Finite Fields and Their Applications 78 (2022) 101959

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Classifying planar monomials over fields of order a prime cubed

Emily Bergman [a], Robert S. Coulter [a,*,1], Irene Villa [b,c,2]

[a] Department of Mathematical Sciences, University of Delaware, Newark, DE, USA
[b] Department of Informatics, University of Bergen, Bergen, Norway
[c] Department of Mathematics, University of Trento, Trento, Italy

ARTICLE INFO

Article history:
Received 22 April 2021
Received in revised form 18 August 2021
Accepted 3 November 2021
Available online xxxx
Communicated by Gary McGuire

MSC:
11T06
12E10
51E15

Keywords:
Planar functions
Permutation polynomials
Projective planes

ABSTRACT

Using Hermite's criteria, we classify planar monomials over fields of order a prime cubed, establishing the Dembowski-Ostrom conjecture for monomials over fields of such orders.

1. Preamble

Let q be a power of some odd prime p. We use $\mathbb{F}_q$ to denote the finite field of q elements and the ring of polynomials in x over $\mathbb{F}_q$ is denoted $\mathbb{F}_q[x]$. Let $f \in \mathbb{F}_q[x]$. A polynomial

* Corresponding author.
E-mail address: coulter@udel.edu (R.S. Coulter).

[1] R.S. Coulter was partially supported by the National Science Foundation, award #1855723.
[2] I. Villa was partially supported by the Research Council of Norway, grant #247742/070, and the Trond Mohn stiftelse (TMS) Foundation.

https://doi.org/10.1016/j.ffa.2021.101959
1071-5797/

$f \in \mathbb{F}_q[x]$ is a *permutation polynomial (PP)* over $\mathbb{F}_q$ if f induces a bijection of $\mathbb{F}_q$ under the evaluation map $y \mapsto f(y)$. Permutation polynomials have undoubtably been a hot topic over the past 40 years and there are a number of surveys giving overviews of these results, the most recent of which we believe to be the survey of Hou [11].

A polynomial f is called *planar* if for every $a \in \mathbb{F}_q^\star$, the difference operator $\Delta_f(x,a) = f(x+a) - f(x)$ is a PP over $\mathbb{F}_q$. In this paper we are specifically interested in planar monomials x^n over $\mathbb{F}_q$. As was noted by Coulter and Matthews in [5], the condition for planarity simplifies significantly in the monomial case. Specifically, x^n is *planar* over $\mathbb{F}_q$ if and only if the polynomial $(x+1)^n - x^n$ is a permutation polynomial. Planar functions were introduced in a more general context by Dembowski and Ostrom [6], while studying projective planes with a collineation group acting transitively on the affine points. In [6], the authors questioned whether, ignoring constants and linearised terms x^{p^i}, the only planar functions over finite fields necessarily had the form

$$\sum_{i,j} a_{ij} x^{p^i+p^j},$$

a form nowadays commonly referred to as a Dembowski-Ostrom (DO) polynomial, or quadratic polynomial. This query is nowadays called the Dembowski-Ostrom conjecture. At the time of writing, the status of this conjecture is as follows:

- ⊡ Over prime fields it has been proved in full, independently by Gluck [8], Hiramine [10], and Rónyai and Szönyi [14]. It should be mentioned that the monomial case was established earlier, by Johnson [12].
- ⊡ Over fields of order p^2 it has been proved for monomials by Coulter [3].
- ⊡ Over fields of order p^4, with $p \geq 5$, it has been proved for monomials by Coulter and Lazebnik [4].
- ⊡ Over fields of characteristic 3 it is false. This was shown by Coulter and Matthews [5], who provided an infinite class of counterexamples, the smallest counterexample being x^{14} over $\mathbb{F}_{3^4}$.
- ⊡ Zieve [15] gives a classification of those monomials that are planar over infinitely many extension fields of $\mathbb{F}_p$, known as exceptionally planar monomials. In particular, this gives a classification of all planar monomials x^n over $\mathbb{F}_q$ when $(n-1)^4 \leq q$, as any such planar monomial is necessarily exceptional. His result yields only the DO monomials and the monomials of Coulter and Matthews mentioned above.

While the prime field classification of planar monomials gives a small impact on the classification for any finite field – specifically that if x^n is planar over $\mathbb{F}_{p^e}$, then $n \equiv 2 \bmod (p-1)$ – taking into account the results of Coulter [3] and Zieve [15] it can be seen that p^3 is the only field order for which we have no additional supporting evidence for the DO conjecture for monomials. In this article, we fill this gap by giving a complete classification of planar monomials over fields of order p^3, establishing the DO conjecture in this case. That is, in this article we prove

Theorem 1. *Let $q = p^3$ with p an odd prime. The monomial x^n is planar over $\mathbb{F}_q$ if and only if $n \equiv p^i + p^j \bmod (q-1)$ with $0 \leq i, j < 3$.*

Since for fields of order p, p^2 and p^4 with $p \geq 5$, the only planar monomials possible yield the Desarguesian plane, our result is the first classification result on planar functions which allows for a non-Desarguesian example. The planar monomial x^{p+1} constructs Albert's twisted field plane of order p^3. It is almost certain that the additional possibility is one of the reasons obtaining a classification of planar monomials over fields of order p^3 turns out to be so much more involved than the equivalent result for fields of order p^4.

The approach taken is similar to the previous classification results, whereby Hermite's criteria is used in a number of cases to eliminate all potential exponents that are not DO exponents. Our proof falls into three main cases, with one of the cases very much more complicated than the other two. In the next section we show how the problem can be broken into these three cases. In Section 3, we resolve the two easier cases. The remainder of the paper considers the more difficult remaining case. In Section 4 we outline how the remaining case is broken down and resolved; there are 2 main subcases. For the first of the 2 main subcases, we end up applying Hermite's criteria with 2 exponents and playing the results off against one another. We do not know of a previous instance of the criteria being used in this way. These results can be found in Section 5. For the remaining main subcase, a first application of Hermite's criteria eliminates all but 11 explicit exponents, see Section 6. These remaining 11 exponents we must contend with individually. The remainder of the paper, the admittedly long Section 7, proceeds through the elimination of these 11 subcases.

2. The basic principles of our approach

We wish to consider the planarity of x^n over $\mathbb{F}_q$. This involves examining the permutation behaviour of the polynomial $f_n(x) = (x+1)^n - x^n$. As planarity is a property of functions (polynomials under evaluation, if you prefer), we need only consider $n < q$. In fact, we may insist on $n \leq q-3$ as it is a necessary condition of planarity that $\gcd(n, q-1) = 2$, see [5], Proposition 2.4. We assume this throughout the paper.

In regards to studying permutation polynomials, we have the following criteria for a polynomial to be one, commonly known as Hermite's criteria.

Lemma 1 *(Hermite, [9]; Dickson, [7]). A polynomial $f \in \mathbb{F}_q[x]$, $q = p^e$, is a permutation polynomial over $\mathbb{F}_q$ if and only if*

(i) f has exactly one root in $\mathbb{F}_q$, and
(ii) the reduction of $f^t \bmod (x^q - x)$, with $0 < t < q-1$ and $t \not\equiv 0 \bmod p$, has degree less than $q-1$.

The t in this lemma is often referred to as Hermite exponent. Hermite's criteria is one of the few general statements for testing whether a polynomial is a PP. It can often be unwieldy, and over time has come to be viewed as not particularly effective. That said, there has been a recent revival in its use, with several results being obtained using it, such as the classifications of planar monomials over fields of order p^2 [3] and p^4 [4], and the results of Chou and Hou [2].

There are several points about Hermite's criteria and our specific problem which we now expand on. For arbitrary $0 < t < q-1$, we may write $f_n(x)^t \bmod (x^q - x)$ as

$$f_n^t \bmod (x^q - x) = \sum_{i=0}^{t} \binom{t}{i} (-1)^{t-i} \left[(x+1)^{ni} \bmod (x^q - x)\right] \left[x^{n(t-i)} \bmod (x^q - x)\right], \tag{1}$$

and first reduce each of the terms $(x+1)^{ni}$ and $x^{n(t-i)}$ independently. Subsequently, unless both terms have degree $q-1$, the only way in which we can obtain x^{q-1} terms in the reduced form of $f_n(x)^t$ is via the actual x^{q-1} term generated. This allows for much simplication in our arguments, and in what follows we shall rely on it consistently without further explanation.

The value of binomial coefficients, whether it be in (1) or in the expansion of $(x+1)^{ni}$, is clearly something we will need to handle. Fortunately, we have the following classical result of Lucas at our disposal.

Lemma 2 *(Lucas, [13]). Let p be a prime and $\alpha \geq \beta$ be positive integers with α and β having base-p expansions $\alpha = (\alpha_t \cdots \alpha_0)_p$ and $\beta = (\beta_t \cdots \beta_0)_p$, respectively. Then*

$$\binom{\alpha}{\beta} \equiv \prod_{i=0}^{t} \binom{\alpha_i}{\beta_i} \bmod p,$$

where we use the convention $\binom{n}{k} = 0$ if $n < k$.

The theorem of Lucas encourages us to consider our exponent n in its base p expansion form. Set $n = (a_{e-1} \cdots a_0)_p$, with $0 \leq a_i < p$ for all i. There are several advantages in considering the base p expansion of n, over and above the possibility of applying Lucas' Theorem.

Firstly, x^{np} is planar over $\mathbb{F}_q$ if and only if x^n is planar over $\mathbb{F}_q$, and the reduction of x^{np} modulo $x^q - x$ is x^m, where $m = (a_{e-2} \cdots a_0 a_{e-1})_p$. Thus, we may cycle the base p digits of n around and could, for instance, choose to place the largest a_i in the most significant bit.

Secondly, if x^n is planar over $\mathbb{F}_q$, then it is necessarily planar over $\mathbb{F}_p$. This follows at once from observing $f_n \in \mathbb{F}_p[x]$. The classification of planar monomials over $\mathbb{F}_p$ now forces $n \equiv 2 \bmod (p-1)$. This provides the necessary condition

$$a_0 + a_1 + \cdots + a_{e-1} = S \equiv 2 \bmod (p-1).$$

Since $a_i < p$ for all $0 \leq i < e$, we have $S = 2 + k(p-1)$ for some $0 \leq k < e$.

2.1. Fixing our setup and the three main cases

For the rest of the paper we fix $q = p^3$, where p is an odd prime, and consider the planarity of the monomial x^n over $\mathbb{F}_q$. In order to avoid certain degenerate situations later, we further assume $p \geq 11$. The cases $p \in \{3, 5, 7\}$ can easily be checked computationally. We write the base p expansion of the integer n with $0 \leq n < q$ by $n = (a_2 a_1 a_0)_p$. Based on our above discussion, there are three possible cases we must deal with:

Case 1. $S = 2$.
Case 2. $S = 2p$.
Case 3. $S = p + 1$.

The first case will be shown to be the only positive case, in that the latter two cases will prove to be empty of planar examples. The great majority of the paper is spent dealing with Case 3.

3. Resolution of Cases 1 and 2

Coulter and Matthews showed $x^{p^i+p^j}$ is planar over $\mathbb{F}_{p^e}$ if and only if $e/\gcd(j-i, e)$ is odd, see [5], Theorem 3.3. This completely resolves Case 1.

Proposition 1. *If $S = 2$, then $n = p^i + p^j$ with $0 \leq i \leq j < 3$, and x^n is always planar over $\mathbb{F}_q$.*

The case $S = 2p$ is also relatively straightforward, the proof following very similarly to the classification of planar monomials over $\mathbb{F}_{p^2}$, even down to the exponent used in [3].

Proposition 2. *If $S = 2p$, then x^n is never planar over $\mathbb{F}_q$.*

Proof. For this case we must have $a_i \geq 2$ for all i and $a_i + a_j > p$ whenever $i \neq j$. We prove Hermite's criteria fails with power $t = p + 1$. We have

$$((x+1)^n - x^n)^t = (x+1)^{n(p+1)} - (x+1)^{np}x^n - (x+1)^n x^{np} + x^{n(p+1)}.$$

We determine the coefficient of x^{q-1} for each of these terms modulo $x^q - x$. Raising a term x^k to the p and reducing modulo $x^q - x$ results in a term with degree a cyclic shift of the base p expansion of k. Thus, for example, we can calculate x^{np} modulo $x^q - x$ easily as an interim step in determining $x^{n(p+1)}$ mod $(x^q - x)$. Proceeding as described we see

$$x^{n(p+1)} = x^{np}x^n \equiv x^{a_2 + a_0 p + a_1 p^2} x^{a_0 + a_1 p + a_2 p^2} \bmod (x^q - x).$$

Set $k = (a_2 + a_0) + (a_0 + a_1)p + (a_1 + a_2)p^2$. Now $n < q - 1$, so that $k < 2(q - 1)$. On the other hand, we also know $a_1 + a_2 > p$, so that $k > q$. Consequently, $x^k \bmod (x^q - x)$ reduces to a term of degree not equal to $q - 1$.

We move to consider the remaining three terms. We note that, as a consequence of Lemma 2, we may write

$$(x+1)^n = \sum_{\alpha_0=0}^{a_0} \sum_{\alpha_1=0}^{a_1} \sum_{\alpha_2=0}^{a_2} \left(\prod_{i=0}^{2} \binom{a_i}{\alpha_i} \right) x^{\alpha_0 + \alpha_1 p + \alpha_2 p^2}.$$

Following a similar method as above, we see that the coefficient of the term of degree $q - 1$ in $(x + 1)^n x^{np} \bmod (x^q - x)$ is

$$\prod_{i=0}^{2} \binom{a_i}{\alpha_i} \bmod p,$$

where $\alpha_0 + a_2 = \alpha_1 + a_0 = \alpha_2 + a_1 = p - 1$. Since $a_i \leq p - 1$, it is clear this coefficient is non-zero. The same argument both shows that the coefficient of the term of degree $q - 1$ in $(x + 1)^{np} x^n \bmod (x^q - x)$ is

$$\prod_{i=0}^{2} \binom{a_i}{\alpha_i} \bmod p,$$

with $a_0 + \alpha_2 = a_1 + \alpha_0 = a_2 + \alpha_1 = p - 1$, and that this coefficient is nonzero also. We note that the two coefficients for x^{q-1} so far determined are, in fact, equal, so that their sum is nonzero modulo p.

The situation for $(x+1)^{n(p+1)}$ is slightly more complicated but still relatively straightforward. Expanding in much the same way as above, it can be seen that the coefficients of resulting terms of degree x^{q-1} in $(x + 1)^{n(p+1)} \bmod (x^q - x)$ are given by

$$\prod_i \prod_j \binom{a_i}{\alpha_i} \binom{a_j}{\beta_j}$$

where $\alpha_0 + \beta_2 = \alpha_1 + \beta_0 = \alpha_2 + \beta_1 = p - 1$. Along with these equations, the bounds on α_i, β_j reduce the resulting coefficient of x^{q-1} in $(x + 1)^{n(p+1)} \bmod (x^q - x)$ to

$$\sum_{\alpha_0=p-1-a_2}^{a_0} \sum_{\alpha_1=p-1-a_0}^{a_1} \sum_{\alpha_2=p-1-a_1}^{a_2} \left(\prod_{i=0}^{2} \binom{a_i}{\alpha_i} \right) \binom{a_0}{p-1-\alpha_1} \binom{a_1}{p-1-\alpha_2} \binom{a_2}{p-1-\alpha_0}.$$

We may rearrange this:

$$\left(\sum_{\alpha_0=p-1-a_2}^{a_0}\binom{a_0}{\alpha_0}\binom{a_2}{p-1-\alpha_0}\right)\left(\sum_{\alpha_1=p-1-a_0}^{a_1}\binom{a_1}{\alpha_1}\binom{a_2}{p-1-\alpha_1}\right)$$
$$\times\left(\sum_{\alpha_2=p-1-a_1}^{a_2}\binom{a_2}{\alpha_2}\binom{a_2}{p-1-\alpha_2}\right).$$

Recalling $a_0+a_2>p$ and $a_i\le p-1$ for all i, we have

$$\begin{aligned}\sum_{\alpha_0=p-1-a_2}^{a_0}\binom{a_0}{\alpha_0}\binom{a_2}{p-1-\alpha_0} &= \sum_{j=p-1}^{a_0+a_2}\binom{a_0}{j-a_2}\binom{a_2}{p-1-(j-a_2)}\\ &= \binom{a_0+a_2}{p-1}\\ &\equiv 0 \bmod p.\end{aligned}$$

Thus the coefficient of x^{q-1} in $(x+1)^{n(p+1)} \bmod (x^q-x)$ is zero.

From the above calculations we see the coefficient of x^{q-1} in $((x+1)^n-x^n)^t \bmod (x_q-x)$ is

$$-2\binom{a_0}{p-1-a_2}\binom{a_1}{p-1-a_0}\binom{a_2}{p-1-a_1}\not\equiv 0 \bmod p.$$

By Hermite's criteria, $(x+1)^n-x^n$ is not a permutation polynomial. Thus x^n is not planar in this case. □

The techniques and ideas used in this proof will occur repeatedly in our remaining proofs.

4. Outline of Case 3 resolution

The remainder of the paper will solely be aimed at proving

Proposition 3. *If $S=p+1$, then x^n is never planar over $\mathbb{F}_q$.*

To establish this statement, we will have to resort to dealing with a number of subcases involving a number of Hermite exponents. (Computational evidence shows there is no possible exponent that will work in all cases. Extensive testing was done before we were able to arrive at the "small" number of Hermite exponents used in our proof.) Recall $n=a_0+pa_1+a_2p^2$. A synthesis of our proof of Proposition 3 is as follows. We assume $S=a_0+a_1+a_2=p+1$ with $a_2\ge a_0,a_1$. We then proceed through a sequence of Hermite's exponents. There are two scenarios.

