathsf{alg}}(G).$$

The result follows by rearranging terms. □

If F and G are monomial functions, then Theorem 1.2 can be simplified as follows.

Corollary 1.3. *If X^d is a planar monomial over $\mathbb{F}_q$ with $0 \leqslant d \leqslant q-1$, then*

$$s_p(e \star d) - s_p(e) \leqslant \frac{n(p-1)}{2},$$

for all e in $\{0, 1, \ldots, q-1\}$.

Proof. Let $F(x) = x^d$ and $G(x) = x^e$. Since $(G \circ F)(x) = x^{e \star d}$, we have $d_{\mathsf{alg}}(G \circ F) = s_p(e \star d)$. The result follows from Theorem 1.2. □

3. Planar polynomials and monomials over $\mathbb{F}_p$ and $\mathbb{F}_{p^2}$

Using the degree bound stated in Theorem 1.2, we again establish the classification of planar polynomials over fields of prime order and planar monomials over fields of prime-square order. Those results were originally obtained in [Glu90, Hir89, RS89] and [Cou06], respectively. For the classification of planar monomials over extensions of prime-order fields, one resorts to the following basic fact, which is immediate from the definition of planarity.

Lemma 3.1. *Let $\mathbb{S}$ be a subfield of $\mathbb{F}_q$ and let F be a planar function on $\mathbb{F}_q$ so that the coefficients of its interpolating polynomial are in $\mathbb{S}$. The restriction of F to $\mathbb{S}$ is planar on $\mathbb{S}$.*

The second crucial ingredient in the classification results from [BCV22, Cou06, CL12] (the proof in [Hir89] also uses similar ideas) is Hermite's criterion for permutation polynomials.

Lemma 3.2 (Hermite's Criterion [LN96, Theorem 7.4])**.** *A polynomial Q in $\mathbb{F}_q[X]$ induces a permutation on $\mathbb{F}_q$ under evaluation if and only if the following two conditions hold:*

1. *Q has exactly one root in $\mathbb{F}_q$, and*
2. *for every positive integer $t \not\equiv 0 \pmod{p}$ less than $q-1$, the reduction of $Q(X)^t$ modulo $X^q - X$ has degree less than $q-1$.*

In the literature, the non-planarity of a polynomial F is often established by constructing an integer t such that Condition 2 is violated for $Q(X) = F(X+\alpha) - F(X)$ with non-zero α. If F is a monomial, then multiplying X by α shows that one can assume $\alpha = 1$ without loss of generality. Our proof of the classification of planar polynomials over prime fields uses the fact that the degree of a polynomial is equal to its algebraic degree, which significantly simplifies the application of the degree bound.

Corollary 3.3. *If F is a planar function on a field of prime order $p \geqslant 13$, then $d_{\mathsf{alg}}(F) = 2$.*

Proof. Without loss of generality, we can assume that $F(x) = \sum_{i=0}^{d} a_i\, x^i$ with $a_0, \ldots, a_d$ in $\mathbb{F}_p$, $a_d = 1$ and $0 \leqslant d \leqslant p-1$. As affine functions are not planar, we have $d \geqslant 2$. Theorem 1.2 with G the identity function implies that $d \leqslant (p+1)/2$. For $2 < d < (p+1)/2$, we will choose an exponent e such that the degree bound in Theorem 1.2 is violated for $G : x \mapsto x^e$. That is, we construct an e such that

$$d_{\mathsf{alg}}(G \circ F) - d_{\mathsf{alg}}(G) > \frac{p-1}{2}.$$

Let us take $e = \lfloor (p-1)/d \rfloor$, so that $d_{\mathsf{alg}}(G \circ F) = d_{\mathsf{alg}}(F^e) = ed$ and $d_{\mathsf{alg}}(G) = e$. This construction works for all d for which $e(d-1) > (p-1)/2$, that is,

$$\left\lfloor \frac{p-1}{d} \right\rfloor (d-1) > \frac{p-1}{2}.$$

This is true provided that $3 \leqslant d \leqslant (p-1)/2$. Indeed, the case of $d \in \{(p-1)/2 - 1, (p-1)/2\}$ is straightforward. For the other cases, using the inequality $\lfloor y \rfloor > y - 1$, we obtain

$$\left\lfloor \frac{p-1}{d} \right\rfloor (d-1) > p - 1 - \left(\frac{p-1}{d} + d - 1 \right)$$

with $(p-1)/d + d - 1 \leqslant (p-1)/2$, provided that $3 \leqslant d \leqslant (p-1)/2 - 2$ since $p \geqslant 13$.

Hence, the only remaining cases are $d = 2$ and $d = (p+1)/2$. The latter case can be ruled out because the unique interpolating polynomial with degree at most $p-1$ of $x \mapsto F(x+1) - F(x) - F(1)$ would have degree $(p-1)/2$. However, $(p-1)/2$ is a non-trivial divisor of $p-1$, so Hermite's criterion implies that this polynomial does not induce a permutation on $\mathbb{F}_p$ under evaluation (see, e.g., [LN96, Corollary 7.5]). □

Note that the cases $p \leqslant 11$ can be handled computationally. Indeed, one only needs to check the planarity of polynomials of degree at most $(p-1)/2$ and without linear or constant term. There are at most 11^4 such polynomials.

The classification of planar monomials over fields of order p^2 is a consequence of the classification for prime-order fields, and the degree bound with $e = 1$. The proof uses the fact that if a monomial function is planar on $\mathbb{F}_{p^2}$, then it must also be planar on $\mathbb{F}_p$ (see Lemma 3.1).

Corollary 3.4. *If F is a planar monomial function on a field of order p^2, then $d_{\mathsf{alg}}(F) = 2$.*

Proof. By restricting $F : x \mapsto x^d$ to $\mathbb{F}_p$ and applying Corollary 3.3, we get $s_p(d) \equiv 2 \pmod{p-1}$. That is, $s_p(d) = 2 + k(p-1)$ for some $k \geqslant 0$. However, the degree bound from Corollary 1.3 with $e = 1$ implies that $s_p(d) \leqslant p$. Hence, $k = 0$ and $s_p(d) = 2$. □

Corollary 3.4 states that if X^d is planar over $\mathbb{F}_{p^2}$, we have $d \equiv p^i + p^j \pmod{p^2 - 1}$ with $0 \leqslant i \leqslant j \leqslant 1$. From the classification of planar Dembowski–Ostrom monomials [CM97], it then follows that X^d is planar over $\mathbb{F}_{p^2}$ if and only if $d \equiv 2p^i \pmod{p^2 - 1}$ with i in $\{0, 1\}$.

Remark 3.5. The proof of Corollary 3.4 only depends on the classification of planar monomials over prime fields and the degree bound for $e = 1$. The latter result was already known from the bound of Hou in [Hou04b, Proposition 4.4]. Note that F is planar on $\mathbb{F}_q$ if and only if every component function $x \mapsto \mathrm{tr}(vF(x))$ with $v \in \mathbb{F}_q^\times$ is bent.

