Journal der mathematischen Ablehnungen
Paper No.27 (2012)

On the classification of planar monomials over fields of square order

Robert S. Coulter and Felix Lazebnik

Department of Mathematical Sciences, University of Delaware,
Newark DE, 19716, U.S.A.

AMS Subject class: 11T06, 12E10

Keywords: planar functions, planar monomials, permutation polynomials

Note: This is a personal preprint; for correct page numbering and references please see the original paper, the proper citation for which is:

R.S. Coulter and F. Lazebnik, *On the classification of planar monomials of square order*, Finite Fields Appl. **18** (2012), 316–336.

Abstract

Let $\mathbb{F}_q$ be a finite field of characteristic p and $\mathbb{F}_q[X]$ denote the ring of polynomials in X over $\mathbb{F}_q$. A polynomial $f \in \mathbb{F}_q[X]$ is called a *permutation polynomial* over $\mathbb{F}_q$ if f induces a bijection of $\mathbb{F}_q$ under substitution. A polynomial $f \in \mathbb{F}_q[X]$ is said to be *planar* over $\mathbb{F}_q$ if for every non-zero $a \in \mathbb{F}_q$, the polynomial $f(X+a) - f(X)$ is a permutation polynomial over $\mathbb{F}_q$. Planar polynomials have only been classified over prime fields, whereas the problem of classifying planar monomials has only been completely resolved over fields of order p and p^2. In this article we study planar monomials over fields of square order, obtaining a complete classification of planar monomials over fields of order p^4.

§ 1. Introduction

Let p be a prime, e a natural number, $q = p^e$ and let $\mathbb{F}_q$ denote the finite field of order q. For any integer n with $0 \leq n < q$, we write $n = (a_{e-1}a_{e-2}\cdots a_0)_p$ to denote the base p expansion of n; so $n = \sum_{i=0}^{e-1} a_i p^i$.

The ring of polynomials in X over $\mathbb{F}_q$ is denoted $\mathbb{F}_q[X]$. A polynomial $f \in \mathbb{F}_q[X]$ is called a *permutation polynomial* over $\mathbb{F}_q$ if f induces a bijection of $\mathbb{F}_q$ under substitution. A polynomial $f \in \mathbb{F}_q[X]$ is said to be *planar* over $\mathbb{F}_q$ if for every non-zero $a \in \mathbb{F}_q$, the polynomial $f(X+a) - f(X)$ is a permutation polynomial over $\mathbb{F}_q$. It is straightforward to show

- no planar polynomial can exist over fields of even characteristic; and
- the polynomial X^2 is planar over any field of odd characteristic.

In light of the first point, we assume that p is an odd prime in all that follows.

The slightly more general concept of a planar function was introduced in 1968 by Dembowski and Ostrom [3], the concept arising naturally from their study of projective planes with a collineation group acting transitively on the affine points. At the end of their paper, they suggested that all planar polynomials might be of a special form; their suggestion is nowadays attributed to them as a conjecture.

Conjecture 1 (Dembowski and Ostrom, 1968). *A planar polynomial is necessarily a Dembowski-Ostrom polynomial; that is, a polynomial over a finite field of characteristic p of the shape*

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

The conjecture was proved for prime fields around 1989 and 1990, independently by Gluck [5], Hiramine [7], and Rónyai and Szönyi [10]. Johnson [8] had already proved the conjecture for monomials over prime fields in 1987, while Coulter [1] established the conjecture for monomials over fields of order p^2 in 2006. In 1997, Coulter and Matthews [2] showed the conjecture to be false in characteristic 3, the smallest counterexample being X^{14} over $\mathbb{F}_{3^4}$. However, the infinite class of counterexamples given in that article remain the only ones known (up to equivalence), and the conjecture remains open for any characteristic larger than 3.

In this paper we consider planar monomials over fields of square order. We prove Conjecture 1 for fields of order p^4 with $p \geq 5$, and reduce the problem significantly for all fields of order p^{2^k} with $p \geq 5$ and $k \geq 3$. Our main results are given in Section 3.

§ 2. Background results

For the convenience of the reader, we gather the most relevant background results together in this section.

Most critical to our approach is the classical criterion of Hermite for a polynomial to be a permutation polynomial.

Lemma 2 (Hermite, [6]; Dickson, [4]). *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 $q-1$.

We will also need the following well known theorem of Lucas.

Lemma 3 (Lucas, [9]). *Let p be a prime and $\alpha \geq \beta$ be positive integers with $\alpha = (\alpha_t \cdots \alpha_0)_p$ and $\beta = (\beta_t \cdots \beta_0)_p$. 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 following lemma simplifies the planarity condition for monomials.

Lemma 4 (Coulter and Matthews, [2, Proposition 2.4]). *The polynomial X^n is planar over $\mathbb{F}_q$ if and only if $(X+1)^n - X^n$ is a permutation polynomial over $\mathbb{F}_q$. Further, if X^n is a planar polynomial over $\mathbb{F}_q$, then $n \equiv 2 \bmod p-1$ and $(n, q-1) = 2$.*

The following corollary of Lemma 4 is used often in this paper.

Lemma 5. *If X^n is planar over $\mathbb{F}_q$, then X^n is planar over every subfield of $\mathbb{F}_q$.*

We note that when $q = p^e = p^{2w}$ and $n = (a_{e-1} \cdots a_0)_p$,

$$n = \sum_{i=0}^{e-1} a_i p^i \equiv \sum_{i=0}^{w-1} (a_i + a_{i+w}) p^i \bmod (p^w - 1),$$

so that by Lemma 5 the w-tuple

$$(a_0 + a_{0+w}, a_1 + a_{1+w}, \ldots, a_{w-1} + a_{e-1})$$

arises naturally when considering the planarity of X^n over $\mathbb{F}_q$.

As already mentioned, the classification of planar monomials over prime fields was given by Johnson.

Lemma 6 (Johnson, [8, Theorem 4.6]). *The monomial X^n is planar over $\mathbb{F}_p$, p an odd prime, if and only if $n \equiv 2 \bmod (p-1)$.*

The classification of planar monomials over fields of order p^2 reads similarly.

Lemma 7 (Coulter, [1, Theorem 2.1]). *The monomial X^n is planar over $\mathbb{F}_{p^2}$, p an odd prime, if and only if $n \equiv 2p^j \bmod (p^2-1)$ for some integer $0 \leq j < 2$.*

Finally, we will use the following important fact.

Lemma 8 (Coulter and Matthews, [2, Theorem 2.3]). *The monomial X^n is planar over $\mathbb{F}_q$ if and only if X^{np^i} is planar over $\mathbb{F}_q$ for any non-negative integer i.*

The practical consequence of Lemma 8 is that when considering the planarity X^n over $\mathbb{F}_{p^e}$ with $n = (a_{e-1} \cdots a_0)_p$, we can, to suit our needs, consider any X^k, where $k = (a_{e-i-1} \cdots a_0 a_{e-1} \cdots a_{e-i})_p$ is a "cyclic shift" of n.

§ 3. Outline of article and main results

We now outline the logic of our approach and state the key theorems of this article. Since X^n and $X^{n \bmod (q-1)}$ are planar equivalent, we shall only consider monomials of degree less than $q-1$.