4.1. All of the a_i are at least 2

In this scenario, we determine the coefficient of x^{q-1} in (1) for the exponent $t=2+p+p^2$ when $2\le a_0,a_1\le a_2$. The situation splits into two subcases based on whether

$a_2 > (p-1)/2$ or $a_2 \leq (p-1)/2$. In the former subcase, the coefficient is clearly non-zero, and so there are no planar monomials in this subcase. When $a_2 \leq (p-1)/2$ we also determine the coefficient of x^{q-1} in (1) for the exponent $t = 2+2p$. We then show that the coefficients of x^{q-1} for $t = 2+2p$ and for $t = 2+p+p^2$ cannot be zero simultaneously, thereby showing that this subcase contains no planar monomials. This concludes the situation where all of the a_i are at least 2. The actual results pertaining to this scenario can be found in Section 5.

4.2. At least one of the a_i is less than 2

In this final situation, we first determine the coefficient of x^{q-1} in (1) for the exponent $t = 2+2p+2p^2$ when at least one of a_0 and a_1 is less than 2. This eliminates many situations, but leaves us with 11 explicit subcases to deal with. We then eliminate the remaining explicit 11 subcases using various Hermite's exponents. This is without doubt the most protracted bit of the proof. The details of these results can be found in the remaining sections.

We again note that calculating $x^{n\alpha} \bmod (x^q - x)$ is the same as calculating $n\alpha \bmod (q-1)$, and that $np \bmod (q-1)$ results in simply a cyclic shift of the base p coefficients. That is, $np \bmod (q-1) = (a_1\ a_0\ a_2)_p$. Additionally, if a b_i in $n\alpha = (b_2\ b_1\ b_0)$ is at least p, say b_2, then determining the base p description of $n\alpha$ results in a subtraction of p from the 1st coordinate, and an adding of 1 to the 3rd coordinate. That is $(b_2\ b_1\ b_0)_p \bmod (q-1) = ((b_2-p)\ b_1\ (b_0+1))_p$. We will refer to such an occurrence as a carry. There is a clear abuse of notation that we use with regards to the base p expansion in this regard. We will, without further explanation, move carries around, and reduce modulo $q-1$ without use of congruence notation.

5. Case 3 when $a_i \geq 2$ for $i = 0, 1, 2$

In this section, we assume $2 \leq a_0, a_1 \leq a_2$. This forces $a_2 \leq p-3$. We need to deal with two Hermite exponents.

5.1. The Hermite exponent $t = 2+p+p^2$

Via Lucas' Theorem, the non-zero binomial coefficients in (1) correspond to the terms $(x+1)^{n\alpha}x^{n\beta}$ and $(x+1)^{n\beta}x^{n\alpha}$ in the following table:

α	β
$2+p+p^2$	0
$1+p+p^2$	1
$p+p^2$	2
$2+p^2$	p
$1+p^2$	$1+p$
p^2	$2+p$

We proceed to work through these six scenarios. Recall that the only way we can obtain an x^{q-1} term in the reduced form of $f_n(x)^t$ having already reduced $(x+1)^{n\alpha}$ and $x^{n\beta}$, is from the x^{q-1} term in the product of $(x+1)^{n\alpha}$ and $x^{n\beta}$. We note that to obtain such a term, the sum of the corresponding coordinates of $n\alpha$ and $n\beta$ must be at least $p-1$ in each case.

5.1.1. $\alpha = 2 + p + p^2$ *and* $\beta = 0$

We have

$$\begin{aligned} n\alpha &= 2a_0 + a_1 + 2a_2 + p(2a_1 + a_2 + a_0) + p^2(2a_2 + a_0 + a_1) \\ &= p + 1 + a_0 + p(p + 1 + a_1) + p^2(p + 1 + a_2) \\ &= 2 + a_0 + p(2 + a_1) + p^2(2 + a_2). \end{aligned}$$

To have an x^{q-1} term from $(x+1)^{n\alpha}$ or $x^{n\alpha}$, we would need $2 + a_i = p - 1$ for $i = 0, 1, 2$. But this is impossible under the restriction $a_0 + a_1 + a_2 = p + 1$ and $p \geq 11$. So we obtain no x^{q-1} term from this scenario.

5.1.2. $\alpha = 1 + p + p^2$ *and* $\beta = 1$

We have

$$\begin{aligned} n\alpha &= a_0 + a_2 + a_1 + p(a_1 + a_0 + a_2) + p^2(a_2 + a_1 + a_0) \\ &= 2 + 2p + 2p^2, \text{ and} \\ n\beta &= a_0 + a_1 p + a_2 p. \end{aligned}$$

Since $n\alpha + n\beta = 2 + a_0 + p(2 + a_1)p + p^2(2 + a_2) < q - 1$, it is clear we cannot obtain an x^{q-1} term from this scenario.

5.1.3. $\alpha = p + p^2$ *and* $\beta = 2$

We have

$$\begin{aligned} n\alpha &= a_2 + a_1 + p(a_0 + a_2) + p^2(a_1 + a_0), \text{ and} \\ n\beta &= 2a_0 + 2a_1 p + 2a_2 p. \end{aligned}$$

If $a_2 > (p-1)/2$. then there is a carry in the first coordinate of $n\beta$ and $a_i < (p-1)/2$ for $i = 0, 1$. Thus $n\beta = 2a_0 + 1 + 2a_1 p + p^2(2a_2 - p)$. However, now the sum of the p^2 coefficients is $a_0 + a_1 + 2a_2 - p = a_2 + 1 < p - 1$. Hence we cannot obtain an x^{q-1} term if $a_2 > (p-1)/2$.

Now suppose $a_2 \leq (p-1)/2$. Then there is no carry in either $n\alpha$ and $n\beta$, and the sum of each coordinate is $a_i + p + 1 > p - 1$. So we must get an x^{q-1} term. For $(x+1)^{n\alpha} x^{n\beta}$, the coefficient of the x^{q-1} term is

$$C_1 = \binom{a_1+a_0}{p-1-2a_2}\binom{a_0+a_2}{p-1-2a_1}\binom{a_2+a_1}{p-1-2a_0}$$
$$= \binom{a_1+a_0}{a_2+2}\binom{a_0+a_2}{a_1+2}\binom{a_2+a_1}{a_0+2}. \tag{2}$$

For $(x+1)^{n\beta}x^{n\alpha}$, the coefficient of the x^{q-1} term is

$$C_2 = \binom{2a_2}{p-1-(a_1+a_0)}\binom{2a_1}{p-1-(a_0+a_2)}\binom{2a_0}{p-1-(a_2+a_1)}$$
$$= \binom{2a_2}{a_2+2}\binom{2a_1}{a_1+2}\binom{2a_0}{a_0+2}. \tag{3}$$

5.1.4. $\alpha = 2+p^2$ *and* $\beta = p$

We have

$$n\alpha = 2a_0 + a_1 + p(2a_1+a_2) + p^2(2a_2+a_0), \text{ and}$$
$$n\beta = a_2 + a_0 p + a_1 p^2.$$

Now $2a_2 + a_0 = a_2 - a_1 + p + 1 > p$, so $n\alpha$ must have a carry. Hence

$$n\alpha = 2a_0 + a_1 + 1 + p(2a_1+a_2) + p^2(a_2 - a_1 + 1).$$

If there is no carry in the 2nd coordinate of $n\alpha$, then the sum of the first coordinates of $n\alpha$ and $n\beta$ is $a_2+1 \leq p-2 < p-1$, so we cannot get an x^{q-1} term if there was no carry in the 2nd coordinate.

If there is a carry in the 2nd coordinate, then the sum of the 2nd coordinates of $n\alpha$ and $n\beta$ could be no larger than

$$2a_1 + a_2 - p + a_0 = a_1 + 1 < p-1,$$

as $a_1 \leq a_2$. Hence we cannot obtain an x^{q-1} term in this situation either.

5.1.5. $\alpha = 1+p^2$ *and* $\beta = 1+p$

We have

$$n\alpha = a_0 + a_1 + p(a_1+a_2) + p^2(a_2+a_0), \text{ and}$$
$$n\beta = a_0 + a_2 + p(a_1+a_0) + p^2(a_2+a_1).$$

There are no carries in either $n\alpha$ or $n\beta$, while the sum of the corresponding coordinates is $a_i + p + 1 > p-1$. So we must obtain an x^{q-1} term. For $(x+1)^{n\alpha}x^{n\beta}$, the coefficient of the x^{q-1} term is

$$C_3 = \binom{a_2+a_0}{p-1-(a_2+a_1)}\binom{a_1+a_2}{p-1-(a_1+a_0)}\binom{a_0+a_1}{p-1-(a_0+a_2)}$$
$$= \binom{a_2+a_0}{a_2+2}\binom{a_1+a_2}{a_1+2}\binom{a_0+a_1}{a_0+2}. \tag{4}$$

For $(x+1)^{n\beta}x^{n\alpha}$, the coefficient of the x^{q-1} term is

$$C_4 = \binom{a_2+a_1}{p-1-(a_2+a_0)}\binom{a_1+a_0}{p-1-(a_1+a_2)}\binom{a_0+a_2}{p-1-(a_0+a_1)}$$
$$= \binom{a_2+a_1}{a_2+2}\binom{a_1+a_0}{a_1+2}\binom{a_0+a_2}{a_0+2}. \tag{5}$$

It is now a simple matter to show $C_3 = C_4$. Indeed, it is enough to expand each of the binomial coefficients in C_3 and C_4 and observe that all numerator and denominator terms pair off.

5.1.6. $\alpha = p^2$ and $\beta = 2+p$

This scenario can be dealt with using an argument very similar to that of the $\alpha = 2+p^2$ and $\beta = p$ scenario. The conclusion will be the same, there is no x^{q-1} term obtained.

5.1.7. Summary of the $t = 2+p+p^2$ exponent

From our analysis of the above scenarios, we see that we have two situations.

- ⊡ If $a_2 > (p-1)/2$, then we only get an x^{q-1} term from the case $\alpha = 1+p^2$, $\beta = 1+p$. In this case, the coefficient of x^{q-1} in $f_n(x)^t \bmod (x^q - x)$ is

$$\binom{2}{1}C_3 + \binom{2}{1}C_4 = 4C_3 \neq 0.$$

  Thus x^n is not planar if $a_2 > (p-1)/2$.
- ⊡ If $a_2 \leq (p-1)/2$, then the coefficient of x^{q-1} in $f_n(x)^t \bmod (x^q - x)$ is

$$4C_3 + C_1 + C_2. \tag{6}$$

5.2. The Hermite exponent $t = 2+2p$

In light of the results for our previous exponent, we further restrict our a_i to the situation where $2 \leq a_0, a_1 \leq a_2 \leq (p-1)/2$.

Via Lucas' Theorem, the non-zero binomial coefficients in (1) correspond to the terms $(x+1)^{n\alpha}x^{n\beta}$ and whenever $\alpha \neq \beta$, $(x+1)^{n\beta}x^{n\alpha}$ in the following table:

α	β
$2+2p$	0
$1+2p$	1
$2p$	2
$2+p$	p
$1+p$	$1+p$

5.2.1. $\alpha = 2+2p$ *and* $\beta = 0$

We have

$$\begin{aligned} n\alpha &= 2a_0 + 2a_2 + p(2a_1 + 2a_0) + p^2(2a_2 + 2a_1) \\ &= 2p + 2 - 2a_1 + p(2p + 2 - 2a_2) + p^2(2p + 2 - 2a_0) \\ &= p + 3 - 2a_1 + p(p + 3 - 2a_2) + p^2(p + 3 - 2a_0). \end{aligned}$$

To obtain an x^{q-1} term in this scenario, we need $p + 3 - 2a_i = p - 1$, so that $a_i = 2$ for $i = 0, 1, 2$, implying $p = 5$. For $p \geq 11$ (as is assumed), we get no x^{q-1} term in this scenario.

5.2.2. $\alpha = 1+2p$ *and* $\beta = 1$

We have

$$\begin{aligned} n\alpha &= a_0 + 2a_2 + p(a_1 + 2a_0) + p^2(a_2 + 2a_1), \text{ and} \\ n\beta &= a_0 + a_1 p + a_2 p^2. \end{aligned}$$

Now $n\alpha$ must have at least one carry, as the sum of its coordinates is $3(a_0 + a_1 + a_2) = 3(p + 1) > 3(p - 1)$. If there are 2 or more carries, then the sum of the coordinates of $n\alpha + n\beta$ will be at most

$$3(p + 1) - 2(p - 1) + a_2 + a_1 + a_0 = 2p + 6 < 3(p - 1) \text{ for } p \geq 11,$$

and so we cannot possibly obtain an x^{q-1} term in that situation.

Suppose, then, there is exactly one carry in $n\alpha$. It can either occur in the 1st or 3rd coordinate of $n\alpha$. If it is in the 1st coordinate, then

$$n\alpha = a_0 + 2a_2 + 1 + p(a_1 + 2a_0) + p^2(a_2 + 2a_1 - p).$$

Now the sum of the p^2 coefficients of $n\alpha$ and $n\beta$ is

$$2a_2 + 2a_1 - p \leq 2(p - 1) - p = p - 2 < p - 1,$$

so we cannot obtain an x^{q-1} term in this scenario. A similar argument shows that the p^0 coefficient carry in $n\alpha$ cannot generate an x^{q-1} term also. Thus we do not obtain an x^{q-1} term in this scenario.

5.2.3. $\alpha = 2p$ and $\beta = 2$

We have

$$n\alpha = 2a_2 + 2a_0 p + 2a_1 p^2, \text{ and}$$
$$n\beta = 2a_0 + 2a_1 p + 2a_2 p^2.$$

There are no carries as $a_i \leq (p-1)/2$. Additionally,

$$2a_i + 2a_j = 2(p+1) - 2a_k \geq 2(p+1) - (p-1) = p + 3 > p - 1,$$

and so we must obtain x^{q-1} terms here. For $(x+1)^{n\alpha} x^{n\beta}$, the coefficient of the x^{q-1} term is

$$C_5 = \binom{2a_2}{p-1-2a_1}\binom{2a_1}{p-1-2a_0}\binom{2a_0}{p-1-2a_2}. \tag{7}$$

For $(x+1)^{n\beta} x^{n\alpha}$, the coefficient of the x^{q-1} term is

$$C_6 = \binom{2a_1}{p-1-2a_2}\binom{2a_0}{p-1-2a_1}\binom{2a_2}{p-1-2a_0}. \tag{8}$$

It is not difficult to show $C_5 = C_6$.

5.2.4. $\alpha = 2 + p$ and $\beta = p$

The argument for this scenario is almost a replica of the argument for $\alpha = 1 + 2p$ and $\beta = 1$. The conclusion will be the same, there is no x^{q-1} term obtained.

5.2.5. $\alpha = 1 + p$ and $\beta = 1 + p$

We have

$$n\alpha = a_0 + a_2 + p(a_1 + a_0) + p^2(a_2 + a_1).$$

As $a_i \leq (p-1)/2$, there are no carries. In this scenario, we must get an x^{q-1} term. For $(x+1)^{n\alpha} x^{n\beta}$, the coefficient of the x^{q-1} term is

$$\begin{aligned} C_7 &= \binom{a_2 + a_1}{p-1-(a_2+a_1)}\binom{a_1 + a_0}{p-1-(a_1+a_0)}\binom{a_0 + a_2}{p-1-(a_0+a_2)} \\ &= \binom{a_2 + a_1}{a_0 - 2}\binom{a_1 + a_0}{a_2 - 2}\binom{a_0 + a_2}{a_1 - 2}. \end{aligned} \tag{9}$$

5.2.6. Summary of the $t = 2 + 2p$ exponent

From our analysis of the above scenarios, we see that the coefficient of x^{q-1} in $f_n(x)^t \bmod (x^q - x)$ is

$$\binom{2}{1}\binom{2}{1} C_7 + C_5 + C_6 = 4C_7 + 2C_5. \tag{10}$$

5.3. Playing the two Hermite exponents $t = 2+p+p^2$ and $t = 2+2p$ against each other

In this final subsection, we shall show that for $2 \leq a_0, a_1 \leq a_2 \leq (p-1)/2$ and $a_0 + a_1 + a_2 = p+1$, it is impossible for both Hermite exponents $t = 2+p+p^2$ and $t = 2+2p$ to fail to generate an x^{q-1} term, and consequently x^n cannot be planar over $\mathbb{F}_q$. The following identity will prove useful.

Lemma 3. *For odd prime p and arbitrary $0 \leq k < p$ we have*

$$(p-1-k)! \equiv \frac{(-1)^{k+1}}{k!} \bmod p.$$

The lemma can be established by first proving

$$\binom{p-1}{k} \equiv (-1)^k \bmod p,$$

using an inductive argument and the identity $\binom{n-1}{k-1} + \binom{n-1}{k} = \binom{n}{k}$. The result then follows from observing $(p-1)! \equiv -1 \bmod p$.