Remark 3.6. The proof of the recent classification of planar monomials over fields of order p^3 can be significantly simplified as well. Indeed, suppose X^d is a planar monomial over $\mathbb{F}_q$ with $q = p^3$ and $1 \leqslant d \leqslant q-1$. Corollary 3.3 and the degree bound with $e = 1$ imply that $s_p(d) = 2+k(p-1)$ for $k \in \{0, 1\}$. In [BCV22], settling the case of $k = 1$ boils down to handling 11 different choices of d (listed on page 22) and proving the non-planarity of X^d. Using the degree bound to establish non-planarity is often much simpler than applying Hermite's criterion, as was done in [BCV22]. For instance, the most complicated exponent to handle was $d = 1+2p+(p-2)p^2$. Applying the degree bound with $e = (p-3)/2+2p+2p^2$ (assuming $p > 11$) directly establishes non-planarity, whereas the method in [BCV22] based on Hermite's criterion needed a long case-analysis.

4. Classifying planar monomials over $\mathbb{F}_{p^{2^k}}$ for $p > 5$

Suppose that $n = 2m$ for an integer $m \geqslant 2$. As any planar monomial over $\mathbb{F}_{p^n}$ must also be planar over the subfield of order p^m, the core of our argument is to show that any planar monomial X^d over $\mathbb{F}_{p^n}$ fulfilling $d \equiv 2p^j \pmod{p^m - 1}$ for a non-negative integer j necessarily fulfills the congruence $d \equiv 2p^i \pmod{p^n - 1}$ for some non-negative integer i. The classification result for n a power of two then follows from an inductive argument, as already remarked in [CL12].

For integers $d_0, \ldots, d_{n-1}$, we denote by $[d_0, d_1, \ldots, d_{n-1}]_p$ the integer $d = \sum_{i=0}^{n-1} d_i \cdot p^i$. If each d_i for $0 \leqslant i \leqslant n-1$ fulfills $0 \leqslant d_i < p$ and not all d_i are equal to $p-1$, we write $d = (d_0, d_1, \ldots, d_{n-1})_p$. In that case, $(d_0, d_1, \ldots, d_{n-1})_p$ is the base-p representation of d and we have $s_p(d) = \sum_{i=0}^{n-1} d_i$. For an integer x, we will write $\bar{x} = p - 1 - x$. If x is a digit in $\{0, 1, \ldots, p-1\}$, then $\bar{x}$ is its complement.

The following lemma on the digits of d with $d \equiv 2p^{m-1} \pmod{p^m - 1}$ was established by Coulter and Lazebnik using elementary arithmetic.

Lemma 4.1 ([CL12]). *Let $n = 2m$ and $d = (d_0, d_1, \ldots, d_{n-1})_p$ such that d is congruent to $2p^{m-1} \pmod{p^m - 1}$. The tuple $(d_0 + d_m, d_1 + d_{m+1}, \ldots, d_{m-1} + d_{n-1})$ is equal to one of the following:*

1. $(0, \ldots, 0, 0, 2)$
2. $(p-1, \ldots, p-1, p-1, p+1)$
3. $(0, \ldots, 0, 0, p, p-1, \ldots, p-1, p-1, 1)$.

To show that X^d with $d \equiv 2p^{m-1} \pmod{p^m - 1}$ is not planar over $\mathbb{F}_{p^n}$, we only need to consider exponents d so that the tuple $(d_0 + d_m, d_1 + d_{m+1}, \ldots, d_{m-1} + d_{n-1})$ falls into one of the above cases.

The only planar monomials belonging to case 1 are those equivalent to X^2, i.e., either $d_{m-1} = 2$ or $d_{n-1} = 2$, corresponding to the monomials $X^{2p^{m-1}}$ and $X^{2p^{n-1}}$ respectively. When $d_{m-1} = d_{n-1} = 1$, the monomial X^d is not planar, because $n/\gcd(n-1-(m-1), n) = 2$. Case 2 was also solved completely in [CL12], but the proof was quite technical. Using the degree bound from Corollary 1.3 with $e = 1$, it is immediate that case 2 does not contain any planar monomials. Indeed, we have $s_p(d) = m(p-1) + 2$, whence $s_p(e \star d) - s_p(e) = m(p-1) + 1 > n(p-1)/2$. Case 3 is the most complicated and was only solved for $n \leqslant 4$. Based on the degree bound, we show that case 3 does not contain any planar monomial functions for $p > 5$, establishing the classification of planar monomials over $\mathbb{F}_{p^{2^k}}$ for $p > 5$.

In the following, we assume $n = 2m$. Let r and s be non-negative integers such that $r + s = m - 2$. For $t, u_1, \ldots, u_s$ in $\{0, \ldots, p-1\}$ with $t \neq 0$, we define $D(t, u_1, \ldots, u_s)$ to be the integer

$$(\overbrace{0, \ldots, 0}^{r}, t, \overbrace{u_1, \ldots, u_s}^{s}, 1, \overbrace{0, \ldots, 0}^{r}, p - t, \overbrace{\bar{u}_1, \ldots, \bar{u}_s}^{s}, 0)_p, \tag{4.1}$$

where $\bar{u}_i = p - 1 - u_i$. Any d corresponding to case 3 is of this form or a cyclic shift of it, because we can assume without loss of generality that the rightmost digit is a zero (in case it is a one, we can apply a cyclic shift). To prove our second main result (Theorem 1.4), we will prove the following lemma. It implies that the only planar monomials that fall into cases 1, 2 or 3 are of the form X^{2p^i}.

Lemma 4.2. *Suppose that $p > 5$, n is even, and let s be a non-negative integer. For all t, $u_1, \ldots, u_s$ in $\{0, \ldots, p-1\}$ with $t \neq 0$, the monomial $X^{D(t, u_1, \ldots, u_s)}$ is not planar over $\mathbb{F}_{p^n}$.*

The main result then follows by an inductive argument. We will prove Lemma 4.2 by showing that, for each $d = D(t, u_1, \ldots, u_s)$, there exists an e in $\{1, \ldots, p^n - 2\}$ such that $ed \equiv (r_0, \ldots, r_{n-1})_p \not\equiv 0 \pmod{p^n - 1}$ (so that $e \star d = (r_0, \ldots, r_{n-1})_p$) and $s_p(e \star d) - s_p(e) \geqslant m(p-1) + 1$. As there is no universal choice for e, the proof is quite technical and split into several cases, depending on the values of the digits t and $u_1, \ldots, u_s$ of d. To find suitable candidates of e, we first conducted computer experiments. However, our proof is completely verifiable by hand. We start by ruling out all but a finite number of cases (for fixed dimension n), independently of p.

4.1. Proof of Lemma 4.2 up to a finite number of cases for fixed n

We start with the simplest case, where not all of $t, u_1, \ldots, u_s$ are in $\{0, 1, p-2, p-1\}$. Note that we do not exclude the case of $p = 5$ here.