Theorem 9. *Let $q = p^e$ with p an odd prime and $e = 2w$ with $w \geq 2$. Suppose X^n is planar over $\mathbb{F}_q$, $n < q$, and there exists an integer j, $0 \leq j < w$, for which $n \equiv 2p^j \bmod (p^w - 1)$. If $n = (a_{e-1} \cdots a_0)_p$, then some cyclic shift of the w-tuple*

$$(a_0 + a_{0+w}, a_1 + a_{1+w}, \ldots, a_{w-1} + a_{e-1})$$

must be one of the following:

$$(0, 0, \ldots, 0, 2),$$
$$(p-1, p-1, \ldots, p-1, p+1), \quad \textit{or}$$
$$(\underbrace{0, 0, \ldots, 0}_{m \geq 0 \text{ times}}, p, \underbrace{p-1, p-1, \ldots, p-1}_{w-2-m \text{ times}}, 1).$$

We shall refer to the three possible w-tuples listed in the above theorem as Cases 1, 2 and 3, respectively. The planarity of Cases 1 and 2 can be resolved completely.

Theorem 10. *Let $q = p^e$ with p an odd prime and $e = 2w$ with $w \geq 2$. Let the natural number $n < q$ be given by $n = (a_{e-1} \cdots a_0)_p$, and suppose*

$$V = (a_0 + a_{0+w}, a_1 + a_{1+w}, \ldots, a_{w-1} + a_{e-1}) = (0, 0, \ldots, 0, 2).$$

Then X^n is planar over $\mathbb{F}_q$ if and only if $n = 2p^j$ for some integer $0 \leq j < e$.

Theorem 11. *Let $q = p^e$ with p an odd prime and $e = 2w$ with $w \geq 2$. Let the natural number $n < q$ be given by $n = (a_{e-1} \cdots a_0)_p$, and suppose*

$$V = (a_0 + a_{0+w}, a_1 + a_{1+w}, \ldots, a_{w-1} + a_{e-1}) = (p-1, p-1, \ldots, p-1, p+1).$$

Then X^n is not planar over $\mathbb{F}_q$.

We note that Theorem 9 provides a way forward to proving Conjecture 1 for monomials over all fields of order p^e, $p \geq 5$, with $e = 2^k$. Using Lemmas 6 and 7 as base cases, an inductive argument on k can be employed. If one could show, for arbitrary $k \geq 2$, that Case 3 contains no examples of planar monomials, then the conditions of Theorem 9 would be satisfied inductively, and Conjecture 1 would be established for monomials over these fields. We are unable to do this in general, though we do complete the classification of planar monomials when $k = 2$.

Theorem 12. *The polynomial X^n is planar over $\mathbb{F}_{p^4}$, $p \geq 5$ an odd prime, if and only if $n \equiv 2p^j \bmod (p^4 - 1)$ for some integer $0 \leq j < 4$.*

Before we present our proofs, we feel it beneficial to give an outline of the proof of this last theorem, as it encompasses most of the general ideas in this article.

Suppose X^n is planar over $\mathbb{F}_{p^4}$, with $n = (a_3\, a_2\, a_1\, a_0)_p$. By Lemma 5, X^n must be planar over both $\mathbb{F}_p$ and $\mathbb{F}_{p^2}$. The classifications of planar monomials over these fields, see Lemmas 6 and 7, show that the conditions of Theorem 9 are satisfied, and therefore a cyclic shift of the 2-tuple $(a_0 + a_2, a_1 + a_3)$ must be one of $(0, 2)$, $(p-1, p+1)$, or $(p, 1)$. Theorem 11 and two lemmas to be established – Lemmas 13 and 14 – exclude the latter two possibilities, while Theorem 10 confirms the form of n in the first case, completing the proof.

Theorem 12 completes the classification of planar monomials over all fields of order p^4 with p an odd prime. The case $p = 3$ is easily checked via computation – the only additional planar monomials obtained are equivalent to the monomial X^n with $n = (3^\alpha + 1)/2$, α odd. As mentioned in the introduction, these constitute the smallest counterexamples to the Dembowski-Ostrom conjecture.

The remainder of the article consists of the proofs of Theorems 9, 10, 11 and 12. We note that our method for establishing Theorem 12 does not appear to generalise in any natural way to a proof that Case 3 yields no further example of a planar monomial in any field of order p^e where $p \geq 5$ and $e = 2^k$, $k \geq 3$.

§ 4. Proof of Theorem 9

By hypothesis,

$$n \equiv 2p^j \bmod (p^w - 1),$$

with $0 \leq j < w$. Without loss of generality we may assume $j = w - 1$, as otherwise we may apply Lemma 8 to obtain n' with the desired property. Such an application will result in a cyclic shift of the w-tuple

$$V = (a_0 + a_{0+w}, a_1 + a_{1+w}, \ldots, a_{w-1} + a_{e-1}).$$

We shall refer to the $(i+1)$st term of this tuple by $V[i]$. We have

$$\begin{aligned} n = \sum_{i=0}^{e-1} a_i p^i &\equiv \sum_{i=0}^{w-1} (a_i + a_{i+w}) p^i \bmod (p^w - 1) \\ &\equiv \sum_{i=0}^{w-1} V[i] p^i \bmod (p^w - 1) \\ &\equiv 2p^{w-1} \bmod (p^w - 1), \end{aligned}$$

where the last step follows from our initial comments above. Since $0 \leq a_i \leq p - 1$ for all i, it follows that

$$\sum_{i=0}^{w-1} V[i] p^i = t(p^w - 1) + 2p^{w-1},$$

where $t \in \{0, 1\}$.

Suppose $t = 1$. Then

$$\sum_{i=0}^{w-1} V[i] p^i = p^w - 1 + 2p^{w-1}. \tag{1}$$

Firstly, (1) modulo p yields $V[0] \equiv -1 \bmod p$. As $0 \leq a_i \leq p-1$ for all i, it follows that $V[0] = a_0 + a_w = p - 1$. Suppose for some integer j that $V[i] = p - 1$ for all $0 \leq i < j < w - 1$. Equation 1 modulo p^{j+1} yields

$$\sum_{i=0}^{w-1} V[i] p^i \equiv -1 \bmod p^{j+1}.$$

On the other hand,

$$\begin{aligned}\sum_{i=0}^{w-1} V[i]p^i &\equiv \sum_{i=0}^{j} V[i]p^i \bmod p^{j+1}\\ &\equiv (p-1)\frac{p^j-1}{p-1} + V[j]p^j \bmod p^{j+1}\\ &\equiv -1 + p^j(1+V[j]) \bmod p^{j+1}.\end{aligned}$$

Thus

$$-1 + p^j(1+V[j]) \equiv -1 \bmod p^{j+1},$$

so that $1+V[j]$ is a multiple of p. Hence $V[j] = a_j + a_{j+w} = p-1$. By induction we have $V[i] = p-1$ for $0 \le i < w-1$. Returning to (1) yields

$$\begin{aligned}p^w - 1 + 2p^{w-1} &= \sum_{i=0}^{w-1} V[i]p^i\\ &= (p-1)\frac{p^{w-1}-1}{p-1} + V[w-1]p^{w-1}\\ &= -1 + p^{w-1}(1+V[w-1]),\end{aligned}$$

from which it follows that $V[w-1] = p+1$. So when $t=1$ we must have

$$V = (p-1, p-1, \ldots, p-1, p+1).$$

Now suppose $t=0$, so that

$$\sum_{i=0}^{w-1} V[i]p^i = 2p^{w-1}. \tag{2}$$

We follow a similar procedure to the previous case. To begin, we have $V[0] \equiv 0 \bmod p$. It follows that $V[0] = a_0 + a_w = 0$ or p. Suppose for some j, $V[i] = 0$ for all $0 \le i < j < w-1$. Then (2) modulo p^{j+1} yields $V[j]p^j \equiv 0 \bmod p^{j+1}$, from which we have $V[j] = 0$ or p. In particular, if $V[i] = 0$ for all $0 \le i < w-1$, then (2) implies $V[w-1] = 2$, so that

$$V = (0, 0, \ldots, 0, 2).$$

Otherwise, there exists some integer m, $0 \le m < w-1$, for which $V[i] = 0$ for all $0 \le i < m$ and $V[m] = p$. If $m = w-2$, then we must have $V[w-1] = 1$ by (2). Otherwise, taking (2) modulo p^{m+2} yields $(1+V[m+1])p^{m+1} \equiv 0 \bmod p^{m+2}$, so that $V[m+1] = p-1$. Now an inductive argument shows $V[i] = p-1$ for all $m+1 \le i < w-1$ and $V[w-1] = 1$. (We omit the details as they are almost exactly the same as our earlier induction.) Thus, in our final case we must have

$$V = (\underbrace{0, 0, \ldots, 0}_{m \ge 0 \text{ times}}, p, \underbrace{p-1, p-1, \ldots, p-1}_{w-2-m \text{ times}}, 1).$$

§ 5. Resolution of Cases 1 and 2

Next we establish Theorems 10 and 11. The first proof is straightforward.