For convenience, we preemptively set

$$\begin{aligned} U &= (a_0+a_2)!\,(a_1+a_0)!\,(a_2+a_1)!, \\ V &= (a_0-2)!\,(a_1-2)!\,(a_2-2)!, \\ W &= (2a_0)!\,(2a_1)!\,(2a_2)!, \end{aligned}$$

and view U, V and W (and hence a_0, a_1, a_2) as elements of $\mathbb{F}_p$. We first derive a relation between U and V. In fact, we prove

Lemma 4. *With $2 \leq a_0, a_1 \leq a_2 \leq (p-1)/2$ and U and V as defined above, we have $UV = -1$.*

Proof. From Lemma 3 we find

$$\begin{aligned} (a_0-2)! &= \frac{(-1)^{a_0-1}}{(p+1-a_0)!} \\ &= \frac{(-1)^{a_0-1}}{(a_1+a_2)!}. \end{aligned}$$

A similar identity can be derived for $(a_1-2)!$ and $(a_2-2)!$. It now follows that

$$\begin{aligned} V &= \frac{(-1)^{a_0+a_1+a_2-3}}{U} \\ &= \frac{-1}{U}, \end{aligned}$$

as claimed. □

Now assume that both the coefficients of x^{q-1}, given in (6) and (10), are zero. We next simplify (6). Taking the equation $4C_3 + C_1 + C_2 = 0$ and multiplying through by $\prod(a_i + 2)!$, we have

$$\begin{aligned} 0 &= 4\frac{U}{V} + \frac{U}{(a_1 + a_2 - a_0 - 2)!\,(a_2 + a_0 - a_1 - 2)!\,(a_0 + a_1 - a_2 - 2)!} + \frac{W}{V} \\ &= 4\frac{U}{V} - UW + \frac{W}{V}, \end{aligned}$$

where we have again used Lemma 3. We therefore find

$$2U + W = 0. \tag{11}$$

Next we shall simplify (10). Taking the equation $2C_7 + C_5 = 0$ and multiplying through by $\prod(p + 3 - 2a_i)!$, we have

$$\begin{aligned} 0 &= 2\frac{U}{V} + \frac{W}{(p - 1 - 2a_0)!\,(p - 1 - 2a_1)!\,(p - 1 - 2a_2)!} \\ &= -2U^2 + (-1)^3 W^2, \end{aligned}$$

again using Lemma 3. From (11) we have $W^2 = 4U^2$, and so $6U^2 = 0$ must hold. However, this is a contradiction as $U \neq 0$ and $p \geq 11$. This means that it is impossible for the Hermite exponents $t = 2 + p + p^2$ and $t = 2 + 2p$ to simultaneously generate a zero coefficient for x^{q-1} in $f_n(x)^t \bmod (x^q - x)$. Hence, x^n cannot be planar when $n = a_0 + a_1 p + a_2 p^2$, $a_0 + a_1 + a_2 = p + 1$ and $2 \leq a_0, a_1 \leq a_2 \leq (p - 1)/2$.

We note that we are unaware of another application of Hermite's criteria which uses two Hermite exponents and two coefficients simultaneously to get a non-PP proof through as we do here.

6. Case 3 when at least one of the a_i is less than 2

We have reached our final scenario, where we know at least one of the a_i is less than 2. Unfortunately, we have more Hermite exponents to deal with in this last situation than in all of the previous work in this paper. This section will deal with only the one Hermite exponent, specifically $t = 2 + 2p + 2p^2$. Using this exponent we can eliminate many of the remaining possible choices for the a_i. However, we shall be left with 11 explicit choices for n.

6.1. The Hermite exponent $t = 2 + 2p + 2p^2$

Assume that $a_2 \geq a_0, a_1$ and $a_0 + a_1 + a_2 = p + 1$. To simplify the equations let $T = 1 + p + p^2$. We have $x^{nT} = x^{(a_0 + a_1 p + a_2 p^2)(1 + p + p^2)} = x^{2T}$. In this case we have

$$\begin{aligned}((x+1)^n - x^n)^{2T} =&(x+1)^{4T} + x^{4T} - 8x^{2T}(x+1)^{2T} \\ &+ A + A^p + A^{p^2} + B + B^p + B^{p^2}, \end{aligned} \tag{12}$$

with

$$\begin{aligned}A =& (x+1)^{n(p^2+1)}x^{np} \\ &\times (4x^{2T} - 2(x+1)^{2T} + (x+1)^{n(p^2+1)}x^{np} - 2x^{n(p^2+p)}(x+1)^n - 2x^{n(p+1)}(x+1)^{np^2}), \\ B =& (x+1)^n x^{n(p^2+p)}(4(x+1)^{2T} - 2x^{2T} + (x+1)^n x^{n(p^2+p)}).\end{aligned}$$

We have

$$\begin{aligned}(x+1)^T =&1 + x + x^p + x^{p^2} + x^{p+1} + x^{p^2+1} + x^{p^2+p} + x^{p^2+p+1}, \\ (x+1)^{2T} =&1 + x^2 + x^{2p} + x^{2p^2} + x^{2(p+1)} + x^{2(p^2+1)} + x^{2(p^2+p)} + x^{2(p^2+p+1)} \\ &+ 2(x + x^p + x^{p^2} + 2x^{p+1} + 2x^{p^2+1} + 2x^{p^2+p} + 4x^{p^2+p+1} \\ &+ x^{p+2} + x^{p^2+2} + 2x^{p^2+p+2} + x^{2p+1} + x^{p^2+2p} + 2x^{p^2+2p+1} \\ &+ x^{2p^2+1} + x^{2p^2+p} + 2x^{2p^2+p+1} + x^{p^2+2p+2} + x^{2p^2+p+2} + x^{2p^2+2p+1}).\end{aligned}$$

We want to show that in equation (12) the only terms of degree $p^3 - 1$ are in A (and A^p, A^{p^2}).

Clearly $(x+1)^{4T} + x^{4T} - 8x^{2T}(x+1)^{2T}$ cannot have a monomial of degree $p^3 - 1$ if $p > 5$.

We rewrite B as $B = 4B_1 - 2B_2 + B_3$ with

$$\begin{aligned}B_1 =&(x+1)^n x^{n(p^2+p)}(x+1)^{2T}, \\ B_2 =&(x+1)^n x^{n(p^2+p)}x^{2T}, \\ B_3 =&(x+1)^{2n}x^{2n(p^2+p)}.\end{aligned}$$

Using

$$(x+1)^n = \sum_{\alpha_0=0}^{a_0}\sum_{\alpha_1=0}^{a_1}\sum_{\alpha_2=0}^{a_2}\prod_{i=0}^{3}\binom{a_i}{\alpha_i}x^{\alpha_0+\alpha_1 p+\alpha_2 p^2}$$

we have

$$B_1 = (x+1)^{2T}\sum_{\alpha_0=0}^{a_0}\sum_{\alpha_1=0}^{a_1}\sum_{\alpha_2=0}^{a_2}\prod_{i=0}^{3}\binom{a_i}{\alpha_i}x^{(\alpha_0+a_1+a_2)+(\alpha_1+a_2+a_0)p+(\alpha_2+a_0+a_1)p^2}.$$

If $a_0 = 0$ (so $a_1 + a_2 = p + 1$), then

$$\begin{aligned}B_1 =&(x+1)^{2T}\sum_{\alpha_1=0}^{a_1}\sum_{\alpha_2=0}^{a_2}\prod_{i=1}^{3}\binom{a_i}{\alpha_i}x^{(a_1+a_2)+(\alpha_1+a_2)p+(\alpha_2+a_1)p^2}\\ =&(x+1)^{2T}\sum_{\alpha_1=0}^{a_1}\sum_{\alpha_2=0}^{a_2}\prod_{i=1}^{3}\binom{a_i}{\alpha_i}x^{(p+1)+(\alpha_1+a_2)p+(\alpha_2+p+1-a_2)p^2}\\ =&(x+1)^{2T}\sum_{\alpha_1=0}^{a_1}\sum_{\alpha_2=0}^{a_2}\prod_{i=1}^{3}\binom{a_i}{\alpha_i}x^{2+(\alpha_1+a_2+1)p+(\alpha_2+1-a_2)p^2}.\end{aligned}$$

Hence it cannot have a term of degree $q-1$.

If $a_0=1$ ($a_1+a_2=p$), then

$$\begin{aligned}B_1 =&(x+1)^{2T}\sum_{\alpha_0=0}^{1}\sum_{\alpha_1=0}^{a_1}\sum_{\alpha_2=0}^{a_2}\prod_{i=1}^{3}\binom{a_i}{\alpha_i}x^{(\alpha_0+a_1+a_2)+(\alpha_1+a_2+1)p+(\alpha_2+1+a_1)p^2}\\ =&(x+1)^{2T}\sum_{\alpha_0=0}^{1}\sum_{\alpha_1=0}^{a_1}\sum_{\alpha_2=0}^{a_2}\prod_{i=1}^{3}\binom{a_i}{\alpha_i}x^{(\alpha_0+p)+(\alpha_1+a_2+1)p+(\alpha_2+1+p-a_2)p^2}\\ =&(x+1)^{2T}\sum_{\alpha_0=0}^{1}\sum_{\alpha_1=0}^{a_1}\sum_{\alpha_2=0}^{a_2}\prod_{i=1}^{3}\binom{a_i}{\alpha_i}x^{(\alpha_0+1)+(\alpha_1+a_2+2)p+(\alpha_2+1-a_2)p^2}.\end{aligned}$$

Hence it cannot have a term of degree $q-1$. The argument is more or less the same for the cases $a_1=0,1$. Moreover, the same arguments work for B_2.

Now we consider B_3. We have

$$\begin{aligned}B_3 =&(x+1)^{2n}x^{2n(p^2+p)}\\ =&\sum\prod\binom{a_i}{\alpha_i}\binom{a_j}{\beta_j}x^{(\alpha_0+\beta_0+2a_1+2a_2)+(\alpha_1+\beta_1+2a_2+2a_0)p+(\alpha_2+\beta_2+2a_0+2a_1)p^2}.\end{aligned}$$

If $a_0=0$ (so $a_1+a_2=p+1$), then

$$\begin{aligned}B_3 =&\sum\prod\binom{a_i}{\alpha_i}\binom{a_j}{\beta_j}x^{2(a_1+a_2)+(\alpha_1+\beta_1+2a_2)p+(\alpha_2+\beta_2+2a_1)p^2}\\ =&\sum\prod\binom{a_i}{\alpha_i}\binom{a_j}{\beta_j}x^{2(p+1)+(\alpha_1+\beta_1+2a_2)p+(\alpha_2+\beta_2+2p+2-2a_2)p^2}\\ =&\sum\prod\binom{a_i}{\alpha_i}\binom{a_j}{\beta_j}x^{4+(\alpha_1+\beta_1+2a_2+2)p+(\alpha_2+\beta_2+2-2a_2)p^2}.\end{aligned}$$

Hence it cannot have a term of degree $q-1$.

If $a_0=1$ ($a_1+a_2=p$), then

$$B_3 =\sum\prod\binom{a_i}{\alpha_i}\binom{a_j}{\beta_j}x^{(\alpha_0+\beta_0+2a_1+2a_2)+(\alpha_1+\beta_1+2a_2+2)p+(\alpha_2+\beta_2+2+2a_1)p^2}$$

$$= \sum \prod \binom{a_i}{\alpha_i}\binom{a_j}{\beta_j} x^{(\alpha_0+\beta_0+2p)+(\alpha_1+\beta_1+2a_2+2)p+(\alpha_2+\beta_2+2+2p-2a_2)p^2}$$
$$= \sum \prod \binom{a_i}{\alpha_i}\binom{a_j}{\beta_j} x^{(\alpha_0+\beta_0+2)+(\alpha_1+\beta_1+2a_2+4)p+(\alpha_2+\beta_2+2-2a_2)p^2}.$$

Hence it cannot have a term of degree $q-1$. Again the $a_1 = 0, 1$ cases are more or less the same.

Let us now consider A. We set

$$A = 4A_1 - 2A_2 + A_3 - 2A_4 - 2A_5,$$

with

$$\begin{aligned}
A_1 &= (x+1)^{n(p^2+1)} x^{np} x^{2T},\\
A_2 &= (x+1)^{n(p^2+1)} x^{np} (x+1)^{2T},\\
A_3 &= (x+1)^{2n(p^2+1)} x^{2np},\\
A_4 &= (x+1)^{n(p^2+2)} x^{n(p^2+2p)},\\
A_5 &= (x+1)^{n(2p^2+1)} x^{n(2p+1)}.
\end{aligned}$$

We will show A_1, A_2, A_3 have no monomial of degree $q-1$.

For A_1 we have

$$\begin{aligned}
A_1 &= (x+1)^{n(p^2+1)} x^{np+2T}\\
&= (x+1)^{(a_0+a_1)+(a_1+a_2)p+(a_2+a_0)p^2} x^{(a_2+2)+(a_0+2)p+(a_1+2)p^2}.
\end{aligned}$$

If $a_0 = 0$, $a_1 + a_2 = p+1$ and

$$\begin{aligned}
A_1 &= (x+1)^{(a_1)+(p+1)p+(a_2)p^2} x^{(a_2+2)+2p+(a_1+2)p^2}\\
&= (x+1)^{(a_1)+p+(a_2+1)p^2} x^{(a_2+2)+2p+(a_1+2)p^2}.
\end{aligned}$$

From this we see this cannot have a monomial of maximal degree.

If $a_0 = 1$, $a_1 + a_2 = p$ and

$$\begin{aligned}
A_1 &= (x+1)^{(a_1+1)+(p)p+(a_2+1)p^2} x^{(a_2+2)+3p+(a_1+2)p^2}\\
&= (x+1)^{(a_1+1)+(a_2+2)p^2} x^{(a_2+2)+3p+(a_1+2)p^2}.
\end{aligned}$$

Again it cannot have a monomial of maximal degree.

For A_2 we have

$$\begin{aligned} A_2 &= (x+1)^{n(p^2+1)+2T} x^{np} \\ &= (x+1)^{(a_0+a_1+2)+(a_1+a_2+2)p+(a_2+a_0+2)p^2} x^{(a_2)+(a_0)p+(a_1)p^2}. \end{aligned}$$

If $a_0 = 0$, $a_1 + a_2 = p + 1$ and

$$\begin{aligned} A_2 &= (x+1)^{(a_1+2)+(p+3)p+(a_2+2)p^2} x^{(a_2)+(0)p+(a_1)p^2} \\ &= (x+1)^{(a_1+2)+3p+(a_2+3)p^2} x^{a_2+a_1p^2}, \end{aligned}$$

and we observe there cannot be a monomial of maximal degree.

If $a_0 = 1$, $a_1 + a_2 = p$ and

$$\begin{aligned} A_2 &= (x+1)^{(a_1+3)+(p+2)p+(a_2+3)p^2} x^{(a_2)+(1)p+(a_1)p^2} \\ &= (x+1)^{(a_1+3)+2p+(a_2+4)p^2} x^{a_2+p+a_1p^2}. \end{aligned}$$

Again we cannot generate a monomial of maximal degree.

For A_3 we have the following:

$$\begin{aligned} A_3 &= (x+1)^{n(2p^2+2)} x^{2np} \\ &= (x+1)^{(2a_0+2a_1)+(2a_1+2a_2)p+(2a_2+2a_0)p^2} x^{(2a_2)+(2a_0)p+(2a_1)p^2}. \end{aligned}$$

If $a_0 = 0$, $a_1 + a_2 = p + 1$ and

$$\begin{aligned} A_3 &= (x+1)^{(2a_1)+(2p+2)p+(2a_2)p^2} x^{(2a_2)+(0)p+(2a_1)p^2} \\ &= (x+1)^{2a_1+2p+(a_2+2)p^2} x^{2a_2+2a_1p^2}. \end{aligned}$$

This cannot have a monomial of maximal degree. If $a_0 = 1$, $a_1 + a_2 = p$ and

$$\begin{aligned} A_3 &= (x+1)^{(2a_1+2)+(2p)p+(2a_2+2)p^2} x^{(2a_2)+2p+(2a_1)p^2} \\ &= (x+1)^{(2a_1+2)+(2a_2+4)p^2} x^{(2a_2)+2p+(2a_1)p^2}. \end{aligned}$$

Again we do not obtain a monomial of maximal degree. Similar arguments deal with A_1, A_2 and A_3 when $a_1 = 0, 1$ too.

For A_4 we have the following:

$$\begin{aligned} A_4 &= (x+1)^{n(p^2+2)} x^{n(p^2+2p)} \\ &= (x+1)^{(2a_0+a_1)+(2a_1+a_2)p+(2a_2+a_0)p^2} x^{(2a_2+a_1)+(2a_0+a_2)p+(2a_1+a_0)p^2}. \end{aligned}$$

The case A_5, up to considering a p power, is symmetrical. Indeed we have

$$\begin{aligned} A_5^{p^2} &= x^{n(p^2+2)}(x+1)^{n(p^2+2p)} \\ &= x^{(2a_0+a_1)+(2a_1+a_2)p+(2a_2+a_0)p^2}(x+1)^{(2a_2+a_1)+(2a_0+a_2)p+(2a_1+a_0)p^2}. \end{aligned}$$

Hence we will just analyse A_4 and then swap the exponents for x and $x+1$. For ease of description, we split this final analysis into four subcases. In each case we use c_4 for the coefficient of x^{q-1} in A_4 and c_5 for the coefficient of x^{q-1} in A_5. We emphasise that there will be a number of exceptions encountered in this final analysis, and these are set aside for later.