Lemma 4.3. *Suppose $p > 3$, $n = 2m$ with $m \geqslant 2$ and let s be a non-negative integer. If $d = D(t, u_1, \ldots, u_s)$ with $t, u_1, \ldots, u_s$ in $\{0, \ldots, p-1\}$ and $t \neq 0$ such that $t \notin \{1, p-1\}$ or $u_j \notin \{0, 1, p-2, p-1\}$ for some j in $\{1, \ldots, s\}$, then there exists an e in $\{1, \ldots, p^n - 1\}$ such that $s_p(e \star d) - s_p(e) > m(p-1)$.*

Proof. Let $r = m - 2 - s$. We will multiply d by $e = hp^m + h + 1$ for various choices of h with $1 \leqslant h < p^m$. First, note that multiplying d by hp^m yields

$$[\overbrace{0, \ldots, 0}^{r}, h(p-t), \overbrace{h\bar{u}_1, \ldots, h\bar{u}_s}^{s}, 0, \overbrace{0, \ldots, 0}^{r}, ht, \overbrace{hu_1, \ldots, hu_s}^{s}, h]_p \pmod{p^n - 1}.$$

The product of d and $h + 1$ is congruent to

$$\begin{aligned}[\overbrace{0, \ldots, 0}^{r}, ht + t, \quad & \overbrace{hu_1 + u_1, \ldots, hu_s + u_s}^{s}, h + 1, \\ \overbrace{0, \ldots, 0}^{r}, (h+1)(p-t), & \overbrace{h\bar{u}_1 + \bar{u}_1, \ldots, h\bar{u}_s + \bar{u}_s}^{s}, 0]_p.\end{aligned}$$

By adding up both results, we find that ed with $e = hp^m + h + 1$ is congruent to (mod $p^n - 1$)

$$[\overbrace{0, \ldots, 0}^{r}, t, \overbrace{u_1, \ldots, u_s}^{s}, 2h + 1, \overbrace{0, \ldots, 0}^{r}, p - t, \overbrace{\bar{u}_1, \ldots, \bar{u}_s}^{s}, 2h]_p. \tag{4.2}$$

We first consider the case that $t \notin \{1, p-1\}$. Let $h = p^{r+1} - 1$. As $1 \leqslant h + 1 < p^m$, we have $s_p(e) = s_p(h+1) + s_p(h)$ with $s_p(h+1) = 1$ and $s_p(h) = (r+1)(p-1)$, so $s_p(e) = (r+1)(p-1) + 1$. Moreover,

$$2h + 1 = (p^{r+1} - 1) + p^{r+1} = (p-1, \ldots, p-1, 1, 0, \ldots, 0)_p$$

with $r + 2$ non-zero digits. Hence, ed is congruent to

$$[\overbrace{p-1, \ldots, p-1}^{r}, t+1, \overbrace{u_1, \ldots, u_s}^{s}, \overbrace{p-1, \ldots, p-1}^{r+1}, p-t+1, \overbrace{\bar{u}_1, \ldots, \bar{u}_s}^{s}, p-2]_p.$$

Since $t \notin \{1, p-1\}$, all elements of the above tuple are in the range $\{0, 1, \ldots, p-1\}$. Hence,

$$e \star d = (\overbrace{p-1, \ldots, p-1}^{r}, t+1, \overbrace{u_1, \ldots, u_s}^{s}, \overbrace{p-1, \ldots, p-1}^{r+1}, p-t+1, \overbrace{\bar{u}_1, \ldots, \bar{u}_s}^{s}, p-2)_p.$$

For the sum of base p digits, using $2r + s + 1 = m + (r+1) - 2$, we have

$$s_p(e \star d) = (2r + s + 1)(p-1) + 2p = m(p-1) + (r+1)(p-1) + 2 > m(p-1) + s_p(e).$$

This establishes the first case.

Let us now consider the case where there exists an index j in $\{1,\dots,s\}$ such that $u_j \notin \{0,1,p-2,p-1\}$. Let $h = p^r - 1 + ((p-1)/2-1)p^r + p^{r+j+1}$. As before, it holds that $s_p(e) = s_p(h+1)+s_p(h)$. Since $s_p(h+1) = (p-1)/2+1$ and $s_p(h) = r(p-1)+(p-1)/2$, this implies $s_p(e) = (r+1)(p-1)+1$. Furthermore,

$$2h+1 = 2p^r - 1 + (p-3)p^r + 2p^{r+j+1} = (p-2)p^r + p^r - 1 + 2p^{r+j+1}$$

so

$$2h+1 = (\overbrace{p-1,\dots,p-1}^{r}, p-2, \overbrace{0,\dots,0}^{j}, 2, \overbrace{0,\dots,0}^{s-j})_p.$$

We now substitute h in (4.2) and distinguish between the cases $r>0$ and $r=0$. By the choice of j, both of u_j+2 and $p-1-u_j+2$ are in $\{0,\dots,p-1\}$. For $r>0$, we obtain

$$\begin{aligned} e \star d = (\overbrace{p-1,\dots,p-1}^{r-1}, p-2, \quad & t, u_1, \dots, u_{j-1}, u_j+2, u_{j+1}, \dots, u_s, p-1, \\ & p-1,\dots,p-1,p-2,p-t,\bar{u}_1,\dots,\bar{u}_{j-1},\bar{u}_j+2,\bar{u}_{j+1},\dots,\bar{u}_s,p-2)_p. \end{aligned}$$

For $r=0$, we obtain that $e \star d$ is equal to

$$(t, u_1, \dots, u_{j-1}, u_j+2, u_{j+1}, \dots, u_s, p-2, p-t, \bar{u}_1, \dots, \bar{u}_{j-1}, \bar{u}_j+2, \bar{u}_{j+1}, \dots, \bar{u}_s, p-3)_p.$$

In both cases, the sum of the base p digits is equal to $s_p(e\star d) = m(p-1)+(r+1)(p-1)+2$. Since $s_p(e) = (r+1)(p-1)+1$ as shown above, the result follows. □

We have now established that, for a fixed dimension n, the number of cases left to check is independent of p. Indeed, t can only take one of 1, $p-1$, while each u_j for $1 \leqslant j \leqslant s$ can be 0, 1, $p-2$, or $p-1$.

4.2. Proof of Lemma 4.2 for the remaining cases

The argument for settling the remaining cases is more technical and assumes $p \neq 5$. For our proof, we need the following technical lemma.

Lemma 4.4. *Let $p>3$. Let s be a positive integer and $u_0,u_1,\dots,u_s \in \{0,1,p-2,p-1\}$. For $v = [2u_1-u_0,\dots,2u_{s-1}-u_{s-2},2u_s-u_{s-1}]_p \neq p^s-1$, there exists δ in $\{-1,0,1\}$ such that*

$$v + \delta\, p^s = [\gamma_1,\dots,\gamma_s]_p,$$

with $\gamma_1,\dots,\gamma_s$ in $\{0,\dots,p-1\}$ and $0 < u_s+\delta+1 \leqslant p-1$. Furthermore, if $u_s=1$, $\delta=1$ and $p>5$, then there exists an index j such that $\gamma_j \notin \{0,1,p-2,p-1\}$.

Proof. For every index j, it holds that $1-p \leqslant 2u_j - u_{j-1} \leqslant 2(p-1)$. Since $(p-1)\sum_{i=0}^{s-1} p^i = p^s-1$, it follows that $v \geqslant 1-p^s \geqslant -p^s$ and $v \leqslant 2(p^s-1) \leqslant 2p^s-1$. Hence, there exists a δ in $\{-1,0,1\}$ such that $0 \leqslant v+\delta p^s \leqslant p^s-1$.

The prove the lower bound $u_s + \delta + 1 > 0$, it is sufficient to analyze the case $u_s = 0$. If $u_s = 0$, then $2u_s - u_{s-1} \leqslant 0$, so v is bounded above by $2(p-1)\sum_{i=0}^{s-2} p^i = 2p^{s-1} - 2 \leqslant p^s - 1$. Hence, $\delta \neq -1$ and consequently $u_s + \delta + 1 > 0$ for all values of u_s.