Proof of Theorem 10. Suppose $V = (0, 0, \ldots, 0, 2)$. Then either $n = 2p^{w-1}$, $2p^{2w-1}$ or $p^{w-1} + p^{2w-1}$.

Suppose $n = 2p^{w-1}$ or $2p^{2w-1}$. An application of Lemma 8 to X^n shows that it is planar equivalent to X^2, and we have already noted X^2 is planar over any field of odd characteristic.

On the other hand, since $(p^{w-1} + p^{2w-1}, q-1) = p^w + 1 > 2$, X^n with $n = p^{w-1} + p^{2w-1}$ cannot be planar over $\mathbb{F}_q$ by Lemma 4. □

Case 2 is more involved; it is a direct generalisation of the proof of [1], Theorem 2.1.

Proof of Theorem 11. Set $f(X) = (X+1)^n - X^n$ and $Q = p^w$. Note $q = p^{2w} = Q^2$. Since $a_{w-1} + a_{2w-1} = p+1$, we must have $2 \leq a_{w-1} < p$ and $2 \leq a_{2w-1} < p$. Consider the polynomial

$$f(X)^{Q+1} = (X+1)^{n(Q+1)} + X^{n(Q+1)} - X^{nQ}(X+1)^n - X^n(X+1)^{nQ}. \tag{3}$$

We show that the reduction of $f(X)^{Q+1}$ modulo $X^q - X$ has degree $q-1$. It will then follow from Lemma 2 that f cannot be a permutation polynomial over $\mathbb{F}_q$ and so X^n is not planar over $\mathbb{F}_q$, establishing the result. We consider the reduction of each summand on the right hand side of (3) separately, determining the coefficient of X^{q-1} in each case.

Set $h(X) = (X+1)^n$. Since $h \in \mathbb{F}_p[X]$, it follows from Lemma 3 that

$$h(X) = \sum_{\alpha_0=0}^{a_0} \sum_{\alpha_1=0}^{a_1} \cdots \sum_{\alpha_{2w-1}=0}^{a_{2w-1}} \left(\prod_{i=0}^{2w-1} \binom{a_i}{\alpha_i} \right) X^{F(\alpha_0, \alpha_1, \ldots, \alpha_{2w-1})},$$

where $F(\alpha_0, \alpha_1, \ldots, \alpha_{2w-1}) = \sum_{i=0}^{2w-1} \alpha_i p^i$. We also have

$$h(X)^Q \equiv \sum_{\alpha_0=0}^{a_0} \sum_{\alpha_1=0}^{a_1} \cdots \sum_{\alpha_{2w-1}=0}^{a_{2w-1}} \left(\prod_{i=0}^{2w-1} \binom{a_i}{\alpha_i} \right) X^{G(\alpha_0, \alpha_1, \ldots, \alpha_{2w-1})} \bmod (X^q - X),$$

where $G(\alpha_0, \alpha_1, \ldots, \alpha_{2w-1}) = \sum_{i=0}^{w-1} \alpha_i p^{w+i} + \alpha_{w+i} p^i$. It follows that $h(X)^{Q+1} \bmod (X^q - X)$ is

$$\sum_{\alpha_0=0}^{a_0} \cdots \sum_{\alpha_{2w-1}=0}^{a_{2w-1}} \sum_{\beta_0=0}^{a_0} \cdots \sum_{\beta_{2w-1}=0}^{a_{2w-1}} \left(\prod_{i=0}^{2w-1} \binom{a_i}{\alpha_i} \binom{a_i}{\beta_i} \right) X^{F(\alpha_0, \ldots, \alpha_{2w-1}) + G(\beta_0, \ldots, \beta_{2w-1})}.$$

It is clear from their general forms that both F and G are always less than $q-1$. Consequently,

$$\begin{aligned} F(\alpha_0, \ldots, \alpha_{2w-1}) + G(\beta_0, \ldots, \beta_{2w-1}) &= \sum_{i=0}^{w-1} (\alpha_i + \beta_{w+i}) p^i + (\alpha_{w+i} + \beta_i) p^{w+i} \\ &< 2(q-1). \end{aligned}$$

Hence the only terms of degree $q-1$ in $h(X)^{Q+1} \bmod (X^q - X)$ are those terms where

$$F(\alpha_0, \ldots, \alpha_{2w-1}) + G(\beta_0, \ldots, \beta_{2w-1}) = q - 1. \tag{4}$$

Since $0 \leq \alpha_i, \beta_i \leq a_i$, we have $\alpha_i + \beta_{w+i} \leq a_i + a_{w+i}$ and $\alpha_{w+i} + \beta_i \leq a_{w+i} + a_i$ for all $0 \leq i \leq w-1$. We note the form of V,

$$\begin{aligned} V &= (a_0 + a_{0+w}, a_1 + a_{1+w}, \ldots, a_{w-1} + a_{e-1}) \\ &= (p-1, p-1, \ldots, p-1, p+1), \end{aligned}$$

thus provides upper bounds on $\alpha_i + \beta_{w+i}$ and $\alpha_{w+i} + \beta_i$.

For (4) to hold, the bounds just given imply $\alpha_i + \beta_{w+i} = \alpha_{w+i} + \beta_i = p-1$ for all $0 \leq i \leq w-1$. Thus we must have $\alpha_i = \beta_i = a_i$ for $0 \leq i \leq w-2$, $w \leq i \leq 2w-2$, and $\alpha_{w-1} + \beta_{2w-1} = \alpha_{2w-1} + \beta_{w-1} = p-1$. However, both $\alpha_{w-1} + \beta_{2w-1}$ and $\alpha_{2w-1} + \beta_{w-1}$ are bounded by $a_{w-1} + a_{2w-1} = p+1$. Therefore, we have

$$\begin{aligned} a_{w-1} - 2 \leq \alpha_{w-1} \leq a_{w-1}, \\ a_{w-1} - 2 \leq \beta_{w-1} \leq a_{w-1}, \end{aligned}$$

and selection of α_{w-1} and β_{w-1} completely determines β_{2w-1} and α_{2w-1}, respectively. Thus the coefficient of X^{q-1} in $h(X)^{Q+1} \bmod (X^q - X)$ is

$$\begin{aligned} c &= \sum_{\alpha_{w-1}=a_{w-1}-2}^{a_{w-1}} \sum_{\beta_{w-1}=a_{w-1}-2}^{a_{w-1}} \binom{a_{w-1}}{\alpha_{w-1}} \binom{a_{2w-1}}{p-1-\alpha_{w-1}} \binom{a_{w-1}}{\beta_{w-1}} \binom{a_{2w-1}}{p-1-\beta_{w-1}} \\ &= \left(\sum_{\alpha_{w-1}=a_{w-1}-2}^{a_{w-1}} \binom{a_{w-1}}{\alpha_{w-1}} \binom{a_{2w-1}}{\alpha_{w-1}+2-a_{w-1}} \right)^2. \end{aligned}$$

Expanding yields

$$\begin{aligned} c &= \left(\binom{a_{w-1}}{2} + \binom{a_{w-1}}{1}\binom{a_{2w-1}}{1} + \binom{a_{2w-1}}{2} \right)^2 \\ &= \left(\frac{a_{w-1}(a_{w-1}-1)}{2} + a_{w-1}a_{2w-1} + \frac{a_{2w-1}(a_{2w-1}-1)}{2} \right)^2 \\ &\equiv \left(\frac{a_{w-1}(a_{w-1}-1)}{2} + a_{w-1}(1-a_{w-1}) + \frac{-a_{w-1}(1-a_{w-1})}{2} \right)^2 \bmod p \\ &\equiv 0 \bmod p. \end{aligned}$$

Hence we get no term of degree $q-1$ from $(X+1)^{n(Q+1)} \bmod (X^q - X)$.