- If $a_0 = 0$, then $a_1 + a_2 = p + 1$ and $2 \le a_1 \le \frac{p+1}{2}$. We have

$$\begin{aligned} A_4 &= (x+1)^{(a_1)+(a_1+p+1)p+(2a_2)p^2}x^{(a_2+p+1)+(a_2)p+(2a_1)p^2} \\ &= (x+1)^{(a_1)+(a_1+1)p+(2a_2+1)p^2}x^{(a_2+1)+(a_2+1)p+(2a_1)p^2} \\ &= (x+1)^{(a_1+1)+(a_1+1)p+(2a_2+1-p)p^2}x^{(a_2+1)+(a_2+1)p+(2a_1)p^2}, \end{aligned}$$

  where the last step is due to the fact $\frac{p+1}{2} \le a_2 \le p-1$. If $a_1 = 2$ or $a_1 = (p+1)/2$, then we do not get a maximal degree term here. These two cases will be dealt with later as explicit exponents #10 and #1, respectively. If $3 \le a_1 \le \frac{p-1}{2}$, then all the exponents are smaller than p and we obtain a term with maximal degree, the coefficient of which is

$$c_4 = \binom{a_1+1}{p-1-(a_2+1)}\binom{a_1+1}{p-1-(a_2+1)}\binom{2a_2+1-p}{p-1-(2a_1)}.$$

  For A_5 we have essentially the same situation with coefficient

$$c_5 = \binom{a_2+1}{p-1-(a_1+1)}\binom{a_2+1}{p-1-(a_1+1)}\binom{2a_1}{p-1-(2a_2+1-p)}.$$

  It is not difficult to verify that $c_4 = c_5$.
- If $a_0 = 1$, then $a_1 \neq 0$ $a_1 + a_2 = p$, $1 \le a_1 \le \frac{p-1}{2}$, and

$$\begin{aligned} A_4 &= (x+1)^{(a_1+2)+(a_1+p)p+(2a_2+1)p^2}x^{(a_2+p)+(a_2+2)p+(2a_1+1)p^2} \\ &= (x+1)^{(a_1+2)+(a_1)p+(2a_2+2)p^2}x^{(a_2)+(a_2+3)p+(2a_1+1)p^2} \\ &= (x+1)^{(a_1+3)+(a_1)p+(2a_2+2-p)p^2}x^{(a_2)+(a_2+3)p+(2a_1+1)p^2}, \end{aligned}$$

  where the last step is due to the fact that $\frac{p+1}{2} \le a_2 \le p-1$. We have $a_2 + 3 \ge p$ if $a_1 \le 3$, and $2a_1 + 1 \ge p$ if $a_1 \ge \frac{p-1}{2}$. If $a_1 \le 3$ or $a_1 = (p-1)/2$, then we do not obtain a maximal degree term. These exponents will be dealt with later as the explicit exponents #6, #7, #11 and #3. If $4 \le a_1 \le \frac{p-3}{2}$, then all exponents are smaller than p and we get a maximal degree term with coefficient

$$c_4 = \binom{a_1+3}{p-1-a_2}\binom{a_1}{p-1-(a_2+3)}\binom{2a_2+2-p}{p-1-(2a_1+1)}.$$

For A_5 we have the same situation with coefficient

$$c_5 = \binom{a_2}{p-1-(a_1+3)}\binom{a_2+3}{p-1-a_1}\binom{2a_1+1}{p-1-(2a_2+2-p)}.$$

Again it is not difficult to verify that $c_4 = c_5$.

- If $a_1 = 0$, then $a_0 + a_2 = p+1$, $2 \le a_0 \le \frac{p+1}{2}$, $\frac{p+1}{2} \le a_2 \le p-1$, and

$$\begin{aligned} A_4 &= (x+1)^{(2a_0)+(a_2)p+(a_2+p+1)p^2} x^{(2a_2)+(a_0+p+1)p+(a_0)p^2} \\ &= (x+1)^{(2a_0+1)+(a_2)p+(a_2+1)p^2} x^{(2a_2)+(a_0+1)p+(a_0+1)p^2} \\ &= (x+1)^{(2a_0+1)+(a_2)p+(a_2+1)p^2} x^{(2a_2-p)+(a_0+2)p+(a_0+1)p^2}. \end{aligned}$$

If $a_0 = 2$ or $a_0 \ge (p-1)/2$, then we do not obtain a maximal degree term. These cases will be dealt with later as explicit exponents #9, #2 and #5. If $3 \le a_0 \le \frac{p-3}{2}$, then all the exponents are smaller than p and we obtain a maximal degree term with coefficient

$$c_4 = \binom{2a_0+1}{p-1-(2a_2-p)}\binom{a_2}{p-1-(a_0+2)}\binom{a_2+1}{p-1-(a_0+1)}.$$

For A_5 we have the same situation producing a maximal degree term with coefficient

$$c_5 = \binom{2a_2-p}{p-1-(2a_0+1)}\binom{a_0+2}{p-1-a_2}\binom{a_0+1}{p-1-(a_2+1)}.$$

It is not difficult to verify that $c_4 = c_5$.

- If $a_1 = 1$, then $a_0 \ne 0$, $a_0 + a_2 = p$, $1 \le a_0 \le \frac{p-1}{2}$, and

$$\begin{aligned} A_4 &= (x+1)^{(2a_0+1)+(2+a_2)p+(a_2+p)p^2} x^{(2a_2+1)+(a_0+p)p+(2+a_0)p^2} \\ &= (x+1)^{(2a_0+2)+(2+a_2)p+(a_2)p^2} x^{(2a_2+1-p)+(a_0+1)p+(3+a_0)p^2} \end{aligned}$$

since we have $\frac{p+1}{2} \le a_2 \le p-1$. If $a_0 \le 2$ or $a_0 = (p-1)/2$, then we do not obtain a maximal degree term. These cases will be dealt with later as explicit exponents #8, #11 and #4. If $3 \le a_0 \le \frac{p-3}{2}$, then all the exponents are smaller than p and we obtain a maximal degree term with coefficient

$$c_4 = \binom{2a_0+2}{p-1-(2a_2+1-p)}\binom{a_2+2}{p-1-(a_0+1)}\binom{a_2}{p-1-(a_0+3)}.$$

For A_5 we have the same situation producing a maximal degree term with coefficient

$$c_5 = \binom{2a_2+1-p}{p-1-(2a_0+2)}\binom{a_0+1}{p-1-(a_2+2)}\binom{a_0+3}{p-1-a_2}.$$

It is not difficult to verify that $c_4 = c_5$.

Summarising all the cases above shows that, exceptions aside, the coefficient of the x^{q-1} term is $-4(c_4 + c_4^p + c_4^{p^2}) = -12c_4 \neq 0$. Thus, apart from the 11 explicit cases set aside, no exponent remaining in Case 3 can be planar.

7. Case 3 and the 11 explicit choices for n

From all of the above analysis, we are left with 11 explicit choices for n which need to be eliminated to complete the proof of Proposition 3 and hence Theorem 1. These 11 remaining exponents n are listed here, along with the Hermite exponent t we use to eliminate them.

Exp.#1. $n = \frac{p+1}{2}(p+p^2)$ with $t = (p-2)+p$ and $t = (p-6)+p+4p^2$,
Exp.#2. $n = \frac{p+1}{2}(1+p^2)$ with $t = (p-2)+p$ and $t = (p-6)+p+4p^2$,
Exp.#3. $n = 1+(\frac{p+1}{2}-1)p+\frac{p+1}{2}p^2$ with $t = 2p+4p^2$,
Exp.#4. $n = (\frac{p+1}{2}-1)+p+\frac{p+1}{2}p^2$ with $t = (p-2)+p$,
Exp.#5. $n = (\frac{p+1}{2}-1)+(\frac{p+1}{2}+1)p^2$ with $t = (p-6)+p+2p^2$,
Exp.#6. $n = 1+3p+(p-3)p^2$ with $t = 2+4p+4p^2$,
Exp.#7. $n = 1+2p+(p-2)p^2$ with $t = (p-1)(p+p^2)$,
Exp.#8. $n = 2+p+(p-2)p^2$ with $t = 1+2p+3p^2$,
Exp.#9. $n = 2+(p-1)p^2$ with $t = 1+2p+3p^2$,
Exp.#10. $n = 2p+(p-1)p^2$ with $t = 2+(p-1)p$,
Exp.#11. $n = 1+p+(p-1)p^2$ with $t = p-1$.

In the remainder of this paper, we deal with each of these remaining exponents in turn. As can be observed, we have to resort to some computational tests for certain characteristics $p \geq 11$. Specifically:

- ⊡ Exponents #1 and #2 need to be eliminated computationally for $p = 29$ when $m = (p-1)/2$ is even, and
- ⊡ Exponent #6 needs to be eliminated computationally for $p \leq 17$ and $p = 373$.

We give some details for the $p = 373$ instance, but as the others are computationally trivial we make no further statements about them. Otherwise, our proofs go through under the general condition $p \geq 11$. Throughout our intent is to provide enough detail to show the coefficient of x^{q-1} is non-zero. We give a full account of one exponent (#7, the most involved one), and otherwise sufficient details to outline the proofs in all others. In the following subsections we use the following notations: $m = \frac{p-1}{2}$ and $y = x+1$.

7.1. Exponent #1

7.1.1. With m odd

We have $n = (m+1)p + (m+1)p^2$ and $t = (p-2) + p$. We claim $(y^n - x^n)^t$ has maximal degree with coefficient

$$c_M = -\binom{p-1}{m} = (-1)^{m+1} \neq 0.$$

More details in the following. We have

$$\begin{aligned}(y^n - x^n)^t &= \sum_{i=0}^{p-2} (-1)^{p-2-i} \binom{p-2}{i} y^{ni} x^{n(p-2-i)} (y^{np} - x^{np}) \\ &= \sum_{i=0}^{p-2} (-1)^{p-2-i} \binom{p-2}{i} (A_i - B_i).\end{aligned}$$

Notice that $x^{2n} = x^{1+p+2p^2}$. For $i = 2k$ (with $k = 0, \ldots, m-1$), then we have

$$\begin{aligned}A_{2k} &= y^{(m+1+k)+kp+(m+1+2k)p^2} x^{(m-k)+(p-1-k)p+(m-2-2k)p^2}, \\ B_{2k} &= y^{k+kp+2kp^2} x^{(p-k)+(p-1-k)p+(p-2-2k)p^2}.\end{aligned}$$

We see B_{2k} cannot reach maximal degree, instead A_{2k} reaches maximal degree only when m is odd and $2k = m-1$. If $i = 2k+1$ (with $k = 0, \ldots, m-1$), then we have

$$\begin{aligned}A_{2k+1} &= y^{(m+2+k)+(m+1+k)p+(1+2k)p^2} x^{(m-k-1)+(m-1-k)p+(p-3-2k)p^2}, \\ B_{2k+1} &= y^{k+(k+m+1)p+(m+1+2k)p^2} x^{(p-k)+(m-1-k)p+(m-2-2k)p^2}.\end{aligned}$$

We see that A_{2k+1} cannot reach maximal degree. Instead B_{2k+1} reaches maximal degree only when m is odd and $2k = m-1$. Hence for the term of degree $p^3 - 1$ we have the following coefficient:

$$\begin{aligned}c &= (-1)^{p-2-(m-1)} \binom{p-2}{m-1} - (-1)^{p-2-(m)} \binom{p-2}{m} \\ &= -\binom{p-2}{m-1} - \binom{p-2}{m} = -\binom{p-1}{m} = (-1)^{m+1} \neq 0.\end{aligned}$$

7.1.2. Exponent #1 with m even

We have $n = (m+1)p + (m+1)p^2$ and $t = (p-6) + p + 4p^2$. The case $p = 29$ can be eliminated computationally and we assume $p \neq 29$ for the remainder of this case. We claim $(y^n - x^n)^t$ has maximal degree with coefficient

$$c_M = \frac{1}{2}\binom{p-6}{m-1}\frac{145}{3} \neq 0.$$

More details in the following. In the following we consider only the case m even and set $v = m/2$. We have

$$\begin{aligned}
&(y^n - x^n)^t \\
&\quad = (y^n - x^n)^{p-6}(y^{np} - x^{np})(y^{4np^2} - 4y^{3np^2}x^{np^2} + 6y^{2np^2}x^{2np^2} - 4y^{np^2}x^{3np^2} + x^{4np^2}) \\
&\quad = \sum_{i=0}^{p-6}(-1)^{p-6-i}\binom{p-6}{i} \\
&\qquad \times (A_1^i - 4A_2^i + 6A_3^i - 4A_4^i + A_5^i - B_1^i + 4B_2^i - 6B_3^i + 4B_4^i - B_5^i),
\end{aligned}$$

where

$$\begin{aligned}
A_j^i &= y^{np+n(5-j)p^2}x^{n(j-1)p^2}y^{ni}x^{n(p-6-i)}, \\
B_j^i &= y^{n(5-j)p^2}x^{np+n(j-1)p^2}y^{ni}x^{n(p-6-i)}.
\end{aligned}$$

We consider whether i is even or not. For $i = 2k$ $(0 \leq k \leq m-3)$ we have the following:

$$\begin{aligned}
A_1^{2k} &= y^{(m+3+k)+(k+4)p+(m+3+2k)p^2}x^{(m-2-k)+(p-3-k)p+(m-6-2k)p^2}, \\
B_1^{2k} &= y^{(2+k)+(k+4)p+(2+2k)p^2}x^{(p-2-k)+(p-3-k)p+(p-6-2k)p^2}, \\
A_2^{2k} &= y^{(2+k)+(m+k+4)p+(m+2+2k)p^2}x^{(p-2-k)+(m-2-k)p+(m-5-2k)p^2}, \\
B_2^{2k} &= y^{(m+2+k)+(m+k+3)p+(1+2k)p^2}x^{(m-1-k)+(m-1-k)p+(p-5-2k)p^2}, \\
A_3^{2k} &= y^{(m+2+k)+(k+2)p+(m+2+2k)p^2}x^{(m-1-k)+(p-1-k)p+(m-5-2k)p^2}, \\
B_3^{2k} &= y^{(1+k)+(k+2)p+(1+2k)p^2}x^{(p-1-k)+(p-1-k)p+(p-5-2k)p^2}, \\
A_4^{2k} &= y^{(1+k)+(m+k+2)p+(m+1+2k)p^2}x^{(p-1-k)+(m-k)p+(m-4-2k)p^2}, \\
B_4^{2k} &= y^{(m+1+k)+(m+k+1)p+(2k)p^2}x^{(m-k)+(m+1-k)p+(p-4-2k)p^2}, \\
A_5^{2k} &= y^{(m+1+k)+(k)p+(m+1+2k)p^2}x^{(m-k)+(p+1-k)p+(m-4-2k)p^2}, \\
B_5^{2k} &= y^{(k)+(k)p+(2k)p^2}x^{(p-k)+(p+1-k)p+(p-4-2k)p^2}.
\end{aligned}$$

The terms B_j^{2k} cannot have terms of maximal degree. The only terms A_j^{2k} of maximal degree are the following (we indicate the corresponding coefficients):

$$\begin{aligned}
A_1^{m-4} &\to \binom{m+m/2+1}{p-m/2}\binom{m/2+2}{m/2}\binom{p-2}{1} = \frac{(v+2)(v+1)}{2}(p-2) \\
&= -(v+2)(v+1)
\end{aligned}$$

$$A_2^{m-4} \to \binom{m/2}{m/2}\binom{m+m/2+2}{p-1-m+m/2}\binom{p-3}{0} = \frac{(3v+2)(3v+1)}{2}$$
$$A_2^{m-2} \to \binom{m/2+1}{m/2+1}\binom{m+m/2+3}{p-m+m/2}\binom{p-1}{2} = \frac{(3v+3)(3v+2)}{2}$$
$$A_3^{m-4} \to \binom{m+m/2}{p-1-m+m/2}\binom{m/2}{m/2-2}\binom{p-3}{0} = \frac{v(v-1)}{2}$$
$$A_3^{m-2} \to \binom{m+m/2+1}{p-m+m/2}\binom{m/2+1}{m/2-1}\binom{p-1}{2} = \frac{v(v+1)}{2}$$
$$A_4^{m-2} \to \binom{m/2}{m/2}\binom{m+m/2+1}{p-m+m/2-2}\binom{p-2}{1} = \frac{(3v+1)(3v)}{2}(p-2) = -(3v+1)(3v)$$
$$A_5^{m-2} \to \binom{m+m/2}{p-1-m+m/2}\binom{m/2-1}{m/2-3}\binom{p-2}{1}$$
$$= \frac{(v-1)(v-2)}{2}(p-2) = -(v-1)(v-2)$$

Hence the overall coefficient (corresponding to i even) of the term of maximal degree is the following

$$\begin{aligned} c_e &= -\binom{p-6}{m-4}[-(v+2)(v+1) - 4\frac{(3v+2)(3v+1)}{2} + 6\frac{v(v-1)}{2}] \\ &- \binom{p-6}{m-2}[-4\frac{(3v+3)(3v+2)}{2} + 6\frac{(v+1)(v)}{2} + 4(3v+1)(3v) - (v-1)(v-2)] \\ &= \binom{p-6}{m-4}[16v^2+24v+6] - \binom{p-6}{m-2}[20v^2-12v-10] \\ &= \binom{p-6}{m-4} + \binom{p-6}{m-2}[v+10]. \end{aligned}$$

For $i = 2k+1$ $(0 \le k \le m-3)$ we have the following

$$A_1^{2k+1} = y^{(m+4+k)+(m+k+5)p+(3+2k)p^2}x^{(m-3-k)+(m-3-k)p+(p-7-2k)p^2},$$
$$B_1^{2k+1} = y^{(2+k)+(m+k+5)p+(m+3+2k)p^2}x^{(p-2-k)+(m-3-k)p+(m-6-2k)p^2},$$
$$A_2^{2k+1} = y^{(3+k)+(k+4)p+(3+2k)p^2}x^{(p-3-k)+(p-3-k)p+(p-7-2k)p^2},$$
$$B_2^{2k+1} = y^{(m+2+k)+(k+3)p+(m+3+2k)p^2}x^{(m-1-k)+(p-2-k)p+(m-6-2k)p^2},$$
$$A_3^{2k+1} = y^{(m+3+k)+(m+k+3)p+(2+2k)p^2}x^{(m-2-k)+(m-1-k)p+(p-6-2k)p^2},$$
$$B_3^{2k+1} = y^{(1+k)+(m+k+3)p+(m+2+2k)p^2}x^{(p-1-k)+(m-1-k)p+(m-5-2k)p^2},$$
$$A_4^{2k+1} = y^{(2+k)+(k+2)p+(2+2k)p^2}x^{(p-2-k)+(p-1-k)p+(p-6-2k)p^2},$$
$$B_4^{2k+1} = y^{(m+1+k)+(k+1)p+(m+2+2k)p^2}x^{(m-k)+(p-k)p+(m-5-2k)p^2},$$

$$A_5^{2k+1} = y^{(m+2+k)+(m+1+k)p+(1+2k)p^2} x^{(m-1-k)+(m+1-k)p+(p-5-2k)p^2},$$
$$B_5^{2k+1} = y^{(k)+(k+m+1)p+(2k+m+1)p^2} x^{(p-k)+(m+1-k)p+(m-4-2k)p^2}.$$