For the upper bound $u_s + \delta + 1 \leqslant p - 1$, it is enough to consider u_s in $\{p-2, p-1\}$. If $u_s = p-2$, then $2u_s - u_{s-1} \geqslant p-3$, so $v \geqslant (p-3)p^{s-1} + (1-p)\sum_{i=0}^{s-2} p^i = (p-4)p^{s-1} + 1 \geqslant 0$. Hence, $\delta \neq 1$ and the bound $u_s + \delta + 1 \leqslant p - 1$ is satisfied. For the case $u_s = p - 1$, we show that $\delta = -1$ when $v \neq p^s - 1$. From $v = 2u_s p^{s-1} - u_0 - (p-2)\sum_{i=0}^{s-2} u_{i+1}p^i$, we see that in this case the value of v is minimized for $u_0 = p - 2$ and $u_1 = u_2 = \ldots = u_s = p - 1$. Hence, $v \geqslant p + (p-1)\sum_{i=1}^{s-1} p^i = p^s$. This implies that $\delta = -1$, from which the upper bound follows.

To prove the final claim, define $v_j = 2u_j - u_{j-1}$. If $u_s = 1$, then $v_s \in \{2, 1, 3-p, 4-p\}$. More precisely, $v_s = 2 - u_{s-1}$. If $\delta = 1$, then it follows that $v_s \in \{3-p, 4-p\}$. Indeed this is trivial if $s = 1$ and, for $s > 1$, this follows from the fact that $-p^{s-1} \leqslant [v_1, \ldots, v_{s-1}]_p \leqslant 2p^{s-1} - 1$. Let now j be the smallest index in $\{1, \ldots, s\}$ with the property that $u_j = 1$ and $v_j \notin \{1, 2\}$. As discussed before, this index j exists and $v_j \in \{4-p, 3-p\}$. In what follows, we assume $p \geqslant 7$.

Case $v_j = 3 - p$. If $j = 1$, then we have $\gamma_j = \gamma_1 = 3$ (and the $-p$ decreases the value γ_2 by 1 as a negative carry). If $j \geqslant 2$, then we have $\gamma_j = 3 + c$, where c is the carry coming from $[v_1, \ldots, v_{j-1}]_p$. As $-p^{j-1} \leqslant [v_1, \ldots, v_{j-1}]_p \leqslant 2p^{j-1} - 1$, the carry c can only take the values $0, 1$, or -1. Hence, $\gamma_j \in \{2, 3, 4\}$. The result follows because $2, 3, 4 \notin \{p-2, p-1\}$ for $p \geqslant 7$.

Case $v_j = 4 - p$. Similarly as in the case above, if $j = 1$, then we have $\gamma_j = \gamma_1 = 4$ and we are done. Let us therefore assume $j \geqslant 2$. We have $\gamma_j = 4 + c$, where $c \in \{-1, 0, 1\}$ is the carry coming from $[v_1, \ldots, v_{j-1}]_p$ (note that for $p \geqslant 11$, the proof would be finished here). As discussed above, if $v_j = 4 - p$, then we have $u_{j-1} = p - 2$, so

$$\begin{aligned} v_{j-1} &\in \{2(p-2), 2(p-2) - 1, 2(p-2) - (p-2), 2(p-2) - (p-1)\} \\ &= \{p + p - 4, p + p - 5, p - 2, p - 3\}. \end{aligned}$$

If $v_{j-1} \in \{p-2, p-3\}$, then we have $c = 0$, so $\gamma_j = 4$ and the result follows. In case $v_{j-1} = p + p - 4$, we have $\gamma_{j-1} = p - 4 + c'$ for a carry $c' \in \{-1, 0, 1\}$, so $\gamma_{j-1} \in \{p-3, p-4, p-5\}$ and the result follows as well. Finally, suppose that $v_{j-1} = p + p - 5$, so that $\gamma_{j-1} = p - 5 + c'$ for a carry $c' \in \{-1, 0, 1\}$. If $j - 1 = 1$, then we have $c' = 0$ (there is no carry), so $\gamma_{j-1} = p - 5$ and the result follows as $p - 5 \notin \{0, 1\}$ if $p \geqslant 7$. In case of $j - 1 \geqslant 2$, we must have $u_{j-2} = 1$, and thus $v_{j-2} \in \{1, 2, 3-p, 4-p\}$. Since $j \geqslant 3$ was chosen as the least integer in $\{2, \ldots, s\}$ with the property that $u_j = 1$ and $v_j \notin \{1, 2\}$, we must have $v_{j-2} \in \{1, 2\}$. In this case we have $c' = 0$, and the result follows. □

Now, we settle the remaining cases, assuming $p > 5$.

Lemma 4.5. *Let $p > 5$, $n = 2m$ with $m \geqslant 2$, and s a non-negative integer. If we have $d = D(t, u_1, \ldots, u_s)$ with t in $\{1, p-1\}$ and $u_1, \ldots, u_s$ in $\{0, 1, p-2, p-1\}$, then there exists an e in $\{1, \ldots, p^n - 1\}$ such that $s_p(e \star d) - s_p(e) > m(p-1)$.*

Proof. Let $r = m - 2 - s$. We will multiply d by

$$e = hp^m + h + 1 + (p-1)p^m = (p - 1 + h)p^m + h + 1$$

for various choices of h with $1 \leqslant h < p^{m+1}$. The case $s = 0$ will be handled separately from the case $s > 0$.

Case $s = 0$. We first multiply d by $(p-1)p^m$ and obtain (see (4.1) for d)

$$d(p-1)p^m \equiv [\overbrace{0, \ldots, 0}^{r}, t, p-1-t, \overbrace{0, \ldots, 0}^{r}, -t, p-1+t]_p \pmod{p^n - 1}.$$

Let $e = hp^m + h + 1 + (p-1)p^m$. By adding the term (4.2) from the proof of Lemma 4.3, we obtain

$$ed \equiv [\overbrace{0, \ldots, 0}^{r}, 2t, 2h - t + p, \overbrace{0, \ldots, 0}^{r}, p - 2t, p - 1 + 2h + t]_p \pmod{p^n - 1}.$$

If $t = p - 1$, then $2t = p + p - 2$, so we can write $e \star d \pmod{p^n - 1}$ as

$$[\overbrace{0, \ldots, 0}^{r}, p-2, 2h+2, \overbrace{0, \ldots, 0}^{r}, 2, p - 2 + 2h + p - 1]_p.$$

In particular, whenever $t \in \{1, p-1\}$, we have

$$e \star d \equiv [\overbrace{0, \ldots, 0}^{r}, t', 2h - u_0 + p, \overbrace{0, \ldots, 0}^{r}, p - t', p - 1 + 2h + u_0]_p \pmod{p^n - 1},$$

where $t' \in \{2, p-2\}$, and $u_0 = 1$ if $t' = 2$ and $u_0 = p - 2$ if $t' = p - 2$.