The next summand is $X^{n(Q+1)}$. Recalling $n \equiv 2p^{w-1} \bmod (Q-1)$, we see that $n(Q+1) \equiv 2p^{2w-1} + 2p^{w-1} \bmod q-1$. It follows that $X^{n(Q+1)} \equiv X^{2p^{2w-1}+2p^{w-1}} \bmod (X^q - X)$. So we get no term of degree $q-1$ from $X^{n(Q+1)}$.

Considering the third summand, we have

$$\begin{aligned} X^{nQ}(X+1)^n &\equiv X^{G(a_0,\ldots,a_{2w-1})} h(X) \bmod (X^q - X) \\ &\equiv \sum_{\alpha_0=0}^{a_0} \sum_{\alpha_1=0}^{a_1} \cdots \sum_{\alpha_{2w-1}=0}^{a_{2w-1}} \left(\prod_{i=0}^{2w-1} \binom{a_i}{\alpha_i} \right) X^{H(\alpha_0,\alpha_1,\ldots,\alpha_{2w-1})} \bmod (X^q - X), \end{aligned}$$

where $H(\alpha_0, \alpha_1, \ldots, \alpha_{2w-1}) = \sum_{i=0}^{w-1} (\alpha_i + a_{w+i})p^i + (\alpha_{w+i} + a_i)p^{w+i}$. The only term of degree $q-1$ in $X^{nQ}(X+1)^n \bmod (X^q - X)$ is the term where $\alpha_i = p-1-a_{w+i}$ and $\alpha_{w+i} = p-1-a_i$ for $0 \le i \le w-1$. The coefficient of this term is

$$\binom{a_{w-1}}{2}\binom{a_{2w-1}}{2}.$$

Determining the coefficient of X^{q-1} in the final summand $X^n(X+1)^{nQ}$ is completely similar to the previous one, and produces the same coefficient.

In summary, the coefficient of X^{q-1} in $f(X)^{Q+1} \bmod (X^q - X)$ is

$$\begin{aligned} -2\binom{a_{w-1}}{2}\binom{a_{2w-1}}{2} &= -2\left(\frac{a_{w-1}(a_{w-1}-1)}{2} \right)\left(\frac{a_{2w-1}(a_{2w-1}-1)}{2} \right) \\ &\equiv -2\left(\frac{a_{w-1}(a_{w-1}-1)}{2} \right)^2 \bmod p \\ &\not\equiv 0 \bmod p, \end{aligned}$$

as $2 \le a_{w-1} \le p-1$. Hence $f(X)^{Q+1} \bmod (X^q - X)$ has degree $q-1$, and by Hermite's Criteria, $f(X)$ cannot be a permutation polynomial over $\mathbb{F}_q$. □

§ 6. Case 3

In this final section, we prove Theorem 12. Though long and technical, the proof is straightforward. As noted in Section 3, we need only deal with Case 3 of Theorem 9. Our proof involves two sub-cases, dependent on whether or not the base p expansion of n has a digit of size $p-1$. We first deal with the case when it does not.

Lemma 13. *Set $p \geq 5$ and $q = p^4$. Fix $n = (a_3 \cdots a_0)_p$ and suppose*

$$V = (a_0 + a_2, a_1 + a_3) = (p, 1).$$

If $0 \leq a_i < p-1$ for all $0 \leq i < 4$, then X^n is not planar over $\mathbb{F}_q$.

Proof. Let $h(X) = (X+1)^n$. By Lemma 3, we have

$$h(X) = \sum_{\alpha_0=0}^{a_0} \sum_{\alpha_1=0}^{a_1} \sum_{\alpha_2=0}^{a_2} \sum_{\alpha_3=0}^{a_3} \left(\prod_{i=0}^{3} \binom{a_i}{\alpha_i} \right) X^{\alpha_0+\alpha_1 p+\alpha_2 p^2+\alpha_3 p^3}. \tag{5}$$

Set $g(X) = (h(X) - X^n)^{1+p+p^2+p^3} \bmod (X^q - X)$. We shall prove $g(X)$ has degree $q-1$, thus proving X^n is not planar. As

$$g(X) = \prod_{i=0}^{3} \left((X+1)^{np^i} - X^{np^i} \right),$$

there are 16 resulting polynomials in the expansion to be considered, and we group them into the following cases:

(i) $X^{n(1+p+p^2+p^3)}$,

(ii) $\left\{ \left(h(X) X^{n(p+p^2+p^3)} \right)^{p^i} \ : \ i \in \{0,1,2,3\} \right\}$,

(iii) $\left\{ \left(h(X)^{1+p^2} X^{n(p+p^3)} \right)^{p^i} \ : \ i \in \{0,1\} \right\}$,

(iv) $\left\{ \left(h(X)^{1+p} X^{n(p^2+p^3)} \right)^{p^i} \ : \ i \in \{0,1,2,3\} \right\}$,

(v) $\left\{ \left(h(X)^{1+p+p^2} X^{np^3} \right)^{p^i} \ : \ i \in \{0,1,2,3\} \right\}$,

(vi) $h(X)^{1+p+p^2+p^3}$.

We group them as such because the arguments used for determining the coefficient of any given term X^k modulo $X^q - X$ for any two polynomials in the same case will be alike, up to and including the coefficient of the term of degree $q-1$. Consequently, the actual coefficient of the degree $q-1$ term is the same for all polynomials within a given case. Before continuing, we mention that only Case (iv) will generate a non-zero coefficient and it is only in this case that we need rely on the hypothesis that all p-digits of n are strictly less than $p-1$.

Since $V = (p, 1)$, we know $a_0+a_1+a_2+a_3 = p+1$. It is worth noting that the maximum degree term we must deal with in any of the polynomials in any of these cases is given by $(1+p+p^2+p^3)(a_0+a_1+a_2+a_3) = (1+p+p^2+p^3)(p+1) < 2(q-1)$. Consequently, the only term of degree $q-1$ in a given case modulo $X^q - X$ will result precisely from the term of degree $q-1$ without reduction in the final multiplication, provided we have reduced the result of raising either $h(X)$ or X^n to any given required power of p.

We now determine the coefficient of X^{q-1} in each case modulo $X^q - X$.

(i) Using the base p expansion of n, we see

$$\begin{aligned} X^{np} \bmod (X^q - X) &= X^{a_3+a_0p+a_1p^2+a_2p^3} \\ X^{np^2} \bmod (X^q - X) &= X^{a_2+a_3p+a_0p^2+a_1p^3} \\ X^{np^3} \bmod (X^q - X) &= X^{a_1+a_2p+a_3p^2+a_0p^3}. \end{aligned} \tag{6}$$

Consequently, $X^{n(1+p+p^2+p^3)} \equiv X^k \bmod (X^q - X)$ where $k = (1+p+p^2+p^3)(a_0+a_1+a_2+a_3) = (1+p+p^2+p^3)(p+1)$. Since $q < k < 2(q-1)$, it is clear this term does not reduce to X^{q-1} modulo $X^q - X$.