The terms A_j^{2k+1} cannot have terms of maximal degree. The only terms B_j^{2k+1} of maximal degree are the following (we indicate the corresponding coefficients):

$$B_1^{m-3} \to \binom{m/2}{m/2}\binom{m+m/2+3}{m+m/2+1}\binom{p-2}{1} = \frac{(3v+3)(3v+2)}{2}(p-2)$$
$$= -(3v+3)(3v+2)$$
$$B_2^{m-3} \to \binom{m+m/2}{m+m/2}\binom{m/2+1}{m/2-1}\binom{p-2}{1} = -(v+1)(v)$$
$$B_3^{m-3} \to \binom{m/2-1}{m/2-1}\binom{m+m/2+1}{m+m/2-1}\binom{p-3}{0} = \frac{(3v+1)(3v)}{2}$$
$$B_3^{m-1} \to \binom{m/2}{m/2}\binom{m+m/2+2}{m+m/2}\binom{p-1}{2} = \frac{(3v+2)(3v+1)}{2}$$
$$B_4^{m-3} \to \binom{m+m/2-1}{m+m/2-1}\binom{m/2-1}{m/2-3}\binom{p-3}{0} = \frac{(v-1)(v-2)}{2}$$
$$B_4^{m-1} \to \binom{m+m/2}{m+m/2}\binom{m/2}{m/2-2}\binom{p-1}{2} = \frac{(v)(v-1)}{2}$$
$$B_5^{m-1} \to \binom{m/2-1}{m/2-1}\binom{m+m/2}{m+m/2-2}\binom{p-2}{1} = \frac{(3v)(3v-1)}{2}(p-2) = -(3v)(3v-1)$$

Hence the overall coefficient (corresponding to i odd) of the term of maximal degree is the following

$$c_o = \binom{p-6}{m-3}[(3v+3)(3v+2) - 4(v+1)(v) - 6\frac{(3v+1)(3v)}{2} + 4\frac{(v-1)(v-2)}{2}]$$
$$+ \binom{p-6}{m-1}[-6\frac{(3v+2)(3v+1)}{2} + 4\frac{(v)(v-1)}{2} + (3v)(3v-1)]$$
$$= \binom{p-6}{m-3}[-20t^2 - 4t + 10] + \binom{p-6}{m-1}[-16v^2 - 32v - 6]$$
$$= \binom{p-6}{m-3}[v+10] + \binom{p-6}{m-1}$$

In total, our coefficient is

$$c_M = c_e + c_o = \binom{p-6}{m-4} + \binom{p-6}{m-2}[v+10] + \binom{p-6}{m-3}[v+10] + \binom{p-6}{m-1}$$
$$= 2\binom{p-6}{m-1} + 2\binom{p-6}{m-2}[v+10]$$

$$= 2\binom{p-6}{m-2}(v+\frac{37}{3}) = \frac{1}{2}\binom{p-6}{m-2}\frac{145}{3}.$$

Hence $c_M = 0$ only for $p = 5, 29$.

7.2. Exponent #2

Exponent #2 is very similar (a swapping of a_0 and a_1) to Exponent #1, and the proof works the same.

7.3. Exponent #3

For Exponent #3 we have $n = 1 + mp + (m+1)p^2$ and $t = 2 + 4p$. Note that

$$\begin{aligned} 2n &= 2 + 2mp + (2m+2)p^2 = 2 + (p-1)p + (p+1)p^2 \\ &= 3 + (p-1)p + p^2, \\ 4n &= 6 + (2p-2)p + 2p^2 \\ &= 6 + (p-2)p + 3p^2. \end{aligned}$$

With $y = (x+1)$,

$$\begin{aligned} &(y^n - x^n)^{2+4p} \\ &\quad = (y^{2n} - 2x^n y^n + x^{2n})(y^{4np} - 4x^{np}y^{3np} + 6x^{2np}y^{2np} - 4x^{3np}y^{np} + x^{4np}) \\ &\quad = y^{2n+4np} - 4x^{np}y^{2n+3np} + 6x^{2np}y^{2n+2np} - 4x^{3np}y^{2n+np} + x^{4np}y^{2n} \\ &\qquad - 2x^n y^{n+4np} + 8x^{n+np}y^{n+3np} - 12x^{n+2np}y^{n+2np} + 8x^{n+3np}y^{n+np} - 2x^{n+4np}y^n \\ &\qquad + x^{2n}y^{4np} - 4x^{2n+np}y^{3np} + 6x^{2n+2np}y^{2np} - 4x^{2n+3np}y^{np} + x^{2n+4np} \\ &\quad = y^{7+5p} - 4x^{m+1+p+mp^2}y^{m+6+3p+(m+1)p^2} + 6x^{1+3p+(p-1)p^2}y^{5+2p+p^2} \\ &\qquad - 4x^{m+3+4p+(m-1)p^2}y^{4+m+(m+2)p^2} + x^{3+6p+(p-2)p^2}y^{3+(p-1)p+p^2} \\ &\qquad - 2x^{1+mp+(m+1)p^2}y^{5+(m+6)p+(m-1)p^2} + 8x^{m+3+(m+1)p}y^{m+4+(m+4)p+(p-1)p^2} \\ &\qquad - 12x^{3+(m+3)p+mp^2}y^{3+(m+3)p+mp^2} + 8x^{m+4+(m+4)p+(p-1)p^2}y^{m+3+(m+1)p} \\ &\qquad - 2x^{5+(m+6)p+(m-1)p^2}y^{1+mp+(m+1)p^2} + x^{3+(p-1)p+p^2}y^{3+6p+(p-2)p^2} \\ &\qquad - 4x^{4+m+(m+2)p^2}y^{m+3+4p+(m-1)p^2} + 6x^{5+2p+p^2}y^{1+3p+(p-1)p^2} \\ &\qquad - 4x^{m+6+3p+(m+1)p^2}y^{m+1+p+mp^2} + x^{7+5p}. \end{aligned}$$

For $p > 7$ it is not difficult to check that the only blocks that allow a term of maximal degree are

$$8x^{m+3+(m+1)p}y^{m+4+(m+4)p+(p-1)p^2} \text{ and } 8x^{m+4+(m+4)p+(p-1)p^2}y^{m+3+(m+1)p}.$$

In this case we have

$$\begin{aligned}
&x^{m+3+(m+1)p}y^{m+4+(m+4)p+(p-1)p^2}\\
&\quad=\sum_{\alpha_0=0}^{m+4}\sum_{\alpha_1=0}^{m+4}\sum_{\alpha_2=0}^{p-1}\binom{m+4}{\alpha_0}\binom{m+4}{\alpha_1}\binom{p-1}{\alpha_2}x^{(m+3+\alpha_0)+(m+1+\alpha_1)p+\alpha_2p^2},\\
&x^{m+4+(m+4)p+(p-1)p^2}y^{m+3+(m+1)p}\\
&\quad=\sum_{\alpha_0=0}^{m+3}\sum_{\alpha_1=0}^{m+1}\binom{m+3}{\alpha_0}\binom{m+1}{\alpha_1}x^{(m+4+\alpha_0)+(m+4+\alpha_1)p+(p-1)p^2}.
\end{aligned}$$

In the first monomial we have $\alpha_0 = m-3$, $\alpha_1 = m-1$ and $\alpha_2 = p-1$. Hence we obtain

$$\binom{m+4}{m-3}\binom{m+4}{m-1}\binom{p-1}{p-1}x^{(p-1)(1+p+p^2)}.$$

In the second case we have $\alpha_0 = \alpha_1 = m-4$, hence we obtain

$$\binom{m+3}{m-4}\binom{m+1}{m-4}x^{(p-1)(1+p+p^2)}.$$

The condition $m \geq 4$ is satisfied since we are considering $p > 7$. Therefore we just need to verify that

$$\binom{m+4}{m-3}\binom{m+4}{m-1}+\binom{m+3}{m-4}\binom{m+1}{m-4}\neq 0.$$

This follows immediately upon recognising that the two terms of the sum are equal:

$$\begin{aligned}
\binom{m+4}{m-3}\binom{m+4}{m-1}&=\frac{(m+4)\cdots(m-2)}{7!}\cdot\frac{(m+4)\cdots(m)}{5!},\\
\binom{m+3}{m-4}\binom{m+1}{m-4}&=\frac{(m+3)\cdots(m-3)}{7!}\cdot\frac{(m+1)\cdots(m-3)}{5!},\\
(m+4)^2(m+3)(m+2)&=(m^2+12)^2\cdot(m^2+m+4) \bmod p,\\
(m-1)(m-2)(m-3)^2&=(m^2+m+4)\cdot(m^2+12)^2 \bmod p.
\end{aligned}$$

This eliminates this exponent.

7.4. Exponent #4

In this case $n = \frac{p-1}{2} + p + \frac{p+1}{2}p^2 = m + p + (m+1)p^2$. Set $t = (p-2) + p$. Therefore

$$\begin{aligned}(y^n - x^n)^t &= (y^n - x^n)^{p-2}(y^n - x^n)^p \\ &= \sum_{i=0}^{p-2}(-1)^{p-2-i}\binom{p-2}{i}y^{ni}x^{n(p-2-i)}(y^{np} - x^{np}) \\ &= \sum_{i=0}^{p-2}(-1)^{i+1}\binom{p-2}{i}[y^{ni+np}x^{n(p-2-i)} - y^{ni}x^{n(p-2-i)+np}] \\ &= \sum_{i=0}^{p-2}(-1)^{i+1}\binom{p-2}{i}[A_i - B_i].\end{aligned}$$

We consider whether i is even or not, and obtain

$$\begin{aligned}A_{2k} &= y^{(m+1)+(m+3k)p+(k+1)p^2}x^{(m)+(m-3-3k)p+(p-k)p^2}, \\ B_{2k} &= y^{(3k)p+(k)p^2}x^{(p-3-3k)p+(p+1-k)p^2}, \\ A_{2k+1} &= y^{(m+3k+2)p+(m+k+2)p^2}x^{(m-4-3k)p+(m-k)p^2}, \\ B_{2k+1} &= y^{(m)+(3k+1)p+(m+k+1)p^2}x^{(m+1)+(p-5-3k)p+(m+1-k)p^2},\end{aligned}$$

where in both cases $0 \le k \le m-1$. The only possible terms of maximal degree are A_{2k} for $\frac{m-2}{3} \le k \le \frac{m}{3}$ and B_{2k+1} for $\frac{p-4}{3} \le k \le \frac{p-2}{3}$ (only one integer k in both ranges). The coefficients are the following

$$\begin{aligned}c_A &= (m+1)(k+1)\binom{m+3k}{p-3} \\ c_B &= m(m+1+k)\binom{3k+1}{p-3}.\end{aligned}$$

Consider now the three possible cases: $m \bmod 3 \equiv 0, 1, 2$. The condition $m \bmod 3 \equiv 1$ is never satisfied since $m = 3j+1$ implies $p = 2m+1 = 6j+3$ so that p is not prime.

- If $m = 3j$ ($p = 6j+1$), then $\frac{m-2}{3} \le k \le \frac{m}{3}$ implies $k = j$ and $\frac{p-4}{3} \le k \le \frac{p-2}{3}$ implies $k = 2j-1$. Hence the general coefficient of maximal degree is

$$\begin{aligned}c_M = &(-1)^{2j+1}\binom{p-2}{2j}(m+1)(j+1)\binom{m+3j}{p-3} \\ &- (-1)^{2(2j-1)+1+1}\binom{p-2}{2(2j-1)+1}m(m+1+2j-1)\binom{3(2j-1)+1}{p-3}\end{aligned}$$

$$
\begin{aligned}
&= -\binom{p-2}{2j}(m+1)(j+1)\binom{p-1}{p-3} - \binom{p-2}{m+j-1}m(m+2j)\binom{p-3}{p-3}\\
&= -\binom{p-2}{2j}(m+1)(j+1) - \binom{p-2}{m+j-1}m(-j-1)\\
&= -(j+1)[\binom{p-2}{2j}(m+1) - \binom{p-2}{4j-1}m]\\
&= -(j+1)[\binom{p-2}{2j}(m+1) - \binom{p-2}{2j}m] \neq 0.
\end{aligned}
$$

- If $m = 3j+2$ ($p = 6j+5$), then $\frac{m-2}{3} \leq k \leq \frac{m}{3}$ implies $k = j$ and $\frac{p-4}{3} \leq k \leq \frac{p-2}{3}$ implies $k = 2j+1$. Hence the general coefficient of maximal degree is

$$
\begin{aligned}
c_M &= (-1)^{2j+1}\binom{p-2}{2j}(m+1)(j+1)\binom{m+3j}{p-3}\\
&\quad - (-1)^{2(2j+1)+1+1}\binom{p-2}{2(2j+1)+1}m(m+1+2j+1)\binom{3(2j+1)+1}{p-3}\\
&= -\binom{p-2}{2j}(m+1)(j+1)\binom{2m-2}{p-3} - \binom{p-2}{j+m+1}m(2m-j)\binom{2m}{p-3}\\
&= -\binom{p-2}{2j}(m+1)(j+1) - \binom{p-2}{j+m+1}m(-1-j)\\
&= -(j+1)[\binom{p-2}{2j}(m+1) - \binom{p-2}{4j+3}m]\\
&= -(j+1)[\binom{p-2}{2j}(m+1) - \binom{p-2}{2j}m] \neq 0.
\end{aligned}
$$

7.5. Exponent #5

In this case $n = \frac{p-1}{2} + \frac{p+3}{2}p^2 = m + (m+2)p^2$. Set $t = (p-6) + p + 2p^2$. Then

$$
\begin{aligned}
(y^n - x^n)^t &= (y^n - x^n)^{p-6}(y^{np} - x^{np})(y^{2np^2} - 2y^{np^2}x^{np^2} + x^{2np^2})\\
&= \sum_{i=0}^{p-6}(-1)^{p-6-i}\binom{p-6}{i}(A_1^i - 2A_2^i + A_3^i - B_1^i + 2B_2^i - B_3^i),
\end{aligned}
$$

where

$$
\begin{aligned}
A_j^i &= y^{np+n(3-j)p^2}x^{n(j-1)p^2}y^{ni}x^{n(p-6-i)}\\
B_j^i &= y^{n(3-j)p^2}x^{np+n(j-1)p^2}y^{ni}x^{n(p-6-i)}.
\end{aligned}
$$

We consider whether i is even or not. For $i = 2k$ ($0 \leq k \leq m-3$) we have the following:

$$A_1^{2k} = y^{(m+3)+(m+k+3)p+(3k)p^2} x^{(m+1)+(m-3-k)p+(p-9-3k)p^2},$$
$$B_1^{2k} = y^{(1)+(k+3)p+(3k)p^2} x^{2+(p-3-k)p+(p-9-3k)p^2},$$
$$A_2^{2k} = y^{(m+2)+(k+1)p+(m+1+3k)p^2} x^{(m+2)+(p-2-k)p+(m-9-3k)p^2},$$
$$B_2^{2k} = y^{(m+2+k)p+(m+3k)p^2} x^{3+(m-1-k)p+(m-8-3k)p^2},$$
$$A_3^{2k} = y^{(m+2)+(m+k)p+(3k)p^2} x^{(m+2)+(m-k)p+(p-9-3k)p^2},$$
$$B_3^{2k} = y^{(0)+(k)p+(3k)p^2} x^{3+(p-k)p+(p-9-3k)p^2}.$$

The terms B_j^{2k} do not have terms of maximal degree. The only terms A_j^{2k} of maximal degree are the following ones (where we also list the corresponding coefficient).

$$A_1^{2k} \text{ with } \frac{2m-7}{3} \leq k \leq \frac{2m}{3} \to \binom{m+3}{m}\binom{3k}{p-8},$$
$$A_2^{2k} \text{ with } \frac{m-8}{3} \leq k \leq \frac{m-1}{3} \to \binom{m+2}{m-1}\binom{3k+1+m}{p-8},$$
$$A_3^{2k} \text{ with } \frac{2m-7}{3} \leq k \leq \frac{2m}{3} \to \binom{m+2}{m-1}\binom{3k}{p-8}.$$

For $i = 2k+1$ $(0 \leq k \leq m-3)$ we have the following

$$A_1^{2k+1} = y^{2+(m+k+4)p+(m+2+3k)p^2} x^{(1)+(m-3-k)p+(m-10-3k)p^2},$$
$$B_1^{2k+1} = y^{(m+1)+(k+3)p+(3k+m+2)p^2} x^{(m+3)+(p-4-k)p+(m-10-3k)p^2},$$
$$A_2^{2k+1} = y^{2+(k+2)p+(2+3k)p^2} x^{(1)+(p-2-k)p+(p-11-3k)p^2},$$
$$B_2^{2k+1} = y^{(m+1)+(m+2+k)p+(1+3k)p^2} x^{(m+3)+(m-2-k)p+(p-10-3k)p^2},$$
$$A_3^{2k+1} = y^{(1)+(m+k+1)p+(m+2+3k)p^2} x^{2+(m-k)p+(m-10-3k)p^2},$$
$$B_3^{2k+1} = y^{(m)+(k)p+(3k+m+2)p^2} x^{(m+4)+(p-1-k)p+(m-10-3k)p^2}.$$

The terms A_j^{2k+1} do not have terms of maximal degree. The only terms B_j^{2k+1} of maximal degree are the following ones (where we also list the corresponding coefficient).

$$B_1^{2k} \text{ with } \frac{m-9}{3} \leq k \leq \frac{m-2}{3} \to \binom{m+1}{m-2}\binom{3k+m+2}{p-8},$$
$$B_2^{2k} \text{ with } \frac{2m-8}{3} \leq k \leq \frac{2m-1}{3} \to \binom{m+1}{m-2}\binom{3k+1}{p-8},$$
$$B_3^{2k} \text{ with } \frac{m-9}{3} \leq k \leq \frac{m-2}{3} \to \binom{m}{m-3}\binom{3k+m+2}{p-8}.$$