If $t' = 2$, let $h = p^{r+1} - 1 - (p-1)/2$. As $0 \leqslant h + 1 < p^m$ and $0 \leqslant p - 1 + h < p^m$, we have $s_p(e) = s_p(h+1) + s_p(p - 1 + h)$. Since

$$s_p(h+1) = r(p-1) + (p-1)/2 + 1 \qquad \text{and} \qquad s_p(p - 1 + h) = (p-1)/2,$$

it follows that

$$s_p(e) = (r+1)(p-1) + 1.$$

From

$$2h = p^{r+1} - 1 + \sum_{i=1}^{r} (p-1)p^i,$$

we obtain

$$\begin{aligned} e \star d &= [\overbrace{p-1, \ldots, p-1}^{r}, t' + 1, p - 1 - u_0, \overbrace{p-1, \ldots, p-1}^{r}, p - t' + 1, p - 2 + u_0]_p \\ &= (\overbrace{p-1, \ldots, p-1}^{r}, 3, p-2, \overbrace{p-1, \ldots, p-1}^{r}, p-1, p-1)_p. \end{aligned}$$

Hence,

$$s_p(e \star d) = 2(r+1)(p-1) + p + 1 = m(p-1) + (r+1)(p-1) + 2 > m(p-1) + s_p(e).$$

If $t' = p-2$, let $h = p^{r+1} - (p-1)$. We then have

$$s_p(e) = s_p(h+1) + s_p(p-1+h) = 2 + r(p-1) + 1 = r(p-1) + 3$$

and

$$2h = 2 - p + p^{r+1} + \sum_{i=1}^{r} (p-1)p^i.$$

If $r > 0$, we obtain

$$\begin{aligned} e \star d \equiv [&p-2, \overbrace{p-1, \ldots, p-1}^{r-1}, t'+1, 2-u_0+p, \\ &p-2, \overbrace{p-1, \ldots, p-1}^{r-1}, p-t'+1, p+1+u_0]_p \\ \equiv [&p-2, \overbrace{p-1, \ldots, p-1}^{r-1}, p-1, 4, p-2, \overbrace{p-1, \ldots, p-1}^{r-1}, 3, p+p-1]_p \\ \equiv (&p-1, \overbrace{p-1, \ldots, p-1}^{r-1}, p-1, 4, p-2, \overbrace{p-1, \ldots, p-1}^{r-1}, 3, p-1)_p \pmod{p^n-1}, \end{aligned}$$

with

$$s_p(e \star d) = 2(r+1)(p-1) + 6 = (r+2)(p-1) + r(p-1) + 6 > m(p-1) + s_p(e).$$

If $r = 0$, then we obtain (using $t' = p-2$ and $u_0 = p-2$) that $e \star d$ is congruent to

$$\begin{aligned} [t', 2-u_0+p, p-t', p+1+u_0]_p &\equiv [p-2, 4, 2, p+p-1]_p \\ &\equiv (p-1, 4, 2, p-1)_p \pmod{p^n-1}. \end{aligned}$$

Hence, $s_p(e \star d) = (r+2)(p-1) + r(p-1) + 6 > m(p-1) + s_p(e)$.

Case $s > 0$**.** Multiplying d by $(p-1)p^m$ modulo $p^n - 1$ yields

$$\begin{aligned} [&\overbrace{0, \ldots, 0}^{r}, t, u_1 - t, \overbrace{u_2 - u_1, u_3 - u_2, \ldots, u_s - u_{s-1}}^{s-1}, p-1-u_s, \\ &\overbrace{0, \ldots, 0}^{r}, -t, -(u_1 - t), \overbrace{-(u_2 - u_1), -(u_3 - u_2), \ldots, -(u_s - u_{s-1})}^{s-1}, p-1+u_s]_p. \end{aligned}$$

Let $e = hp^m + h + 1 + (p-1)p^m$. By addition with term (4.2) from the proof of Lemma 4.3, we obtain that $e \star d$ is congruent to

$$\begin{aligned} [&\overbrace{0, \ldots, 0}^{r}, \quad 2t, 2u_1 - t, \overbrace{2u_2 - u_1, \ldots, 2u_s - u_{s-1}}^{s-1}, 2h - u_s + p, \\ &0, \ldots, 0, p-2t, \overline{2u_1 - t}, \overline{2u_2 - u_1}, \ldots, \overline{2u_s - u_{s-1}}, p-1+2h+u_s]_p. \end{aligned}$$

If $t = p-1$, then we have $2t = p+p-2$, so we can write $e \star d \pmod{p^n-1}$ as

$$[\overbrace{0,\dots,0}^{r}, \quad p-2, 2u_1-(p-2), \overbrace{2u_2-u_1,\dots,2u_s-u_{s-1}}^{s-1}, 2h-u_s+p,$$
$$0,\dots,0,\ p-(p-2), \overline{2u_1-(p-2)}, \overline{2u_2-u_1}, \dots, \overline{2u_s-u_{s-1}}, p-1+2h+u_s]_p.$$

Hence, in any case of $t \in \{1, p-1\}$, we have

$$e \star d \equiv [\overbrace{0,\dots,0}^{r}, \quad t', \overbrace{2u_1-u_0,\dots,2u_s-u_{s-1}}^{s}, 2h-u_s+p,$$
$$0,\dots,0, p-t', \overline{2u_1-u_0}, \dots, \overline{2u_s-u_{s-1}}, p-1+2h+u_s]_p \pmod{p^n-1},$$

where $t' \in \{2, p-2\}$ and $u_0 = 1$ if $t' = 2$ and $u_0 = p-2$ if $t' = p-2$. Define $v = [2u_1-u_0,\dots,2u_s-u_{s-1}]_p$. Note that $v \neq p^s-1$, as $u_0 \neq p-1$. By Lemma 4.4, there exists a δ in $\{-1,0,1\}$ such that $v = (\gamma_1,\dots,\gamma_s)_p - \delta p^s$ with $\gamma_1,\dots,\gamma_s$ in $\{0,\dots,p-1\}$. Hence, $e \star d$ is congruent to

$$[\overbrace{0,\dots,0}^{r}, t', \overbrace{\gamma_1,\dots,\gamma_s}^{s}, 2h-u_s+p-\delta, \overbrace{0,\dots,0}^{r}, p-t', \overbrace{\bar{\gamma}_1,\dots,\bar{\gamma}_s}^{s}, p-1+2h+u_s+\delta]_p.$$

We finish the proof using a case distinction between three subcases corresponding to $u_s \notin \{0,1\}$ and $r=0$, $u_s \notin \{0,1\}$ and $r>0$, and $u_s \in \{0,1\}$.

Subcase $u_s \notin \{0,1\}$ and $r=0$. We choose $h=1$ so that $s_p(e)=3$. We have

$$e \star d = [t'+1, \overbrace{\gamma_1,\dots,\gamma_s}^{s}, p-u_s+2-\delta, p-t', \overbrace{\bar{\gamma}_1,\dots,\bar{\gamma}_s}^{s}, 1+u_s+\delta]_p. \tag{4.3}$$

By assumption, $u_s \in \{p-2, p-1\}$ and $p>5$, so $0 \leqslant p-u_s+2-\delta \leqslant p-1$. Moreover, by Lemma 4.4, $0 \leqslant 1+u_s+\delta \leqslant p-1$. Hence,

$$s_p(e \star d) = (s+2)(p-1)+6 = m(p-1)+6 > m(p-1)+s_p(e).$$

Subcase $u_s \notin \{0,1\}$ and $r>0$. Let $h = ((p-1)/2)\,p^r - (p-1)$. Since

$$s_p(h+1) = r(p-1)-(p-1)/2+1 \qquad \text{and} \qquad s_p(p-1+h) = (p-1)/2,$$

we have

$$s_p(e) = s_p(h+1)+s_p(p-1+h) = r(p-1)+1.$$

Furthermore,

$$2h = (p-1)p^r - 2(p-1) = (p-2)p^r + 2 - p + \sum_{i=1}^{r-1}(p-1)p^i.$$

Hence, $e \star d$ is

$$[\overbrace{p-1,\dots,p-1}^{r-1}, p-2, \quad t', \overbrace{\gamma_1,\dots,\gamma_s}^{s}, 2-u_s-\delta,$$
$$\overbrace{p-1,\dots,p-1}^{r-1}, p-2, p-t', \overbrace{\bar{\gamma}_1,\dots,\bar{\gamma}_s}^{s}, 1+u_s+\delta]_p.$$