(ii) We consider $h(X)X^{n(p+p^2+p^3)} \bmod (X^q - X)$. As noted, we need only determine the coefficient of the term of degree $q-1$ in $h(X)X^{n(p+p^2+p^3)}$. In the expansion of

$$h(X)X^{np}X^{np^2}X^{np^3},$$

by combining (5) and (6), we arrive at the equations

$$\begin{aligned} p-1 &= \alpha_0 + a_3 + a_2 + a_1 \\ &= \alpha_1 + a_0 + a_3 + a_2 \\ &= \alpha_2 + a_1 + a_0 + a_3 \\ &= \alpha_3 + a_2 + a_1 + a_0. \end{aligned}$$

Here $0 \le \alpha_i \le a_i$ for each i. However, there are no solutions to this system as $a_0 + a_2 = p > p-1$. So there is no term of degree $q-1$ in any of the polynomials in this case.

(iii) We consider $h(X)^{1+p^2}X^{n(p+p^3)} \bmod (X^q - X)$. Proceeding as in the previous case, we obtain the four equations

$$\begin{aligned} p-1 &= \alpha_0 + a_3 + \beta_2 + a_1 \\ &= \alpha_1 + a_0 + \beta_3 + a_2 \\ &= \alpha_2 + a_1 + \beta_0 + a_3 \\ &= \alpha_3 + a_2 + \beta_1 + a_0, \end{aligned}$$

with $0 \le \alpha_i, \beta_i \le a_i$ for each i. Here, we use $\{\alpha_i\}$ for the exponents in $h(X)$ and $\{\beta_i\}$ for the exponents in $h(X)^{p^2} \bmod (X^q - X)$. Again, as with the previous case we find no solution to this system because $a_0 + a_2 = p > p-1$. Hence we get no term of degree $q-1$ in any of the polynomials in this case.

(iv) We consider $h(X)^{1+p}X^{n(p^2+p^3)} \bmod (X^q - X)$. The four equations which result in this case are

$$\begin{aligned} p-1 &= \alpha_0 + \beta_3 + a_2 + a_1 \\ &= \alpha_1 + \beta_0 + a_3 + a_2 \\ &= \alpha_2 + \beta_1 + a_0 + a_3 \\ &= \alpha_3 + \beta_2 + a_1 + a_0, \end{aligned}$$

with $0 \le \alpha_i, \beta_i \le a_i$ for each i. There are two possible situations: either $a_1 = 0$ and $a_3 = 1$, or $a_1 = 1$ and $a_3 = 0$. The two situations yield symmetric arguments, and so we deal with the case where $a_1 = 0$ and $a_3 = 1$ only. It is immediate that $\alpha_1 = \beta_1 = 0$ and $0 \le \alpha_3, \beta_3 \le 1$. Using the fact $a_0 + a_2 = p$, the 4 equations reduce to

$$\begin{aligned} \alpha_0 &= a_0 - 1 - \beta_3 \\ \beta_0 &= a_0 - 2 \\ \alpha_2 &= a_2 - 2 \\ \beta_2 &= a_2 - 1 - \alpha_3. \end{aligned}$$

Thus, when $a_3 = 1$, the coefficient of X^{q-1} in $h(X)^{1+p}X^{n(p^2+p^3)} \bmod (X^q - X)$ is given by

$$\binom{a_0}{2}\binom{a_2}{2}\left(\sum_{\alpha_3=0}^{1}\sum_{\beta_3=0}^{1}\binom{a_0}{\beta_3+1}\binom{a_2}{\alpha_3+1}\right) = \left(\frac{a_0a_2(a_0+1)(a_2+1)}{4}\right)\binom{a_0}{2}\binom{a_2}{2}.$$

As mentioned, if $a_1 = 1$ and $a_3 = 0$, then we get a symmetric argument which yields the same coefficient. There are 4 polynomials in this case with the same coefficient for X^{q-1}, and so the sum total of this case's contribution to the coefficient of the X^{q-1} term in $g(X)$ is

$$a_0a_2(a_0+1)(a_2+1)\binom{a_0}{2}\binom{a_2}{2},$$

which is non-zero modulo p as $a_i < p-1$ by hypothesis.

(v) We consider $h(X)^{1+p+p^2}X^{np^3} \bmod (X^q - X)$. The four equations which result in this case are

$$\begin{aligned} p-1 &= \alpha_0 + \beta_3 + \gamma_2 + a_1 \\ &= \alpha_1 + \beta_0 + \gamma_3 + a_2 \\ &= \alpha_2 + \beta_1 + \gamma_0 + a_3 \\ &= \alpha_3 + \beta_2 + \gamma_1 + a_0, \end{aligned}$$

with $0 \le \alpha_i, \beta_i, \gamma_i \le a_i$ for each i. As with the previous case, we deal with the situation where $a_0 = 0$, $a_3 = 1$; the other case yielding a symmetric argument. Using $a_0 + a_2 = p$ where appropriate, the four equations now reduce to

$$\begin{aligned} \alpha_0 + \gamma_2 &= p - 1 - \beta_3 \\ \beta_0 &= a_0 - 1 - \gamma_3 \\ \alpha_2 + \gamma_0 &= p - 2 \\ \beta_2 &= a_2 - 1 - \alpha_3. \end{aligned}$$

Using our bounds on $\alpha_i, \beta_i\gamma_i$, we may reduce the first and third equations further:

$$\begin{aligned} a_0 - 1 - \beta_3 \le \alpha_0 &\le a_0 \\ a_2 - 2 \le \alpha_2 &\le a_2. \end{aligned}$$

Thus the resulting coefficient of X^{q-1} in this case, with $a_3 = 1$, is given by

$$\sum_{\alpha_3=0}^{1}\sum_{\beta_3=0}^{1}\sum_{\gamma_3=0}^{1}\sum_{\alpha_0=a_0-1-\beta_3}^{a_0}\sum_{\alpha_2=a_2-2}^{a_2}\binom{a_0}{\alpha_0}\binom{a_2}{\alpha_2}\binom{a_0}{\gamma_3+1}\binom{a_2}{\alpha_3+1}\binom{a_0}{p-2-\alpha_2}\binom{a_2}{p-1-\beta_3-\alpha_0}.$$

This summation may be rewritten as the product $S_1S_2S_3S_4$ where

$$\begin{aligned} S_1 &= \sum_{\beta_3=0}^{1}\sum_{\alpha_0=a_0-1-\beta_3}^{a_0}\binom{a_0}{\alpha_0}\binom{a_2}{p-1-\alpha_0-\beta_3}, \\ S_2 &= \sum_{\alpha_2=a_2-2}^{a_2}\binom{a_2}{\alpha_2}\binom{a_0}{p-2-\alpha_2}, \\ S_3 &= \sum_{\alpha_3=0}^{1}\binom{a_2}{\alpha_3+1}, \\ S_4 &= \sum_{\gamma_3=0}^{1}\binom{a_0}{\gamma_3+1}. \end{aligned}$$

Using $a_0 + a_2 = p$, one finds

$$\begin{aligned} S_1 &= \binom{a_0}{1}\binom{a_2}{a_2} + \binom{a_0}{a_0}\binom{a_2}{1} + \binom{a_0}{2}\binom{a_2}{a_2} + \binom{a_0}{1}\binom{a_2}{1} + \binom{a_0}{a_0}\binom{a_2}{2} \\ &= a_0 + a_2 + a_0a_2 + \frac{a_0^2 - a_0 + a_2^2 - a_2}{2} \\ &= p + \frac{(a_0+a_2)^2 - (a_0+a_2)}{2} \\ &= p + p\left(\frac{p-1}{2}\right) \\ &\equiv 0 \bmod p. \end{aligned}$$

Thus we get no term of degree $q-1$ from any of the polynomials in this case.