We consider in the following the case $m \equiv 0 \bmod 3$ and $m \equiv 2 \bmod 3$ (as already noted if $m \equiv 1 \bmod 3$, then $3 \mid p$). The overall coefficient for the term of maximal degree is the following:

$$\begin{aligned}
c_M = &- \sum_{k=\frac{2m-7}{3}}^{\frac{2m}{3}} \binom{p-6}{2k}\binom{3k}{p-8}[\binom{m+3}{m}+\binom{m+2}{m-1}] \\
&+ 2\sum_{k=\frac{m-8}{3}}^{\frac{m-1}{3}} \binom{p-6}{2k}\binom{m+2}{m-1}\binom{3k+m+1}{p-8} \\
&- \sum_{k=\frac{m-9}{3}}^{\frac{m-2}{3}} \binom{p-6}{2k+1}\binom{3k+m+2}{p-8}[\binom{m+1}{m-2}+\binom{m}{m-3}] \\
&+ 2\sum_{k=\frac{2m-8}{3}}^{\frac{2m-1}{3}} \binom{p-6}{2k+1}\binom{m+1}{m-2}\binom{3k+1}{p-8} \\
= &- \sum_{k=\frac{2m-7}{3}}^{\frac{2m}{3}} \binom{p-6}{2k}\binom{3k}{p-8}\frac{(m+2)(m+1)}{3} \\
&+ 2\sum_{k=\frac{m-8}{3}}^{\frac{m-1}{3}} \binom{p-6}{2k}\binom{m+2}{m-1}\binom{3k+m+1}{p-8} \\
&+ \sum_{k=\frac{m-9}{3}}^{\frac{m-2}{3}} \binom{p-6}{2k+1}\binom{3k+m+2}{p-8}\frac{m(m-1)}{3} \\
&+ 2\sum_{k=\frac{2m-8}{3}}^{\frac{2m-1}{3}} \binom{p-6}{2k+1}\binom{m+1}{m-2}\binom{3k+1}{p-8}.
\end{aligned}$$

7.5.1. $m = 3t$

In this case $p = 6t+1$.

$$\begin{aligned}
c_M = &- \sum_{k=2t-2}^{2t} \binom{p-6}{2k}\binom{3k}{p-8}\frac{(m+2)(m+1)}{3} \\
&+2\sum_{k=t-2}^{t-1} \binom{p-6}{2k}\binom{m+2}{m-1}\binom{3k+m+1}{p-8} \\
&+ \sum_{k=t-3}^{t-1} \binom{p-6}{2k+1}\binom{3k+m+2}{p-8}\frac{m(m-1)}{3} + 2\sum_{k=2t-2}^{2t-1} \binom{p-6}{2k+1}\binom{m+1}{m-2}\binom{3k+1}{p-8}
\end{aligned}$$

$$= \frac{1}{2}[7\binom{p-6}{2t-1} - 35\binom{p-6}{2t-3} + \binom{p-6}{2t-5}] - \frac{21}{4}[\binom{p-6}{2t-4} - \binom{p-6}{2t-2}]$$
$$= -\frac{21}{4}\binom{p-6}{2t-4}2\frac{t+1}{(t-1)(2t-3)} \neq 0.$$

7.5.2. $m = 3t+2$

In this case $p = 6t+5$.

$$\begin{aligned} c_M = &- \sum_{k=2t-1}^{2t+1} \binom{p-6}{2k}\binom{3k}{p-8}\frac{(m+2)(m+1)}{3} \\ &+ 2\sum_{k=t-2}^{t} \binom{p-6}{2k}\binom{m+2}{m-1}\binom{3k+m+1}{p-8} \\ &+ \sum_{k=t-2}^{t} \binom{p-6}{2k+1}\binom{3k+m+2}{p-8}\frac{m(m-1)}{3} + 2\sum_{k=2t-1}^{2t+1} \binom{p-6}{2k+1}\binom{m+1}{m-2}\binom{3k+1}{p-8} \\ = &-\frac{1}{3}(m-1)[\binom{p-6}{2t+1} - 35\binom{p-6}{2t-1} + 7\binom{p-6}{2t-3}] \\ &- \frac{1}{2}(m+1)[\binom{p-6}{2t-4} - 35\binom{p-6}{2t-2} + 7\binom{p-6}{2t}] \\ = &-\frac{1}{6}(m+1)\binom{p-6}{2t-2}\frac{2t+25}{(t+1)(2t+3)t(2t-1)} \neq 0. \end{aligned}$$

In either scenario, Exponent #5 is eliminated.

7.6. Exponent #6

Let $n = 1+3p+(p-3)p^2$ and $t = 2+4p+4p^2$. The cases with $p \leq 17$ can be checked computationally, and we assume $p \geq 19$ for this case. A similar approach to that used for Exponent #3 can be performed here. Note

$$\begin{aligned} n &= 1+3p+(p-3)p^2, \\ 2n &= 3+6p+(p-6)p^2, \\ 3n &= 5+9p+(p-9)p^2, \\ 4n &= 7+12p+(p-12)p^2. \end{aligned}$$

We have a more complicated expression to consider:

$$\begin{aligned} &(y^n - x^n)^{2+4p+4p^2} \\ &\quad = (y^{2n} - 2x^n y^n + x^{2n})(y^{4np} - 4x^{np}y^{3np} + 6x^{2np}y^{2np} - 4x^{3np}y^{np} + x^{4np}) \end{aligned}$$

$$
\begin{aligned}
&\cdot (y^{4np^2} - 4x^{np^2}y^{3np^2} + 6x^{2np^2}y^{2np^2} - 4x^{3np^2}y^{np^2} + x^{4np^2}) \\
&= (y^{3+6p+(p-6)p^2} - 2x^{1+3p+(p-3)p^2}y^{1+3p+(p-3)p^2} + x^{3+6p+(p-6)p^2}) \\
&\cdot (y^{(p-12)+7p+12p^2} - 4x^{(p-3)+p+3p^2}y^{(p-9)+5p+9p^2} + 6x^{(p-6)+3p+6p^2}y^{(p-6)+3p+6p^2} \\
&- 4x^{(p-9)+5p+9p^2}y^{(p-3)+p+3p^2} + x^{(p-12)+7p+12p^2}) \\
&\cdot (y^{12+(p-12)p+7p^2} - 4x^{3+(p-3)p+p^2}y^{9+(p-9)p+5p^2} + 6x^{6+(p-6)p+3p^2}y^{6+(p-6)p+3p^2} \\
&- 4x^{9+(p-9)p+5p^2}y^{3+(p-3)p+p^2} + x^{12+(p-12)p+7p^2})
\end{aligned}
$$

A careful analysis of all the blocks x^iy^j obtained and the relative exponents, it is clear that the only blocks that contain a monomial of maximal degree are the following ones:

$$
\begin{aligned}
A_1 &= -4x^{np^2+2n}y^{4np+3np^2} \\
&= -4x^{6+3p+(p-4)p^2}y^{(p-3)+(p-2)p+17p^2}, \\
A_2 &= -4x^{3np^2+2n}y^{4np+np^2} \\
&= -4x^{12+(p-3)p+(p-1)p^2}y^{(p-9)+4p+14p^2} \\
A_3 &= -4x^{4np+3np^2}y^{np^2+2n} \\
&= -4x^{(p-3)+(p-2)p+17p^2}y^{6+3p+(p-4)p^2}, \\
A_4 &= -4x^{4np+np^2}y^{3np^2+2n} \\
&= -4x^{(p-9)+4p+14p^2}y^{12+(p-3)p+(p-1)p^2}.
\end{aligned}
$$

If we set c_i to be the coefficient of the monomial of maximal degree, we obtain

$$
\begin{aligned}
c_1 &= -4\binom{p-3}{p-7}\binom{p-2}{p-4}\binom{17}{3}, \\
c_2 &= -4\binom{p-9}{p-13}\binom{4}{2}\binom{14}{0}, \\
c_3 &= -4\binom{6}{2}\binom{3}{1}\binom{p-4}{p-18}, \\
c_4 &= -4\binom{12}{8}\binom{p-3}{p-5}\binom{p-1}{p-15}.
\end{aligned}
$$

Therefore we need to prove that $c_1 + c_2 + c_3 + c_4 \neq 0$. We first do some simplifications. Working modulo p we have

$$
c_1 = -4\binom{p-3}{p-7}\binom{p-2}{p-4}\binom{17}{3}
$$

$$\begin{aligned}
&= -4\binom{p-3}{4}\binom{p-2}{2}\binom{17}{3} \\
&= -4\frac{3\times 4\times 5\times 6}{4!}\frac{2\times 3}{2}\frac{17\times 16\times 15}{3!} \\
&= -2^5 3^2 5^2 17.
\end{aligned}$$

Next,

$$\begin{aligned}
c_2 &= -4\binom{p-9}{p-13}\binom{4}{2}\binom{14}{0} \\
&= -4\binom{p-9}{4}\frac{4\times 3}{2} \\
&= -4\frac{9\times 10\times 11\times 12}{4!}\times 2\times 3 \\
&= -2^3 3^3 5\times 11.
\end{aligned}$$

For c_3, we find

$$\begin{aligned}
c_3 &= -4\binom{6}{2}\binom{3}{1}\binom{p-4}{p-18} \\
&= -4\frac{6\times 5}{2}\times 3\times \frac{4\times 5\times\cdots\times 17}{14!} \\
&= -2^5 3^2 5^2 17 = c_1.
\end{aligned}$$

On a similar note, we find

$$\begin{aligned}
c_4 &= -4\binom{12}{8}\binom{p-3}{p-5}\binom{p-1}{p-15} \\
&= -4\frac{12\times 11\times 10\times 9}{4!}\frac{3\times 4}{2}\times(-1)^{p-15} \\
&= -2^3 3^3 5\times 11 = c_2.
\end{aligned}$$

Thus, we find

$$\begin{aligned}
c_1 + c_2 + c_3 + c_4 &= -2^6 3^2 5^2 17 + -2^4 3^3 5\times 11 \\
&= -2^4 3^2 5(340+33) \\
&= -2^4\times 3^2\times 5\times 373.
\end{aligned}$$

Thus, for $p \neq 373$, we have a non-zero coefficient for the maximal degree term. For $p = 373$, we test directly using the Magma Algebra package [1]. Using Magma's standard construction of $\mathbb{F}_q$, with $q = 373^3$, and the planar equivalent exponent $n' = p^2 n \bmod (q-1)$, we find $(g^i+1)^{n'} - g^{in'} = (g^j+1)^{n'} - g^{jn'}$ with $i = 92$, $j = 5737$ where g is a primitive

element of $\mathbb{F}_q$. This eliminates the final possible prime for which Exponent #6 could be planar, and so it is never planar.

7.7. Exponent #7

Set $n = 1 + 2p + (p-2)p^2$. and $t = (p-1)(p+1)$. This case turns out to be the most involved of all of our explicit exponents. Firstly, with $y = x + 1$, we have

$$\begin{aligned}(y^n - x^n)^t &= \sum_{k=0}^{t} \binom{t}{k} y^{nk}(-1)^k x^{nt-nk} \\ &= \sum_{i,j=0}^{p-1} (-1)^{i+j} y^{ni+njp}(-1)^{i+j} x^{4p^2-4p-ni-njp} \\ &= \sum_{i,j=0}^{p-1} y^{ni+njp} x^{4p^2-4p-ni-njp}.\end{aligned}$$

Set $i + j = w$. Then it can be shown that, with $x^{4p^2-4p-ni-njp} = x^\alpha$ and $y^{ni+njp} = y^\beta$, we have

$$\begin{aligned}\alpha &= (4j - 2w) + p(p - (2w + 4)) + p^2(2w + 3 - 4j) \\ \beta &= (2w - 4j) + 2pw + p^2(4j - 2w).\end{aligned}$$

It is immediate that we can never have an x^{q-1} term when $i = j$, that is when $2j = w$. As shall be shown, we obtain non-zero coefficients for the x^{q-1} term only when $w \in \{(p-3)/2, (p-1)/2, p-2, p-1, p, p+(p-3)/2, p+(p-1)/2\}$. For ease of notation, we define four binomial sums. Specifically, we set s_i, with $0 \le i \le 3$, to be

$$s_i = \sum_{j=0}^{k} \binom{4j+i}{3},$$

where k is the largest integer satisfying $4k + i < p$.

7.7.1. When $w < (p-3)/2$

Since $w < (p-3)/2$, we see that $2w + 4 < p$. We concentrate on the p term of α and β. Now $p - 1 - (p - (2w + 4)) = 2w + 3$, and the most carries we can see occur for the p terms of α and of β is a shift of 1 in either direction, with one going up while the other goes down, so that (with $\epsilon = \pm 1$)

$$\binom{2w+\epsilon}{2w+3+\epsilon}$$

is clearly always 0 and we can never obtain a x^{q-1} term from this case.

7.7.2. When $w = (p-3)/2$

We now have

$$\alpha = (4j+3) + p(p-2) + p^2(p-(4j+1))$$
$$\beta = (p-(4j+3)) + p(p-3) + p^2((4j+3)-p).$$

Keeping in mind that $2j \neq w$, we have the following cases to deal with: $4j+3 < p$, $4j+1 = p$, and $p+2 < 4j+3 \leq 2p-3$. It is immediate from consideration of the p^2 terms of α and β that there is no x^{q-1} term when $4j+1 = p$.

For $4j+3 < p$, only β has a carry, becoming

$$\beta = (p-(4j+4)) + p(p-3) + p^2(4j+3).$$

We now obtain an x^{q-1} term with coefficient

$$\binom{p-(4j+4)}{p-1-(4j+3)}\binom{p-3}{1}\binom{4j+3}{p-1-(p-(4j+1))} = (p-3)\binom{4j+3}{3}.$$

Consequently, it can be seen that we obtain an overall coefficient of

$$d_1 = -3s_3.$$

For $p+2 < 4j+3 \leq 2p-3$, after dealing with carries we have

$$\alpha = (4j+2-p) + p(p-1) + p^2(2p-(4j+1))$$
$$\beta = (2p-(4j+3)) + p(p-4) + p^2((4j+3)-p).$$

This yields an x^{q-1} term with coefficient

$$\binom{2p-(4j+3)}{p-1-(4j+2-p)}\binom{p-4}{0}\binom{4j+3-p}{p-1-(2p-(4j+1))} = \binom{4j+3-p}{3}.$$

Summing over all cases, we obtain an overall coefficient of

$$d_2 = \begin{cases} s_2 & \text{if } p \equiv 1 \bmod 4, \\ s_0 & \text{if } p \equiv 3 \bmod 4. \end{cases}$$

7.7.3. When $w = (p-1)/2$

In this case our exponents simplify to

$$\alpha = (4j+1) + p(p-4) + p^2(p-(4j-1))$$
$$\beta = (p-(4j+1)) + p(p-1) + p^2((4j+1)-p).$$

As $2j \neq w$, we are left with three situations: $4j+1 < p$, $4j-1 = p$, and $p+2 < 4j+1 \leq 2p-1$. When $4j-1 = p$, it is clear from inspecting the p^2 terms of α and β that there is no x^{q-1} term.

For $4j+1 < p$, only β has a carry, becoming

$$\beta = (p-(4j+2)) + p(p-1) + p^2(4j+1).$$

The coefficient of the x^{q-1} term so generated is

$$\binom{p-(4j+2)}{p-1-(4j+1)}\binom{p-1}{3}\binom{4j+1}{p-1-(p-(4j-1))} = (-1)\binom{4j+1}{3}.$$

Summing, we obtain the coefficient

$$d_3 = -s_1.$$

For $p+2 < 4j+1 \leq 2p-1$, we find

$$\begin{aligned}\alpha &= (4j-p) + p(p-3) + p^2(2p-(4j-1))\\ \beta &= (2p-(4j+1)) + p(p-2) + p^2((4j+1)-p).\end{aligned}$$

This generates an x^{q-1} term with coefficient

$$\binom{2p-(4j+1)}{p-1-(4j-p)}\binom{p-2}{2}\binom{4j+1-p}{p-1-(2p-(4j-1))} = 3\binom{4j+1-p}{3}.$$

Proceeding to sum over all cases yields the coefficient

$$d_4 = \begin{cases} 3s_0 & \text{if } p \equiv 1 \bmod 4,\\ 3s_2 & \text{if } p \equiv 3 \bmod 4.\end{cases}$$

7.7.4. When $(p-1)/2 < w < p-2$

With w in this range, we first deal with some carries for α and β, obtaining

$$\begin{aligned}\alpha &= (4j-2w) + p(2p-(2w+4)) + p^2(2w+2-4j)\\ \beta &= (2w-4j) + p(2w-p) + p^2(4j+1-2w).\end{aligned}$$

We concentrate on the p terms of α and β. As $-2p < 2w-4j < 2p$, the p terms can only ever receive a carry of 1 in either direction, with one going up while the other goes down. Thus to construct an x^{q-1} term, the binomial generated by the p term would be

$$\binom{2w-p+\epsilon}{p-1-(2p-(2w+4)-\epsilon)} = \binom{2w-p+\epsilon}{2w-p+3+\epsilon} = 0.$$

Hence there is no x^{q-1} term generated in this case.

7.7.5. When $w = p - 2$

For $w = p - 2$, we have

$$\alpha = (4j + 5) + p(p - 2) + p^2(p - (4j + 3))$$
$$\beta = p - (4j + 6) + p(p - 3) + p^2(4j + 5).$$

For this case, we split the situation into multiple subcases: $4j + 5 < p$, $4j + 5 = p$, $4j + 3 = p$, $p + 3 < 4j + 6 < 2p$, $4j + 6 = 2p$, $2p + 1 < 4j + 5 < 3p$, $4j + 5 = 3p$, $4j + 3 = 3p$, $3p + 2 < 4j + 5$.