To determine the sum of base-p digits of $e \star d$, we use the same argument as for the case $r = 0$ above. If $r - 1 > 0$, then $e \star d$ is equal to

$$(\overbrace{p-1,\dots,p-1}^{r-1}, \qquad p-2, t', \overbrace{\gamma_1,\dots,\gamma_s}^{s}, p-u_s+2-\delta,$$
$$p-2, \overbrace{p-1,\dots,p-1}^{r-2}, p-2, p-t', \overbrace{\bar{\gamma}_1,\dots,\bar{\gamma}_s}^{s}, 1+u_s+\delta)_p.$$

If $r - 1 = 0$, then $e \star d$ equals

$$(p-2, t', \overbrace{\gamma_1,\dots,\gamma_s}^{s}, p-u_s+2-\delta, p-3, p-t', \overbrace{\bar{\gamma}_1,\dots,\bar{\gamma}_s}^{s}, 1+u_s+\delta)_p.$$

In both cases, we obtain $s_p(e \star d) = m(p-1) + r(p-1) + 2 > m(p-1) + s_p(e)$.

Subcase $u_s \in \{0, 1\}$**.** Let $z \in \{1, \dots, s+1\}$ and $h = (p^{r+1+z} - 1) + (p^{r+1} - 1) - (p-1)/2$. Equivalently, $h = p^{r+1+z} - 1 + (p-1)/2 + \sum_{i=1}^{r}(p-1)p^i$. Let us first analyze the sum of base-p digits of e. If $z \neq s+1$, then we have $0 \leqslant p - 1 + h < p^m$ and $0 \leqslant h + 1 < p^m$ with

$$s_p(h+1) = (p-1)/2 + r(p-1) + 1 \qquad \text{and} \qquad s_p(p-1+h) = (p-1)/2,$$

yielding

$$s_p(e) = (r+1)(p-1) + 1.$$

If $z = s+1$, then $r+1+z = m$, so $(p-1+h)p^m + h + 1$ is congruent to

$$\begin{aligned} &\frac{p-1}{2} + \sum_{i=1}^{r}(p-1)p^i + p^m + \left(\frac{p-1}{2} - 2\right)p^m + p^{r+1+m} + 1 \\ \equiv &\left(\frac{p-1}{2} + 1\right) + \sum_{i=1}^{r}(p-1)p^i + \left(\frac{p-1}{2} - 1\right)p^m + p^{r+1+m} \pmod{p^n - 1}. \end{aligned}$$

We take e with $1 \leqslant e \leqslant p^n - 1$ congruent to $(p-1+h)p^m + h + 1$, so that $s_p(e) = (r+1)(p-1)+1$ as well. Multiplying h by 2, we obtain $2h = p^{r+1} + 2p^{r+1+z} - 3 + \sum_{i=1}^{r}(p-1)p^i$. We now consider the cases $(u_s, \delta) \neq (1, 1)$ and $(u_s, \delta) = (1, 1)$ separately.

In case $(u_s, \delta) \neq (1, 1)$, choosing $z = s + 1$ yields

$$\begin{aligned} e \star d \equiv [&\overbrace{p-1,\dots,p-1}^{r}, \qquad t'+1, \overbrace{\gamma_1,\dots,\gamma_s}^{s}, p-u_s-1-\delta, \\ &p-1,\dots,p-1, p-t'+1, \bar{\gamma}_1,\dots,\bar{\gamma}_s, p-2+u_s+\delta]_p \pmod{p^n-1}. \end{aligned}$$

From Lemma 4.4, we have $0 \leqslant u_s + \delta < p - 1$ (note that $v \neq p^s - 1$ as $u_0 \neq p - 1$). Hence, $0 < p-1-u_s-\delta \leqslant p-1$. Furthermore, by assumption $u_s \in \{0, 1\}$ and $(u_s, \delta) \neq (1, 1)$, so $0 \leqslant p - 2 + u_s + \delta \leqslant p - 1$. Hence,

$$e \star d = (\overbrace{p-1,\dots,p-1}^{r}, \quad t'+1, \overbrace{\gamma_1,\dots,\gamma_s}^{s}, p-u_s-1-\delta,$$
$$p-1,\dots,p-1,p-t'+1,\bar{\gamma}_1,\dots,\bar{\gamma}_s,p-2+u_s+\delta)_p,$$

with $s_p(e \star d) = (r+s+2)(p-1)+(r+1)(p-1)+2 > m(p-1)+s_p(e)$.

Finally, let us consider the case $(u_s,\delta) = (1,1)$. By Lemma 4.4, there exists an index j in $\{1,\dots,s\}$ such that $\gamma_j \notin \{0,1,p-2,p-1\}$. By choosing $z=j$, we obtain

$$\begin{aligned} e \star d &= [\overbrace{p-1,\dots,p-1}^{r}, \quad t'+1,\gamma_1,\dots,\gamma_{z-1},\gamma_z+2,\gamma_{z+1},\dots,\gamma_s,p-u_s-3-\delta,\\ &\quad p-1,\dots,p-1,p-t'+1,\bar{\gamma}_1,\dots,\bar{\gamma}_{z-1},\bar{\gamma}_z+2,\bar{\gamma}_{z+1},\dots,\bar{\gamma}_s,p-4+u_s+\delta]_p\\ &= (p-1,\dots,p-1, \quad t'+1,\gamma_1,\dots,\gamma_{z-1},\gamma_z+2,\gamma_{z+1},\dots,\gamma_s,p-5,\\ &\quad p-1,\dots,p-1,p-t'+1,\bar{\gamma}_1,\dots,\bar{\gamma}_{z-1},\bar{\gamma}_z+2,\bar{\gamma}_{z+1},\dots,\bar{\gamma}_s,p-2)_p, \end{aligned}$$

with $s_p(e \star d) = (r+s+2)(p-1)+(r+1)(p-1)+2 > m(p-1)+s_p(e)$. □

For $p=5$, the only situation in which the construction of e in the proof of Lemma 4.5 might fail is when $s>0$ and $u_s \in \{1,p-2\}$. Indeed, if $u_s = p-2$, then $p-u_s+2-\delta$ in expression (4.3) can be equal to p when $\delta=-1$ (then $u_{s-1} \in \{0,1\}$). If $u_s=1$ and $\delta=1$ (i.e., $u_s=1, u_{s-1} \in \{p-2,p-1\}$), then Lemma 4.4 does not guarantee existence of an index j such that $\gamma_j \notin \{0,1,p-2,p-1\}$ if $p=5$.

4.3. Proof of the main result

As already explained by Coulter and Lazebnik in [CL12], an inductive argument now yields the classification of planar monomials over $\mathbb{F}_{p^{2^k}}$ for $p>5$.