(vi) For $(X+1)^{n(1+p+p^2+p^3)}$, following in much the same way as the previous cases, we obtain the four equations

$$\begin{aligned} p-1 &= \alpha_0 + \beta_3 + \gamma_2 + \delta_1 \\ &= \alpha_1 + \beta_0 + \gamma_3 + \delta_2 \\ &= \alpha_2 + \beta_1 + \gamma_0 + \delta_3 \\ &= \alpha_3 + \beta_2 + \gamma_1 + \delta_0, \end{aligned}$$

with $0 \le \alpha_i, \beta_i, \gamma_i, \delta_i \le a_i$ for each i. Again we concentrate on the situation with $a_1 = 0$ and $a_3 = 1$, knowing a similar argument produces the same results for the alternate possibility. Our four equations simplify to

$$\begin{aligned} \alpha_0 + \gamma_2 &= p - 1 - \beta_3 \\ \beta_0 + \delta_2 &= p - 1 - \gamma_3 \\ \alpha_2 + \gamma_0 &= p - 1 - \delta_3 \\ \beta_2 + \delta_0 &= p - 1 - \alpha_3. \end{aligned}$$

In much the same way as the previous case, these equations force the following bounds:

$$\begin{aligned} a_0 - 1 - \beta_3 \le \alpha_0 \le a_0, \\ a_0 - 1 - \gamma_3 \le \beta_0 \le a_0, \\ a_2 - 1 - \delta_3 \le \alpha_2 \le a_2 \\ a_2 - 1 - \alpha_3 \le \beta_2 \le a_2. \end{aligned}$$

Thus the coefficient of X^{q-1} in this case, with $a_3 = 1$, is given by

$$\sum_{\alpha_3=0}^{1}\sum_{\beta_3=0}^{1}\sum_{\gamma_3=0}^{1}\sum_{\delta_3=0}^{1}\sum_{\alpha_0=a_0-1-\beta_3}^{a_0}\sum_{\beta_0=a_0-1-\gamma_3}^{a_0}\sum_{\alpha_2=a_2-1-\delta_3}^{a_2}\sum_{\beta_2=a_2-1-\alpha_3}^{a_2}\binom{a_0}{\alpha_0}\binom{a_2}{\alpha_2}\times$$
$$\binom{a_0}{\beta_0}\binom{a_2}{\beta_2}\binom{a_0}{p-1-\delta_3-\alpha_2}\binom{a_2}{p-1-\beta_3-\alpha_0}\binom{a_0}{p-1-\alpha_3-\beta_2}\binom{a_2}{p-1-\gamma_3-\beta_0}.$$

Rearranging this sum, we extract the factor

$$\sum_{\beta_3=0}^{1}\sum_{\alpha_0=a_0-1-\beta_3}^{a_0}\binom{a_0}{\alpha_0}\binom{a_2}{p-1-\beta_3-\alpha_0},$$

which is the same as S_1 from the previous case. Again we may conclude that we obtain no term of degree $q-1$ in this case.

We have completed our examination of the various cases. Only one of our cases yielded a non-zero coefficient for X^{q-1} in $g(X)$, and thus $g(X)$ has degree $q-1$. By Hermite's criteria we know $(X+1)^n - X^n$ is not a permutation polynomial over $\mathbb{F}_q$, and thus X^n is not planar over $\mathbb{F}_q$. □

It remains to resolve the case where the base p expansion of n contains a digit of size $p-1$.

Lemma 14. *Set $p \geq 5$ and $q = p^4$. Fix $n = (a_3 \cdots a_0)_p$ and suppose*

$$V = (a_0 + a_2, a_1 + a_3) = (p, 1).$$

If there exists an integer i, $0 \leq i < 4$ for which $a_i = p-1$, then X^n is not planar over $\mathbb{F}_q$.

Proof. Under the restrictions, there are only four possibilities for n:

$$n \in \{(1\,1\,0\,(p-1))_p, (0\,1\,1\,(p-1))_p, (1\,(p-1)\,0\,1)_p, (0\,(p-1)\,1\,1)_p\}.$$

Of these possibilities, the last is a cyclic shift of the 1st, while the 3rd is a cyclic shift of the 2nd. It follows from Lemma 8 that we need only resolve the two cases $n = (0\,1\,1\,(p-1))_p = p^2 + 2p - 1$ and $n = (1\,1\,0\,(p-1))_p = p^3 + p^2 + p - 1$. We deal with the two possibilities separately, but in similar ways.

Let $n = p^2 + 2p - 1$ and $f(X) = (X+1)^n - X^n$. We are interested in the coefficient C of X^{q-1} in $g(X) = f(X)^{p^2-1} \bmod (X^q - X)$ – in fact, we wish to show $C \neq 0$. Since $p^4 < \mathrm{Deg}(f^{p^2-1}) < 2(p^4-1)$, the X^{q-1} term in $g(X)$ is actually the X^{q-1} term in f^{p^2-1}. First we verify by a direct computation that for $p = 5$, $C \equiv 1 \bmod 5$, and for $p = 7$, $C \equiv 3 \bmod 7$. In what follows we assume that $p \geq 11$.

We have

$$\begin{aligned}
f(X)^{p^2-1} &= [(X+1)^n - X^n]^{p^2-1} \\
&= \sum_{i=0}^{p^2-1} (-1)^i \binom{p^2-1}{i} (X+1)^{n(p^2-1-i)} X^{in} \\
&= \sum_{i=0}^{p^2-1} (-1)^i \binom{p^2-1}{i} \sum_{j=0}^{n(p^2-1-i)} \binom{n(p^2-1-i)}{j} X^{n(p^2-1-i)-j} X^{in} \\
&= \sum_{i=0}^{p^2-1} (-1)^i \binom{p^2-1}{i} \sum_{j=0}^{n(p^2-1-i)} \binom{n(p^2-1-i)}{j} X^{n(p^2-1)-j}. \qquad (7)
\end{aligned}$$

In order to find the coefficient C from (7), we set $n(p^2-1) - j = q - 1 = p^4 - 1$, which gives $j = j_0 = n(p^2-1) - (p^4-1)$. The range of the index i can be found by solving the inequality $n(p^2-1-i) \geq n(p^2-1) - (p^4-1)$, which results in $0 \leq i \leq p^2 - 2p + 3$. Therefore

$$C = \sum_{i=0}^{p^2-2p+3} (-1)^i \binom{p^2-1}{i} \binom{N_i}{j_0},$$

where from now on $N_i = n(p^2-1-i)$. For ease of notation, we set $C_i = \binom{N_i}{j_0}$.