It is very quickly checked that we get no x^{q-1} term from the cases where $4j + 5 = p$, $4j + 3 = p$, $4j + 5 = 3p$ and $4j + 3 = 3p$.

For $4j + 5 < p$, the coefficient is

$$\binom{p - 4j - 6}{p - 1 - 4j - 5}\binom{p - 3}{1}\binom{4j + 5}{p - 1 - p + 4j + 3} = (p - 3)\binom{4j + 5}{4j + 2} = (p - 3)\binom{4j + 5}{3}.$$

This situation thus yields the overall coefficient of

$$d_5 = -3s_1.$$

For $p + 3 < 4j + 6 < 2p$, after dealing with carries we find

$$\alpha = (4j + 4 - p) + p(p - 1) + p^2(2p - (4j + 3))$$
$$\beta = 2p - (4j + 5) + p(p - 4) + p^2(4j + 5 - p).$$

Thus the coefficient of x^{q-1} when $p + 3 < 4j + 6 < 2p$ is

$$\binom{2p - (4j + 5)}{p - 1 - (4j + 4 - p)}\binom{p - 4}{0}\binom{4j + 5 - p}{p - 1 - (2p - (4j + 3))} = \binom{4j + 5 - p}{3}.$$

If we sum, we find that since $4j + 5 < 2p - 1$, we're missing the very last term in either s_0 or s_2, depending on $p \bmod 4$. In either case this would be $\binom{p-1}{3} = -1^3 = -1$. Thus we obtain the overall coefficient of

$$d_6 = 1 + \begin{cases} s_0 & \text{if } p \equiv 1 \bmod 4, \\ s_2 & \text{if } p \equiv 3 \bmod 4. \end{cases}$$

For $4j + 6 = 2p$, we have

$$\alpha = (p - 2) + p(p - 1) + 3p^2$$
$$\beta = 1 + p(p - 4) + p^2(p - 1).$$

The coefficient of x^{q-1} generated from $y^\beta x^\alpha$ is

$$\binom{1}{1}\binom{p-4}{0}\binom{p-1}{p-1-3} = (-1)^3 = -1.$$

This singleton case thus produces the coefficient $d_7 = -1$.

For $2p+1 < 4j+5 < 3p$, we after carries we find

$$\alpha = (4j+3-2p) + 0 \times p + p^2(3p-(4j+2))$$
$$\beta = 3p-(4j+4) + p(p-5) + p^2(4j+5-2p),$$

from which it is clear we get no x^{q-1} term.

Finally, for $3p+2 < 4j+5$, after carries we have

$$\alpha = (4j+2-3p) + p + p^2(4p-(4j+2))$$
$$\beta = 4p-(4j+3) + p(p-6) + p^2(4j+5-3p),$$

from which it is again clear we have no x^{q-1} term.

7.7.6. When $w = p-1$

A first simplification of our exponents produces

$$\alpha = (4j+2) + p(p-4) + p^2(2p-(4j+1))$$
$$\beta = (2p-(4j+2)) + p(p-2) + p^2(4j+3-2p).$$

We have the following eight cases to consider: $4j+3 < p$, $4j+3 = p$, $4j+1 = p$, $p+2 < 4j+3 < 2p$, $2p < 4j+3 < 3p$, $4j+3 = 3p$, $4j+1 = 3p$, $3p < 4j+1 \leq 4p-3$. The four cases involving equalities are easily eliminated by considering either of the p^0 or p^2 terms of α and β. This leaves us just the four cases $4j+3 < p$, $p+2 < 4j+3 < 2p$, $2p < 4j+3 < 3p$, and $3p < 4j+1 \leq 4p-3$.

When $4j+3 < p$, dealing with our carries produces

$$\alpha = (4j+3) + p(p-4) + p^2(p-(4j+1))$$
$$\beta = (p-(4j+4)) + p(p-1) + p^2(4j+3).$$

We obtain an x^{q-1} term with coefficient

$$\binom{p-(4j+4)}{p-1-(4j+3)}\binom{p-1}{3}\binom{4j+3}{p-1-(p-(4j+1))} = (-1)\binom{4j+3}{3}.$$

We sum and obtain the overall coefficient of

$$d_8 = -s_3.$$

When $p+2 < 4j+3 < 2p$, after considering carries, we have

$$\alpha = (4j+2-p) + p(p-3) + p^2(2p-(4j+1))$$
$$\beta = (2p-(4j+3)) + p(p-2) + p^2(4j+3-p).$$

Here we obtain an x^{q-1} term with coefficient

$$\binom{2p-(4j+3)}{p-1-(4j+2-p)}\binom{p-2}{2}\binom{4j+3-p}{p-1-(2p-(4j+1))} = 3\binom{4j+3-p}{3}.$$

Overall, this produces the coefficient

$$d_9 = \begin{cases} 3s_2 & \text{if } p \equiv 1 \bmod 4, \\ 3s_0 & \text{if } p \equiv 3 \bmod 4. \end{cases}$$

When $2p < 4j+3 < 3p$, we must have also have $4j+1 > 2p$ as otherwise $w = 2j$. Dealing with carries, our exponents are

$$\alpha = (4j+1-2p) + p(p-2) + p^2(3p-(4j+1))$$
$$\beta = (3p-(4j+2)) + p(p-3) + p^2(4j+3-2p).$$

The coefficient for the x^{q-1} term is

$$\binom{3p-(4j+2)}{p-1-(4j+1-2p)}\binom{p-3}{1}\binom{4j+3-2p}{p-1-(3p-(4j+1))} = -3\binom{4j+3-2p}{3}.$$

Now we get the coefficient

$$d_{10} = -3s_1.$$

Finally, when $3p < 4j+1 \leq 4p-3$, we simplify our exponents to find

$$\alpha = (4j-3p) + p(p-1) + p^2(4p-(4j+1))$$
$$\beta = (4p-(4j+1)) + p(p-4) + p^2(4j+3-3p).$$

The coefficient for the x^{q-1} term is

$$\binom{4p-(4j+1)}{p-1-(4j-3p)}\binom{p-4}{0}\binom{4j+3-3p}{p-1-(4p-(4j+1))} = \binom{4j+3-3p}{3},$$

and summing we get the overall coefficient

$$d_{11} = \begin{cases} s_0 & \text{if } p \equiv 1 \bmod 4, \\ s_2 & \text{if } p \equiv 3 \bmod 4. \end{cases}$$

7.7.7. When $w = p$

A first simplification of our exponents produces

$$\alpha = (4j+1) + p(p-6) + p^2(p-(4j-1))$$
$$\beta = (p-(4j+2)) + p + p^2(4j+2).$$

An immediate observation from looking at the coefficient of the p terms is that we cannot possibly obtain an x^{q-1} term with $4j+2 \leq 2p$. We therefore have just the following three cases: $2p < 4j-1 < 3p-2$, $4j+1 = 3p$, $4j+1 > 3p$. The case where $4j+1 = 3p$ is also quickly eliminated.

When $2p < 4j-1 < 3p-2$, we find α and β become

$$\alpha = (4j-1-2p) + p(p-4) + p^2(3p-(4j-1))$$
$$\beta = (3p-4j) + p(p-1) + p^2(4j+1-2p).$$

The coefficient for the x^{q-1} term is

$$\binom{3p-4j}{p-1-(4j-1-2p)}\binom{p-1}{3}\binom{4j+1-2p}{p-1-(3p-(4j-1))} = -\binom{4j+1-2p}{3}.$$

Taking the sum of these coefficients produces the overall coefficient

$$d_{12} = -s_3.$$

When $4j+1 > 3p$, we find

$$\alpha = (4j-2-3p) + p(p-3) + p^2(4p-(4j-1))$$
$$\beta = (4p-(4j-1)) + p(p-2) + p^2(4j+1-3p).$$

This produces an x^{q-1} term with coefficient

$$\binom{4p-4j+1}{p-1-(4j-2-3p)}\binom{p-2}{2}\binom{4j+1-3p}{p-1-(4p-(4j-1))} = 3\binom{4j+1-3p}{3}.$$

We sum to obtain

$$d_{13} = \begin{cases} 3s_2 & \text{if } p \equiv 1 \bmod 4, \\ 3s_0 & \text{if } p \equiv 3 \bmod 4. \end{cases}$$

7.7.8. When $p < w < p + (p-3)/2$

For this situation, let us rewrite w as $w = p + w'$ with $0 < w' < (p-3)/2$. A first simplification of α and β yields

$$\alpha = (4j + 2 - 2w') + p(p - (2w' + 6)) + p^2(2w' + 1 - 4j)$$
$$\beta = (2w' - 2 - 4j) + p(2w' + 2) + p^2(4j + 2 - 2w').$$

Concentrating on the p terms of both α and β one sees that then it is impossible to construct a $p-1$ multiple of p, as the carries will only ever make a difference of at most 2 when we need a minimum of 3 carries in total. Hence, we never get an x^{q-1} term in this case.

7.7.9. When $w = p + (p-3)/2$

In this case, we note that $j \geq (p-1)/2$, so that $4j + 3 > 2p$ always. With this in mind, our first simplification of our exponents leads us to

$$\alpha = (4j + 3 - 2p) + p(p - 2) + p^2(3p - (4j + 3))$$
$$\beta = (3p - (4j + 4)) + p(p - 3) + p^2(4j + 5 - 2p).$$

There are 4 cases to deal with: $2p < 4j + 3 < 3p - 2$, $4j + 5 = 3p$, $4j + 3 = 3p$, $3p < 4j + 3 \leq 4p - 2$, and $j = p - 1$ ($4j + 5 = 4p + 1$). By inspection it is immediate that when $4j + 5 = 3p$, $4j + 3 = 3p$ or $j = p - 1$, we cannot possibly generate an x^{q-1} term.

When $2p < 4j + 3 < 3p - 2$, we can immediately read off the coefficient of x^{q-1}, finding

$$\binom{3p - 4j - 4}{p - 1 - 4j - 3 + 2p}\binom{p-3}{1}\binom{4j + 5 - 2p}{p - 1 - (3p - (4j + 3))} = -3\binom{4j + 5 - 2p}{3}.$$

Summing over them all produces the overall coefficient

$$d_{14} = -3s_3.$$

When $4j + 3 > 3p$, after dealing with carries we obtain

$$\alpha = (4j + 2 - 3p) + p(p - 1) + p^2(4p - (4j + 3))$$
$$\beta = (4p - (4j + 3)) + p(p - 4) + p^2(4j + 5 - 3p).$$

When generating an x^{q-1} term we now get the coefficient

$$\binom{4p - 4j - 3}{p - 1 - 4j - 2 + 3p}\binom{p-4}{0}\binom{4j + 5 - 3p}{p - 1 - (4p - (4j + 3))} = \binom{4j + 5 - 3p}{3},$$

and summing now produces the overall coefficient of

$$d_{15} = \begin{cases} s_2 & \text{if } p \equiv 1 \bmod 4, \\ s_0 & \text{if } p \equiv 3 \bmod 4. \end{cases}$$

7.7.10. When $w = p + (p-1)/2$

Now we have $j \geq (p+1)/2$, so that $4j > 2p+1$ always holds. With this in mind, our first simplification of our exponents leads us to

$$\alpha = (4j + 1 - 2p) + p(p-4) + p^2(3p - (4j+1))$$
$$\beta = (3p - (4j+2)) + p(p-1) + p^2(4j + 3 - 2p).$$

There are 4 cases: $2p < 4j+1 < 3p-2$, $4j+3 = 3p$, $4j+1 = 3p$, and $4j+1 > 3p$. It is again easily seen that the $4j+3 = 3p$ and $4j+1 = 3p$ cases cannot possibly generate an x^{q-1} term.

When $2p < 4j+1 < 3p-2$, we read off the coefficient of x^{q-1}, finding

$$\binom{3p-4j-2}{p-1-4j-1+2p}\binom{p-1}{3}\binom{4j+3-2p}{p-1-(3p-(4j+1))} = -\binom{4j+3-2p}{3}.$$

This produces the overall coefficient

$$d_{16} = -s_1.$$

When $4j+1 > 3p$, we get

$$\alpha = (4j - 3p) + p(p-3) + p^2(4p - (4j+1))$$
$$\beta = (4p - (4j+1)) + p(p-2) + p^2(4j + 3 - 3p).$$

When generating an x^{q-1} term we now get the coefficient

$$\binom{4p-4j-1}{p-1-4j+3p}\binom{p-2}{2}\binom{4j+3-3p}{p-1-(4p-(4j+1))} = 3\binom{4j+3-3p}{3}.$$

This gives an the overall coefficient of

$$d_{17} = \begin{cases} 3s_0 & \text{if } p \equiv 1 \bmod 4, \\ 3s_2 & \text{if } p \equiv 3 \bmod 4. \end{cases}$$

7.7.11. When $w > p + (p-1)/2$

Again we rewrite w as $w = p + w'$ with $(p-1)/2 < w' < p-2$. Simplifying our exponents, while utilising the fact $p < 4j - 2w' < 3p$, we obtain

$$\alpha = (4j - 2w' - p) + p(2p - 2w' - 5) + p^2(2p - (4j - 2w'))$$
$$\beta = (2p - (4j + 1 - 2w')) + p(2w' - p) + p^2(4j + 3 - 2w' - p).$$

Examination of the p terms of α and β in two separate cases, namely $p < 4j - 2w' < 2p$ and $2p < 4j - 2w' < 3p$, shows that it is again impossible to construct a $p-1$ multiple of p. We therefore cannot obtain an x^{q-1} term here.

7.7.12. Final determination of the coefficient

We are now in a position to finally determine the coefficient of the maximal degree term. Denote this coefficient by D. We have $D = d_1 + d_2 + \cdots + d_{17}$, all of which are some multiple of s_i, apart from d_6 and d_7, which together sum to an s_i. We can split the situation into two components C and C_p, with C independent of p, while C_p appears to depend on $p \bmod 4$ (though in the end it doesn't).

Thus, $D = C + C_p$ where

$$C = -8(s_1 + s_3)$$

and

$$C_p = 8(s_0 + s_2).$$

Thus our coefficient is

$$D = 8\sum_{k=3}^{p-1}(-1)^k\binom{k}{3}.$$

It remains to determine this sum. For any natural number n we define $W(n)$ to be

$$W(n) = \sum_{k=1}^{n}(-1)^k k(k+1)(k+2),$$

so that

$$\sum_{k=3}^{p-1}(-1)^k\binom{k}{3} = \frac{1}{6}W(p-3).$$

We now determine a closed formula for $W(n)$. We restrict ourselves to n even for simplicity. Induction easily proves

$$S(n) = \sum_{k=1}^{n}(-1)^k k = \frac{n}{2}$$

$$T(n) = \sum_{k=0}^{n}(-1)^k k^2 = \frac{n(n+1)}{2}$$

$$U(n) = \sum_{k=0}^{n} k^3 = \frac{n^2(n+1)^2}{4}.$$

We need to determine

$$V(n) = \sum_{k=0}^{n}(-1)^k k^3.$$

For n even we have

$$\begin{aligned} V(n) &= \sum_{k=0}^{n} (-1)^k k^3 \\ &= 2\sum_{k=0}^{n/2} (2k)^3 - n^3 - \sum_{k=0}^{n-1} k^3 \\ &= 16U(n/2) - n^3 - U(n-1) \\ &= \frac{n^2(2n+3)}{4}. \end{aligned}$$

Combining these we find

$$\begin{aligned} W(n) &= \sum_{k=1}^{n} (-1)^k k(k+1)(k+2) \\ &= \sum_{k=1}^{n} (-1)^k (k^3 + 3k^2 + 2k) \\ &= V(n) + 3T(n) + 2S(n) \\ &= \frac{n(n+2)(2n+5)}{4}. \end{aligned}$$

Working in $\mathbb{F}_q$, we now find

$$\begin{aligned} D &= 8\sum_{k=3}^{p-1} (-1)^k \binom{k}{3} \\ &= \frac{8}{6} W(p-3) \\ &= \frac{8}{6} \frac{(p-3)(p-1)(2p-1)}{4} \\ &= \frac{8}{6} \frac{(-3)(-1)(-1)}{4} \\ &= -1. \end{aligned}$$

Thus we have a non-zero coefficient for the x^{q-1} term, and Exponent #7 is never planar over $\mathbb{F}_{p^3}$. We conclude the consideration of this case by noting that for all the effort needed to deal with this exponent, the whole case is remarkably well behaved.