Theorem 1.4. *Let k be a non-negative integer and $p>5$. The monomial X^d is planar over $\mathbb{F}_{p^{2^k}}$ if and only if $d \equiv 2p^i \pmod{p^{2^k}-1}$ for some non-negative integer i.*

Proof. Since every monomial X^{2p^i} is planar over $\mathbb{F}_{p^{2^k}}$, we only need to show that any planar monomial X^d over $\mathbb{F}_{p^{2^k}}$ is of the form $d \equiv 2p^i \pmod{p^{2^k}-1}$. The proof is by induction on k. The statement holds for $k \in \{0,1\}$, see [Joh87, Cou06] and our new proofs in Section 3. Suppose that the statement holds for $k-1$ and define $m=2^{k-1}$ and $n=2m=2^k$. If X^d is planar over $\mathbb{F}_{p^n}$, then it must be planar over the subfield $\mathbb{F}_{p^m}$. The induction hypothesis yields $d \equiv 2p^j \pmod{p^m-1}$ for some non-negative integer j. Hence, a cyclic shift of $(d_0+d_m, d_1+d_{m+1},\dots,d_{m-1}+d_{n-1})$ must be in one of the three cases listed in Lemma 4.1, where $d=(d_0,d_1,\dots,d_{n-1})_p$. The only planar monomials in case 1 have exponent $d=2p^i$ for some non-negative integer i. As discussed earlier, case 2 does not contain planar monomials. Finally, Lemma 4.2 implies that case 3 does not contain planar monomials either. □

5. A conjecture on the base-p digit sum of integers

Based on computations, we raise the following conjecture.

Conjecture 5.1. For all positive integers $d \leqslant q-1$ with $d \not\equiv 1 \pmod{p-1}$ and $d \not\equiv \lfloor (p+1)/2 \rfloor \pmod{p-1}$, there exists a positive integer $e \leqslant q-1$ such that

$$s_p(e \star d) - s_p(e) > \frac{n(p-1)}{2}, \tag{5.1}$$

unless

(i) $s_p(d) = 2$, or

(ii) $p = 5$, n odd, and $d = 5^j(5^i+1)/3$ for some non-negative integers i, j.

Note that if either $d \equiv 1 \pmod{p-1}$ or $d \equiv \lfloor (p+1)/2 \rfloor \pmod{p-1}$, then there are many d for which no positive $e \leqslant q-1$ exists such that inequality (5.1) holds. The exceptional case $d = 5^j(5^i+1)/3$ for $p = 5$ resembles the counterexample $d = 3^j(3^i+1)/2$ for $p = 3$ to the original Dembowski–Ostrom conjecture that was found by Coulter and Matthews [CM97].

Conjecture 5.1 has been proven for $n = 1$; see the proof of Corollary 3.3. Moreover, we computationally verified it for all $p \leqslant 800$ if $n = 2$, for all $p \leqslant 400$ if $n = 3$, and, if $n \geqslant 4$, for all (p, n) with $p^n \leqslant 10^9$.

Remark 5.2. In the computational verification, we included non-prime p as well. The only counterexamples we found were for the case $p = 9$ with d of the form $d = 3p^i$.

Some special cases of the conjecture. A proof of the implication in Conjecture 5.1 for any special case of (q, d) shows that the monomial X^d is not planar over $\mathbb{F}_q$. In particular, Conjecture 5.1 for the special case $d \equiv 2 \pmod{p-1}$ implies the classification of planar monomials over finite fields of characteristic $p > 5$.

If $s_p(d) > n(p-1)/2$, then Conjecture 5.1 holds with $e = 1$. We are also able to prove Conjecture 5.1 when $d \equiv r \pmod{p-1}$ and all base-p digits of d are at least r.

Lemma 5.3. *Let $n \geqslant 2$ and $d = (d_0, d_1, \ldots, d_{n-1})_p$. If $d \equiv r \pmod{p-1}$ with $2 \leqslant r \leqslant p-1$ and $d_i \geqslant r$ for all i in $\{0, 1, \ldots, n-1\}$, then there exists a positive integer $e \leqslant q-1$ such that*

$$s_p(e \star d) - s_p(e) > \frac{n(p-1)}{2}.$$

Proof. Since $d \equiv s_p(d) \pmod{p-1}$, it follows that $s_p(d) = k(p-1) + r$ for a non-negative integer $k \leqslant n$. We can assume $k < n/2$ as otherwise, $s_p(d) - 1 \geqslant n(p-1)/2 + 1$ so that $e = 1$ is sufficient. Multiplying d by $e = \sum_{i=0}^{n-2} p^i$ yields

$$ed \equiv [s_p(d) - d_1, s_p(d) - d_2, \ldots, s_p(d) - d_{n-1}, s_p(d) - d_0]_p \pmod{q-1}.$$

By substituting $s_p(d) = k(p-1) + r$, we get

$$\begin{aligned} ed &\equiv [kp + r - k - d_1, kp + r - k - d_2, \ldots, kp + r - k - d_{n-1}, kp + r - k - d_0]_p \\ &\equiv [r - d_1, r - d_2, \ldots, r - d_{n-1}, r - d_0]_p \\ &\equiv [p - 1 + r - d_1, p - 1 + r - d_2, \ldots, p - 1 + r - d_{n-1}, p - 1 + r - d_0]_p \pmod{q-1}. \end{aligned}$$

Since $d_i \geqslant r$ for all i, then if $d \neq (r, r, \ldots, r)_p$, we have that ed is congruent to

$$(p-1+r-d_1, p-1+r-d_2, \ldots, p-1+r-d_{n-1}, p-1+r-d_0)_p = e \star d.$$

If $d = (r, r, \ldots, r)_p$, then we have $ed = q - 1 = e \star d$. Hence,

$$s_p(e \star d) = n(p-1) + nr - s_p(d) = (n-k)(p-1) + r(n-1) > \frac{n(p-1)}{2} + r(n-1).$$

Since $s_p(e) = n - 1$ and $r \geqslant 1$, the result follows. □

This yields the following corollary on the non-planarity of monomials.

Corollary 5.4. *Let $n \geqslant 2$ and $d = (d_0, d_1, \ldots, d_{n-1})_p$. If $d_i > 1$ for all i in $\{0, 1, \ldots, n-1\}$, then X^d is not planar over $\mathbb{F}_q$.*

Acknowledgements

We thank the anonymous reviewers for their helpful comments and suggestions.

References

[Ax64] James Ax. Zeroes of polynomials over finite fields. *Am. J. Math.*, 86(2):255–261, 1964. doi:10.2307/2373163.

[BCV22] Emily Bergman, Robert S. Coulter, and Irene Villa. Classifying planar monomials over fields of order a prime cubed. *Finite Fields Their Appl.*, 78:101959, 2022. doi:10.1016/J.FFA.2021.101959.

[Bey21] Tim Beyne. A geometric approach to linear cryptanalysis. In Mehdi Tibouchi and Huaxiong Wang, editors, *Advances in Cryptology - ASIACRYPT 2021*, volume 13090 of *Lecture Notes in Computer Science*, pages 36–66. Springer, 2021. doi:10.1007/978-3-030-92062-3_2.

[Bey23] Tim Beyne. *A geometric approach to symmetric-key cryptanalysis*. PhD thesis, KU Leuven, 2023.