As $\binom{p^2-1}{i} + \binom{p^2-1}{i-1} = \binom{p^2}{i} \equiv 0 \bmod p$ for all $1 \leq i < p^2$, and $\binom{p^2-1}{0} = 1$, we obtain $\binom{p^2-1}{i} \equiv (-1)^i \bmod p$. This implies

$$C \equiv \sum_{i=0}^{p^2-2p+3} C_i \bmod p.$$

We note

$$j_0 = (p^2 + 2p - 1)(p^2 - 1) - (p^4 - 1) = (1\ (p-3)\ (p-2)\ 2)_p.$$

As $0 \le i \le p^2-2p+3 = ((p-2)\ 3)_p$, we can write i in the form $i = (b\ a)_p = a+bp$, where $0 \le a \le 3$ for $b = p-2$, and $0 \le a \le p-1$ for $0 \le b \le p-3$. Simplifying the notation $N_i = N_{(b\ a)_p}$ to just $N_{(a,b)}$, we obtain

$$\begin{aligned} N_i = N_{(a,b)} &= (1+a) + (-2-2a+b)p + (-2-a-2b)p^2 + (p+2-b)p^3 \\ &= (1+a) + (-2-2a+b)p + (p-2-a-2b)p^2 + (p+1-b)p^3. \end{aligned} \tag{8}$$

Let $x[k]$ denote the p-digit of a nonnegative integer x at p^k, $k \ge 0$. Since $j_0 = (1\ (p-3)\ (p-2)\ 2)_p$, applying Lemma 3 yields

$$C_i = \binom{N_i}{j_0} \equiv \binom{N_i[0]}{2}\binom{N_i[1]}{p-2}\binom{N_i[2]}{p-3}\binom{N_i[3]}{1} \bmod p.$$

Note that $C_i \not\equiv 0 \bmod p$ if and only if the following four conditions are met:

$$\left\{ \begin{array}{rcl} 2 & \le N_i[0] \le & p-1 \\ p-2 & \le N_i[1] \le & p-1 \\ p-3 & \le N_i[2] \le & p-1 \\ 1 & \le N_i[3] \le & p-1 \end{array} \right\}. \tag{9}$$

We also have

$$C \equiv \sum_{i=0}^{p^2-2p+3} C_i \bmod p \equiv \sum_{C_i \not\equiv 0 \bmod p} C_i \bmod p.$$

We now show that $C_i \equiv 0 \bmod p$ for all but very few values of $i = a+bp$.

Claim 1. *Let $0 \le i = a+bp \le p^2-2p+3$. Then*

$$C_i \not\equiv 0 \bmod p \quad \left\{ \begin{array}{l} \textit{for precisely six values of } i \textit{ if } p \equiv 1,2 \bmod 5, \textit{ and} \\ \textit{for precisely four values of } i \textit{ if } p \equiv 3,4 \bmod 5. \end{array} \right.$$

Proof of Claim 1. If $a = 0$ or $a = p-1$, then $N_i[0] < j_0[0]$ and so $C_i \equiv 0 \bmod p$. For $(a,b) = (a, p-2)$ with $a = 1,2,3$, direct substitution into N_i gives the following base p expansions for N_i:

$$\begin{aligned} N_{(1,p-2)} &= (2\ 1\ (p-6)\ 2)_p \\ N_{(2,p-2)} &= (2\ 0\ (p-8)\ 3)_p \\ N_{(3,p-2)} &= (1\ (p-1)\ (p-10)\ 4)_p. \end{aligned}$$

We see that in all these cases $N_i[1]$ does not satisfy the inequality in (9). Hence, for these i, $C_i \equiv 0 \bmod p$ also.

We now take a closer look at the base p expansions of N_i, assuming $1 \le a \le p-2$ and $0 \le b \le p-3$. These inequalities imply that $-2p+2 \le -2-2a+b \le p-7$ and $-2p+6 \le p-2-a-2b \le p-3$. Then (8) and (9) give that $N_i[0] = 1+a$ and

$$N_i[1] = -2-2a+b \equiv -1, -2 \bmod p.$$

This implies $b \equiv 2a, 2a+1 \bmod p$, or, more precisely,

$$b = \begin{cases} 2a \text{ or } 2a+1 & \text{if } 1 \le a < p/2; \\ 2a-p \text{ or } 2a+1-p & \text{if } p/2 < a \le p-2. \end{cases}$$

Substituting corresponding values of a and b in (8), we obtain the following expressions for N_i:

$$\begin{cases} (1+a) + (-2)p + (p-2-5a)p^2 + (p+1-2a)p^3 & \text{if } 1 \le a < p/2; \\ (1+a) + (-1)p + (p-4-5a)p^2 + (p-2a)p^3 & \text{if } 1 \le a < p/2; \\ (1+a) + (p-2)p + (3p-4-5a)p^2 + (2p+1-2a)p^3 & \text{if } p/2 < a \le p-2; \\ (1+a) + (p-1)p + (3p-6-5a)p^2 + (2p-2a)p^3 & \text{if } p/2 < a \le p-2. \end{cases}$$

Now we rewrite these expressions in a way which exhibits the p-digits of the number by the usual "borrowing" of digits from the greater powers of p. The exact form of the result depends on the congruence class of p modulo 5. For example, for $p = 5k + 1$, we obtain the following expressions, where $N_i[0]$ and $N_i[3]$ are given in terms of k, and $N_i[1]$ and $N_i[2]$ in terms of p. Each case represents at most two possibilities, as $1 \le a < p/2$ gives $a = k, 2k$, and $p/2 < a \le p - 2$ gives $a = 3k, 4k$. We list only those cases where the p-digits satisfy the inequalities (9).

$$\begin{cases} (k+1) + (p-2)p + (p-2)p^2 + (3k+1)p^3 & \text{if } a = k,\ b = 2k; \\ (2k+1) + (p-2)p + (p-1)p^2 + kp^3 & \text{if } a = 2k,\ b = 4k; \\ (2k+1) + (p-1)p + (p-3)p^2 + (k-1)p^3 & \text{if } a = 2k,\ b = 4k+1; \\ (3k+1) + (p-2)p + (p-1)p^2 + (4k+2)p^3 & \text{if } a = 3k,\ b = k-1; \\ (3k+1) + (p-1)p + (p-3)p^2 + (4k+1)p^3 & \text{if } a = 3k,\ b = k; \\ (4k+1) + (p-1)p + (p-2)p^2 + 2kp^3 & \text{if } a = 4k,\ b = 3k. \end{cases} \tag{10}$$

In order to find all pairs (a, b), which satisfy these conditions and $1 \le a \le p - 2$ and $0 \le b \le p - 3$, we consider separately each nonzero congruence class p modulo 5: $p = 5k + r$, $1 \le r \le 4$. Within each such class, the problem becomes trivial. Case $r = 1$ was considered above in (10). Proceeding this way, and arranging all possible values of (a, b) in increasing order of $i = a + bp$, we obtain the following pairs (a, b) for which $C_i \not\equiv 0 \bmod p$:

$$\begin{cases} r = 1: & (a,b) = (3k, k-1),\ (3k, k),\ (k, 2k),\ (4k, 3k),\ (2k, 4k),\ (2k, 4k+1); \\ r = 2: & (a,b) = (3k+1, k),\ (k, 2k),\ (k, 2k+1),\ (4k+1, 3k),\ (4k+1, 3k+1), \\ & \qquad (2k, 4k+1); \\ r = 3: & (a,b) = (3k+1, k),\ (k, 2k+1),\ (4k+2, 3k+1),\ (2k+1, 4k+2); \\ r = 4: & (a,b) = (3k+2, k),\ (k, 2k+1),\ (4k+3, 3k+2),\ (2k+1, 4k+3). \end{cases} \tag{11}$$

Claim 1 is established. □

Observe that for each choice of r in (11), the pairs (a, b) and $(p - 1 - a, p - 1 - b)$ are distinct and appear simultaneously. They correspond to the numbers i and $p^2 - 1 - i$. It is easy to check that for any (a, b) from (11), $C_{(a,b)} \equiv C_{(p-1-a,p-1-b)} \bmod p$. For example, for $r = 1$, $(a, b) = (3k, k - 1)$ and $(a, b) = (2k, 4k + 1)$, the p-digits can be taken from the fourth and the third line of (10), and we obtain

$$\begin{aligned} C_{(3k,k-1)} &\equiv \binom{3k+1}{2}\binom{p-2}{p-2}\binom{p-1}{p-3}\binom{4k+2}{1} \bmod p \\ &\equiv \left(\frac{(3k+1)(3k)}{2}\right)(1)\left(\frac{(-1)(-2)}{2}\right)(4k+2) \bmod p \\ &\equiv \left(\frac{(p-2k)(p-2k-1)}{2}\right)(p-(k-1)) \bmod p \\ &\equiv \binom{2k+1}{2}\binom{p-1}{p-2}\binom{p-3}{p-3}\binom{k-1}{1} \bmod p \\ &\equiv C_{(2k,4k+1)} \bmod p. \end{aligned}$$

A similar verification can be done in all cases.[1] The values of p, a, b, the corresponding p-digits of $C_i \not\equiv 0 \bmod p$, and the simplified form of $C_i \bmod p$ are collected in Table 1. Due to the symmetry $C_{(a,b)} \equiv C_{(p-1-a,p-1-b)} \bmod p$, we exhibit data for $i \le (p^2 - 2p + 3)/2$ only.