7.8. Exponent #8

We set $n = 2 + p + (p-2)p^2$ and $t = 1 + 2p + 3p^2$. Then we have

$$\begin{aligned}(y^n - x^n)^t = {} & y^{2+p+9p^2} - 3y^{1+3p+6p^2}x^{1+(p-2)p+2p^2} + 3y^{5p+3p^2}x^{2+(p-4)p+5p^2} \\ & - y^{(p-1)+6p}x^{3+(p-6)p+8p^2} - 2y^{4+(p-2)p+7p^2}x^{(p-2)+2p+p^2} \\ & + 6y^{3+5p^2}x^{(p-1)+4p^2} - 6y^{2+2p+2p^2}x^{(p-1)p+6p^2} + 2y^{4p+(p-1)p^2}x^{1+(p-3)p+9p^2} \\ & + y^{6+(p-5)p+6p^2}x^{(p-4)+5p+2p^2} - 3y^{5+(p-3)p+3p^2}x^{(p-3)+3p+5p^2} \\ & + 3y^{4+(p-1)p}x^{(p-2)+p+8p^2} - y^{2+p+(p-2)p^2}x^{(p-1)+(p-1)p+10p^2} \\ & - y^{(p-1)+(p-1)p+10p^2}x^{2+p+(p-2)p^2} + 3y^{(p-2)+p+8p^2}x^{4+(p-1)p} \\ & - 3y^{(p-3)+3p+5p^2}x^{5+(p-3)p+3p^2} + y^{(p-4)+5p+2p^2}x^{6+(p-5)+6p^2} \\ & + 2y^{1+(p-3)p+9p^2}x^{4p+(p-1)p^2} - 6y^{5+(p-3)p+3p^2}x^{2+2p+2p^2} \\ & + 6y^{(p-1)+4p^2}x^{3+5p^2} - 2y^{(p-2)+2p+p^2}x^{4+(p-2)p+7p^2} \\ & - y^{3+(p-6)p+8p^2}x^{(p-1)+6p} + 3y^{2+(p-4)p+5p^2}x^{5p+3p^2} \\ & - 3y^{1+(p-2)p+2p^2}x^{1+3p+6p^2} + x^{2+p+9p^2}.\end{aligned}$$

It is clear that, for $p > 7$, the only blocks that can admit a monomial of maximal degree are

$$\begin{aligned}A_1 &= -y^{2+p+(p-2)p^2}x^{(p-1)+(p-1)p+10p^2} \\ &= -\sum \binom{2}{\alpha_0}\binom{1}{\alpha_1}\binom{p-2}{\alpha_2}x^{(p-1+\alpha_0)+(p-1+\alpha_1)p+(10+\alpha_2)p^2} \\ A_2 &= -y^{(p-1)+(p-1)p+10p^2}x^{2+p+(p-2)p^2} \\ &= -\sum \binom{p-1}{\alpha_0}\binom{p-1}{\alpha_1}\binom{10}{\alpha_2}x^{(2+\alpha_0)+(1+\alpha_1)p+(p-2+\alpha_2)p^2},\end{aligned}$$

hence the two coefficients for the monomial of maximal degree are

$$\begin{aligned}c_1 &= -\binom{2}{0}\binom{1}{0}\binom{p-2}{p-11} \\ &= -\binom{p-2}{p-11} \\ &= \frac{2 \times 3 \times \cdots \times 10}{9!} \\ &= 10.\end{aligned}$$

$$\begin{aligned} c_2 &= -\binom{p-1}{p-3}\binom{p-1}{p-2}\binom{10}{1} \\ &= -(-1)^{2p-5}10 \\ &= 10. \end{aligned}$$

Hence the coefficient of the maximal degree term is $20 \neq 0$. This eliminates this exponent.

7.9. Exponent #9

We consider $n = 2 + (p-1)p^2$ and $t = 1 + 2p + 3p^2$. Then we have

$$\begin{aligned} (y^n - x^n)^t = {} & y^{1+3p+8p^2} - 3y^{1+4p+5p^2}x^{(p-1)p+2p^2} + 3y^{1+5p+2p^2}x^{(p-2)p+5p^2} \\ & - y^{6p+(p-1)p^2}x^{(p-3)p+8p^2} - 2y^{2+8p^2}x^{(p-1)+2p} \\ & + 6y^{2+p+5p^2}x^{(p-1)+p+3p^2} - 6y^{2+2p+2p^2}x^{(p-1)+6p^2} \\ & + 2y^{1+3p+(p-1)p^2}x^{(p-1)+(p-1)p+8p^2} + y^{3+(p-3)p+7p^2}x^{(p-2)+5p} \\ & - 3y^{3+(p-2)p+4p^2}x^{(p-2)+4p+3p^2} + 3y^{3+(p-1)p+p^2}x^{(p-2)+3p+6p^2} \\ & - y^{2+(p-1)p^2}x^{(p-2)+2p+9p^2} - y^{(p-2)+2p+9p^2}x^{2+(p-1)p^2} \\ & + 3y^{(p-2)+3p+6p^2}x^{3+(p-1)p+p^2} - 3y^{(p-2)+4p+3p^2}x^{3+(p-2)p+4p^2} \\ & + y^{(p-2)+5p}x^{3+(p-3)p+7p^2} + 2y^{(p-1)+(p-1)p+8p^2}x^{1+3p+(p-1)p^2} \\ & - 6y^{(p-1)+6p^2}x^{2+2p+2p^2} + 6y^{(p-1)+p+3p^2}x^{2+p+5p^2} \\ & - 2y^{(p-1)+2p}x^{2+8p^2} - y^{(p-3)p+8p^2}x^{6p+(p-1)p^2} \\ & + 3y^{(p-2)p+5p^2}x^{1+5p+2p^2} - 3y^{(p-1)p+2p^2}x^{1+4p+5p^2} + x^{1+3p+8p^2}. \end{aligned}$$

Clearly, for $p > 7$, the only blocks that admit a monomial of maximal degree are

$$\begin{aligned} A_1 &= 2y^{1+3p+(p-1)p^2}x^{(p-1)+(p-1)p+8p^2} \\ &= 2\sum \binom{1}{\alpha_0}\binom{3}{\alpha_1}\binom{p-1}{\alpha_2}x^{(p-1+\alpha_0)+(p-1+\alpha_1)p+(8+\alpha_2)p^2} \\ A_2 &= 2y^{(p-1)+(p-1)p+8p^2}x^{1+3p+(p-1)p^2} \\ &= 2\sum \binom{p-1}{\alpha_0}\binom{p-1}{\alpha_1}\binom{8}{\alpha_2}x^{(1+\alpha_0)+(3+\alpha_1)p+(p-1+\alpha_2)p^2}, \end{aligned}$$

hence the two coefficients for the monomial of maximal degree are

$$c_1 = 2\binom{1}{0}\binom{3}{0}\binom{p-1}{p-9}$$

$$\begin{aligned} &= 2(-1)^8 \\ &= 2. \end{aligned}$$

$$\begin{aligned} c_2 &= 2\binom{p-1}{p-2}\binom{p-1}{p-4}\binom{8}{0} \\ &= 2(-1)^{2p-6} \\ &= 2. \end{aligned}$$

Thus the coefficient of the x^{q-1} term is 4, and we have eliminated this exponent.

7.10. Exponent #10

Let $n = 2p + (p-1)p^2$ and $t = 2 + (p-1)p$. Then

$$\begin{aligned} n(p-1-i) &= (2p-2-2i)p + (p-1)(p-1-i)p^2 \\ &= (2p-2-2i)p + (p-1) - (i+1) + (i+1)p^2 \\ &= (p-i-2) + (2p-2i-2)p + (i+1)p^2, \\ ni &= 2ip + i(p-1)p^2 \\ &= (i-1) + 2ip + (p-i)p^2. \end{aligned}$$

Now

$$\begin{aligned} (y^n - x^n)^2 &= y^{2n} - 2x^n y^n + x^{2n} \\ &= y^{1+4p+(p-2)p^2} - 2x^{2p+(p-1)p^2} y^{2p+(p-1)p^2} + x^{1+4p+(p-2)p^2}. \end{aligned}$$

Hence we have

$$\begin{aligned} (y^n - x^n)^{(p-1)p} &= \sum_{i=0}^{p-1} y^{inp} x^{n(p-1-i)p} \\ &= \sum_{i=0}^{p-1} y^{(p-i)+(i-1)p+2ip^2} x^{(i+1)+(p-i-2)p+(2p-2i-2)p^2}. \end{aligned}$$

Then

$$(y^n - x^n)^t = A_1 - 2A_2 + A_3,$$

where we set

$$A_1 = y^{1+4p+(p-2)p^2} \sum_{i=0}^{p-1} y^{(p-i)+(i-1)p+2ip^2} x^{(i+1)+(p-i-2)p+(2p-2i-2)p^2}$$
$$= \sum_{i=0}^{p-1} y^{(p-i+2)+(i+3)p+(2i-2)p^2} x^{(i+1)+(p-i-2)p+(2p-2i-2)p^2}$$
$$A_2 = x^{2p+(p-1)p^2} y^{2p+(p-1)p^2} \sum_{i=0}^{p-1} y^{(p-i)+(i-1)p+2ip^2} x^{(i+1)+(p-i-2)p+(2p-2i-2)p^2}$$
$$= \sum_{i=0}^{p-1} y^{(p-i+1)+(i+1)p+(2i-1)p^2} x^{(i+2)+(p-i)p+(2p-2i-3)p^2}$$
$$A_3 = x^{1+4p+(p-2)p^2} \sum_{i=0}^{p-1} y^{(p-i)+(i-1)p+2ip^2} x^{(i+1)+(p-i-2)p+(2p-2i-2)p^2}$$
$$= \sum_{i=0}^{p-1} y^{(p-i)+(i-1)p+2ip^2} x^{(i+3)+(p-i+2)p+(2p-2i-4)p^2}.$$

We start analysing A_1 for which we have the following exponents:

$$3 \le p-i+2 \le p+2, \qquad 3 \le i+3 \le p+2, \qquad -2 \le 2i-2 \le 2p-4,$$
$$1 \le i+1 \le p, \qquad -1 \le p-i-2 \le p-2, \qquad 0 \le 2p-2i-2 \le 2p-2.$$

For $i \le 2$ we cannot obtain a term of maximal degree since $p-i+2 \ge p$ and $(p-i+2-p)+(i+1)=3$. The same holds for $i=p-1$, since $(p-i+2)+(i+1-p)=3$, and for $i=p-2$, since $(i+3-p)+(p-i-2)=1$. (It is easy to check these terms.) Hence we just need to consider the following:

$$\sum_{i=3}^{p-3} y^{(p-i+2)+(i+3)p+(2i-2)p^2} x^{(i+1)+(p-i-2)p+(2p-2i-2)p^2}.$$

Apart from the coefficients related to the p^2 part, all the rest are positive and less than p. Now if $i \le \frac{p-3}{2}$, we have $2i-2 \le p-5$ and $2p-2i-2 \ge 2p-p+3-2 = p+1$. Therefore the maximal degree cannot be reached since $(2i-2)+(2p-2i-2-p) = p-4$. If $i \ge \frac{p+3}{2}$ we have $2i-2 \ge p+1$ and $2p-2i-2 \le p-5$. Therefore the maximal degree cannot be reached since $(2i-2-p)+(2p-2i-2) = p-4$. Hence we remain with $i \in \{\frac{p-1}{2}, \frac{p+1}{2}\} = \{m, m+1\}$. Hence the coefficient related to the maximal degree is

$$c_1 = \binom{m+3}{m-1}\binom{m+3}{m+1}\binom{p-3}{0} + \binom{m+2}{m-2}\binom{m+4}{m+2}\binom{p-1}{2}$$
$$= \frac{(m+3)(m+2)(m+1)m}{2!4!}[(m+3)(m+2)+(m+4)(m-1)]$$
$$= \frac{(m+3)(m+2)(m+1)m}{2!4!} \cdot (-m-2)$$

$$= \frac{-(m+3)(m+2)^2(m+1)m}{2 \times 4!}.$$

Analysing A_2, we have

$$A_2 = \sum_{i=0}^{p-1} y^{(p-i+1)+(i+1)p+(2i-1)p^2} x^{(i+2)+(p-i)p+(2p-2i-3)p^2}.$$

We have the following exponents:

$$2 \leq p-i+1 \leq p+1, \qquad 1 \leq i+1 \leq p, \qquad -1 \leq 2i-1 \leq 2p-3,$$
$$2 \leq i+1 \leq p+1, \qquad 1 \leq p-i \leq p, \qquad -1 \leq 2p-2i-3 \leq 2p-3.$$

If one of the exponents is greater than or equal to p, then similarly to the previous case, we cannot obtain a monomial of maximal degree. Hence analysing the restriction on the exponents it is possible to derive that the only value for i which produces a maximal degree term is $i = m$. Therefore the coefficient is

$$\begin{aligned} c_2 &= \binom{m+2}{m-2}\binom{m+1}{m-1}\binom{p-2}{1} \\ &= \frac{-(m+2)(m+1)^2m^2(m-1)}{4!}. \end{aligned}$$

For A_3,

$$A_3 = \sum_{i=0}^{p-1} y^{(p-i)+(i-1)p+2ip^2} x^{(i+3)+(p-i+2)p+(2p-2i-4)p^2}.$$

We have the following exponents:

$$1 \leq p-i \leq p, \qquad -1 \leq i-1 \leq p-2, \qquad 0 \leq 2i \leq 2p-2,$$
$$3 \leq i+3 \leq p+2, \qquad 3 \leq (p-i+2) \leq p-2, \qquad -2 \leq 2p-2i-4 \leq 2p-4.$$

With the same argument as before we have the only possible monomial of maximal degree for $i \in \{\frac{p-3}{2}, \frac{p-1}{2}\} = \{m-1, m\}$. Hence we have coefficient

$$c_3 = \binom{m+2}{m-2}\binom{m-2}{m-4}\binom{p-3}{0} + \binom{m+1}{m-3}\binom{m-1}{m-3}\binom{p-1}{2}.$$

It is not difficult to prove that $c_1 = c_3$. In total we have a maximal degree term with coefficient $c = 2c_1 - 2c_2$. Now

$$\begin{aligned}
c_1 - c_2 &= \frac{-(m+3)(m+2)^2(m+1)m}{2\times 4!} + \frac{(m+2)(m+1)^2m^2(m-1)}{4!} \\
&= \frac{m(m+1)(m+2)}{2\times 4!}\left(2(m-1)(m)(m+1) - (m+3)(m+2)\right) \\
&= \frac{m(m+1)(m+2)}{2\times 4!}\left(2m^3 - m^2 - 7m - 6\right) \\
&= \frac{m(m+1)(m+2)}{2\times 4!}\left(2\frac{-1}{2^3} - \frac{1}{2^2} + \frac{7}{2} - 6\right) \\
&= \frac{m(m+1)(m+2)}{2\times 4!}\left(-3\right),
\end{aligned}$$

which is clearly non-zero for $p \geq 11$. Thus Exponent #10 is eliminated.

7.11. Exponent #11

Let $n = 1 + p + (p-1)p^2$ and $t = p - 1$. Then

$$\begin{aligned}
n(p-1-i) &= (p-1-i) + (p-1-i)p + (p-1-i)(p-1)p^2 \\
&= (p-3-2i) + (p-i)p + (i+1)p^2, \\
ni &= i + ip + i(p-1)p^2 \\
&= (2i-1) + ip + (p-i)p^2.
\end{aligned}$$

In this case we have

$$\begin{aligned}
(y^n - x^n)^{p-1} &= \sum_{i=0}^{p-1} y^{ni} x^{n(p-1-i)} \\
&= \sum_{i=0}^{p-1} y^{2i-1+ip+(p-i)p^2} x^{(p-3-2i)+(p-i)p+(i+1)p^2}.
\end{aligned}$$

For $i = 0$ or $i = p-1$ it is easy to verify that we cannot obtain a monomial of maximal degree. For $i \leq \frac{p-3}{2}$ and for $i \geq \frac{p+1}{2}$, by analysing the coefficients related to the p^0 exponent, it can be observed that no term of maximal degree can be obtained. Hence we are left with the case $i = \frac{p-1}{2} = m$, which is

$$y^{p-2+mp+(m+1)p^2} x^{(p-2)+mp+(m+1)p^2}.$$

Hence the coefficient corresponding to the term of degree $p^3 - 1$ is

$$\begin{aligned}
c =& \binom{p-2}{p-1-(p-2)}\binom{m}{p-1-m}\binom{m+1}{p-1-(m+1)} \\
=& \binom{p-2}{1}\binom{m}{m}\binom{m+1}{m-1}
\end{aligned}$$

$$
\begin{aligned}
&= -2\frac{(m+1)(m)}{2} \\
&= -\left(-\frac{1}{2}+1\right)\left(-\frac{1}{2}\right) \\
&= \frac{1}{4} \neq 0.
\end{aligned}
$$

This eliminates Exponent #11, the last remaining explicit case.

References

[1] W. Bosma, J. Cannon, C. Playoust, The Magma algebra system I: the user language, J. Symb. Comput. 24 (1997) 235–265.
[2] W-S. Chou, X-D. Hou, On a conjecture of Fernando, Hou and Lappano concerning permutation polynomials over finite fields, Finite Fields Appl. 56 (2019) 58–92.
[3] R.S. Coulter, The classification of planar monomials over fields of prime square order, Proc. Am. Math. Soc. 134 (2006) 3373–3378.
[4] R.S. Coulter, F. Lazebnik, On the classification of planar monomials over fields of square order, Finite Fields Appl. 18 (2012) 316–336.
[5] R.S. Coulter, R.W. Matthews, Planar functions and planes of Lenz-Barlotti class II, Des. Codes Cryptogr. 10 (1997) 167–184.
[6] P. Dembowski, T.G. Ostrom, Planes of order n with collineation groups of order n^2, Math. Z. 103 (1968) 239–258.
[7] L.E. Dickson, The analytic representation of substitutions on a power of a prime number of letters with a discussion of the linear group, Ann. Math. 11 (1897) 65–120, pp. 161–183.
[8] D. Gluck, Affine planes and permutation polynomials, in: Coding Theory and Design Theory, Part II (Design Theory), in: The IMA Volumes in Mathematics and Its Applications, vol. 21, Springer-Verlag, 1990, pp. 99–100.
[9] C. Hermite, Sur les fonctions de sept lettres, C. R. Acad. Sci. Paris 57 (1863) 750–757.
[10] Y. Hiramine, A conjecture on affine planes of prime order, J. Comb. Theory, Ser. A 52 (1989) 44–50.
[11] X-D. Hou, Permutation polynomials over finite fields – a survey of recent advances, Finite Fields Appl. 32 (2015) 82–119.
[12] N.L. Johnson, Projective planes of order p that admit collineation groups of order p^2, J. Geom. 30 (1987) 49–68.
[13] E. Lucas, Théorie des fonctions numériques simplement périodiques, Am. J. Math. 1 (1878) 184–240, 289–321.
[14] L. Rónyai, T. Szőnyi, Planar functions over finite fields, Combinatorica 9 (1989) 315–320.
[15] M.E. Zieve, Planar functions and perfect nonlinear monomials over finite fields, Des. Codes Cryptogr. 75 (2015) 71–80.