[BV24] Tim Beyne and Michiel Verbauwhede. Ultrametric integral cryptanalysis. In Kai-Min Chung and Yu Sasaki, editors, *Advances in Cryptology - ASIACRYPT 2024*, volume 15490 of *Lecture Notes in Computer Science*, pages 392–423. Springer, 2024. doi:10.1007/978-981-96-0941-3_13.

[CD01] Claude Carlet and Sylvie Dubuc. On generalized bent and q-ary perfect non-linear functions. In Dieter Jungnickel and Harald Niederreiter, editors, *Finite Fields and Applications*, pages 81–94. Springer, 2001. doi:10.1007/978-3-642-56755-1_8.

[CDY05] Claude Carlet, Cunsheng Ding, and Jin Yuan. Linear codes from perfect nonlinear mappings and their secret sharing schemes. *IEEE Trans. Inf. Theory*, 51(6):2089–2102, 2005. doi:10.1109/TIT.2005.847722.

[CH08] Robert S. Coulter and Marie Henderson. Commutative presemifields and semifields. *Adv. Math.*, 217(1):282–304, 2008. doi:10.1016/j.aim.2007.07.007.

[CL12] Robert S. Coulter and Felix Lazebnik. On the classification of planar monomials over fields of square order. *Finite Fields Their Appl.*, 18(2):316–336, 2012. doi:10.1016/J.FFA.2011.09.002.

[CM97] Robert S. Coulter and Rex W. Matthews. Planar functions and planes of Lenz-Barlotti class II. *Des. Codes Cryptogr.*, 10(2):167–184, 1997. doi:10.1023/A:1008292303803.

[Cou06] Robert Coulter. The classification of planar monomials over fields of prime square order. *Proc. Am. Math. Soc.*, 134(11):3373–3378, 2006. doi:10.1090/s0002-9939-06-08346-8.

[CV02] Anne Canteaut and Marion Videau. Degree of composition of highly nonlinear functions and applications to higher order differential cryptanalysis. In Lars R. Knudsen, editor, *Advances in Cryptology - EUROCRYPT 2002*, volume 2332 of *Lecture Notes in Computer Science*, pages 518–533. Springer, 2002. doi:10.1007/3-540-46035-7_34.

[Ded31] Richard Dedekind. Ideale in Normalkörpern. In Robert Fricke, Emmy Noether, and Øystein Ore, editors, *Gesammelte mathematische Werke, Zweiter Band*. Friedrich Vieweg & Sohn, Braunschweig, 1931.

[DGV95] Joan Daemen, René Govaerts, and Joos Vandewalle. Correlation matrices. In Bart Preneel, editor, *Fast Software Encryption: Second International Workshop. Leuven, Belgium, 14-16 December 1994, Proceedings*, volume 1008 of *Lecture Notes in Computer Science*, pages 275–285. Springer, 1995. doi:10.1007/3-540-60590-8_21.

[DO68] Peter Dembowski and Thedore G. Ostrom. Planes of order n with collineation groups of order n^2. *Math. Z.*, 103(3):239–258, 1968. doi:10.1007/BF01111042.

[GK23] Faruk Göloğlu and Lukas Kölsch. An exponential bound on the number of non-isotopic commutative semifields. *Trans. Am. Math. Soc.*, 376(03):1683–1716, 2023. doi:10.1090/tran/8785.

[Glu90] David Gluck. A note on permutation polynomials and finite geometries. *Discret. Math.*, 80(1):97–100, 1990. doi:10.1016/0012-365X(90)90299-W.

[Hir89] Yutaka Hiramine. A conjecture on affine planes of prime order. *J. Comb. Theory, Ser. A*, 52(1):44–50, 1989. doi:10.1016/0097-3165(89)90060-5.

[Hou04a] Xiang-Dong Hou. A note on the proof of Niho's conjecture. *SIAM J. Discrete Math.*, 18(2):313–319, 2004. doi:10.1137/S0895480103432817.

[Hou04b] Xiang-Dong Hou. p-ary and q-ary versions of certain results about bent functions and resilient functions. *Finite Fields Their Appl.*, 10(4):566–582, 2004. doi:10.1016/J.FFA.2003.12.004.

[HS97] Tor Helleseth and Daniel Sandberg. Some power mappings with low differential uniformity. *Appl. Algebra Eng. Commun. Comput.*, 8(5):363–370, 1997. doi:10.1007/S002000050073.

[HX01] Henk D. L. Hollmann and Qing Xiang. A proof of the Welch and Niho conjectures on cross-correlations of binary m-sequences. *Finite Fields Their Appl.*, 7(2):253–286, 2001. doi:10.1006/ffta.2000.0281.

[Joh87] Norman L. Johnson. Projective planes of prime order p that admit collineation groups of order p^2. *J. Geom.*, 30:49–68, 1987. doi:10.1007/BF01223263.

[Kob84] Neal Koblitz. *p-adic Numbers, p-adic Analysis, and Zeta-Functions*. Graduate Texts in Mathematics. Springer Science & Business Media, 2nd edition, 1984. doi:10.1007/978-1-4612-1112-9.

[Lan90] Serge Lang. *Cyclotomic fields I and II*. Graduate Texts in Mathematics. Springer Science & Business Media, 2nd edition, 1990. doi:10.1007/978-1-4612-0987-4.

[LN96] Rudolf Lidl and Harald Niederreiter. *Finite Fields*. Encyclopedia of Mathematics and its Applications. Cambridge University Press, 2nd edition, 1996. doi:10.1017/CBO9780511525926.

[LV05] Philippe Langevin and Pascal Véron. On the non-linearity of power functions. *Des. Codes Cryptogr.*, 37(1):31–43, 2005. doi:10.1007/S10623-004-3803-9.

[McE71] Robert J. McEliece. On periodic sequences from GF(q). *J. Comb. Theory, Ser. A*, 10(1):80–91, 1971. doi:10.1016/0097-3165(71)90066-5.

[McE72] Robert J. McEliece. Weight congruences for p-ary cyclic codes. *Discrete Math.*, 3(1-3):177–192, 1972. doi:10.1016/0012-365X(72)90032-5.

[Men96] Giampaolo Menichetti. n-dimensional algebras over a field with a cyclic extension of degree n. *Geom. Dedicata*, 63:69–94, 1996. doi:10.1007/BF00181186.

[Pot16] Alexander Pott. Almost perfect and planar functions. *Des. Codes Cryptogr.*, 78(1):141–195, 2016. doi:10.1007/S10623-015-0151-X.

[RS89] Lajos Ronyai and Tamás Szőnyi. Planar functions over finite fields. *Combinatorica*, 9:315–320, 1989. doi:10.1007/BF02125898.

[Ste16] Benjamin Steinberg. *Representation theory of finite monoids*. Universitext. Springer Cham, 2016. doi:10.1007/978-3-319-43932-7.

[Sti90] Ludwig Stickelberger. Ueber eine Verallgemeinerung der Kreistheilung. *Math. Ann.*, 37:321–367, 1890. doi:10.1007/BF01721360.

[WQWX07] Guobiao Weng, Weisheng Qiu, Zeying Wang, and Qing Xiang. Pseudo-Paley graphs and skew Hadamard difference sets from presemifields. *Des. Codes Cryptogr.*, 44(1-3):49–62, 2007. doi:10.1007/S10623-007-9057-6.

[Zie15] Michael E. Zieve. Planar functions and perfect nonlinear monomials over finite fields. *Des. Codes Cryptogr.*, 75:71–80, 2015. doi:10.1007/s10623-013-9890-8.