[1] Here we decided against presenting a general argument, since the number of cases to verify is small, and each case is trivial.

p	a	b	$C_i[0]$	$C_i[1]$	$C_i[2]$	$C_i[3]$	$C_i = C_{(a,b)} \not\equiv 0 \bmod p$
$5k+1$	$3k$	$k-1$	$3k+1$	$p-2$	$p-1$	$4k+2$	$\binom{3k+1}{2}(4k+2)$
	$3k$	k	$3k+1$	$p-1$	$p-3$	$4k+1$	$-\binom{3k+1}{2}(4k+1)$
	k	$2k$	$k+1$	$p-2$	$p-2$	$3k+1$	$-2\binom{k+1}{2}(3k+1)$
$5k+2$	$3k+1$	k	$3k+2$	$p-2$	$p-3$	$4k+2$	$\binom{3k+2}{2}(4k+2)$
	k	$2k$	$k+1$	$p-2$	$p-1$	$3k+2$	$\binom{k+1}{2}(3k+2)$
	k	$2k+1$	$k+1$	$p-1$	$p-3$	$3k+1$	$-\binom{k+1}{2}(3k+1)$
$5k+3$	$3k+1$	k	$3k+2$	$p-1$	$p-2$	$4k+3$	$2\binom{3k+2}{2}(4k+3)$
	k	$2k+1$	$k+1$	$p-1$	$p-2$	$3k+2$	$2\binom{k+1}{2}(3k+2)$
$5k+4$	$3k+2$	k	$3k+3$	$p-2$	$p-2$	$4k+4$	$-2\binom{3k+3}{2}(4k+4)$
	k	$2k+1$	$k+1$	$p-1$	$p-1$	$3k+3$	$-\binom{k+1}{2}(3k+3)$

Table 1.

We may now readily check that for each of the four congruency classes of p,

$$C \equiv \sum_{C_i \not\equiv 0 \bmod p} C_i \bmod p \not\equiv 0 \bmod p.$$

For $p = 5k+1$, we have

$$\begin{aligned} C &\equiv 2\left[\binom{3k+1}{2}(4k+2) - \binom{3k+1}{2}(4k+1) - 2\binom{k+1}{2}(3k+1)\right] \bmod p \\ &\equiv -k(2k-1)(3k+1) \bmod p \\ &\not\equiv 0 \bmod p. \end{aligned}$$

For $p = 5k+3$, we have

$$\begin{aligned} C &\equiv 2\left[2\binom{3k+2}{2}(4k+3) + 2\binom{k+1}{2}(3k+2)\right] \bmod p \\ &\equiv 2(3k+2)\left[(3k+1)(4k+3) + (k+1)k\right] \bmod p \\ &\equiv 2(3k+2)\left[(3k+1)(-k) + (k+1)k\right] \bmod p \\ &\equiv -4k^2(3k+2) \bmod p \\ &\not\equiv 0 \bmod p. \end{aligned}$$

The remaining cases $p = 5k+2$ and $p = 5k+4$ are handled similarly. In each case, it follows from Lemma 2 that $f(X)$ is not a permutation polynomial over $\mathbb{F}_{p^4}$, and so X^n is not planar over $\mathbb{F}_{p^4}$. This ends our proof for $n = p^2 + 2p - 1$.

Now we consider the case where $n = p^3 + p^2 + p - 1$. As in the first case, we will show that the coefficient C of X^{q-1} in $f(X)^{p^2-1} \bmod (X^q - X)$ is not zero. The same computations as in (7), but this time with $n = p^3 + p^2 + p - 1$, yield

$$f(X) = \sum_{i=0}^{p^2-1} \sum_{j=0}^{n(p^2-1-i)} \binom{n(p^2-1-i)}{j} X^{n(p^2-1)-j},$$

where we have again used $\binom{p^2-1}{i} \equiv (-1)^i \bmod p$. For a positive integer m, $X^m \equiv X^{q-1} \bmod (X^q - X)$ if and only if $m = t(q-1)$ for some positive integer t. In order to find C, we set $n(p^2-1) - j = t(q-1)$, which gives

$$j = j_t = n(p^2-1) - t(q-1).$$

The ranges of i and t can be found by solving the inequalities $n(p^2-1-i) \geq n(p^2-1)-t(q-1) \geq 0$, which results in $1 \leq t \leq p$ and $0 \leq i \leq t(q-1)/n \leq \lfloor p(q-1)/n \rfloor = p^2-p$. Let C_t denote the coefficient of $X^{t(q-1)}$ in $f(X)^{p^2-1}$. Then

$$C = \sum_{t=1}^{p} C_t.$$

As $\binom{a}{b} = 0$ for $0 \leq a < b$, we ignore the upper bound $t(q-1)/n$ on i, and obtain

$$C_t \equiv \sum_{i=0}^{p^2-1} \binom{N_i}{j_t} \bmod p,$$

where again $N_i = n(p^2-1-i)$.

Claim 2. *Let $0 \leq i \leq p^2-1$. The following statements hold.*

(i) If $i \neq (p-1)k$ or $1 \leq t \leq p-2$, then

$$\binom{N_i}{j_t} \equiv 0 \bmod p.$$

(ii) If $i = (p-1)k$ and $0 \leq k \leq \frac{p+1}{2}$, then

$$\binom{N_i}{j_{p-1}} \equiv p-k \bmod p \quad \textit{and} \quad \binom{N_i}{j_p} \equiv p-k+1 \bmod p.$$

(iii) If $i = (p-1)k$ and $\frac{p+1}{2} < k \leq p$, then

$$\binom{N_i}{j_{p-1}} \equiv k \bmod p \quad \textit{and} \quad \binom{N_i}{j_p} \equiv k-1 \bmod p.$$

Proof of Claim 2. Let $i = (b\ a)_p = a+bp$, $0 \leq a, b \leq p-1$. We again adopt the notation $N_{(a,b)}$ for N_i. Then

$$N_{(a,b)} = (1+a) + (-1-a+b)p + (p-2-(a+b))p^2 + (p-1-(a+b))p^3 + (p-b)p^4. \tag{12}$$

We proceed by partitioning all values of N_i and j_t into several classes, defined by their p-digits, and then applying Lemma 3 in order to determine $\binom{N_i}{j_t} \bmod p$. Rewriting

$$j_t = n(p^2-1) - t(q-1) = (p+1-t)p^4 - 2p^2 - p + (1+t)$$

in base p we get

$$j_t = \begin{cases} ((p-t)\ (p-1)\ (p-3)\ (p-1)\ (1+t))_p & \text{if } 1 \leq t \leq p-2; \\ (1\ (p-1)\ (p-2)\ 0\ 0)_p & \text{if } t = p-1; \\ ((p-1)\ (p-2)\ 0\ 1)_p & \text{if } t = p. \end{cases}$$

For $a = 0$, substituting into (12) we obtain

$$\begin{aligned} N_{(0,b)} &= ((p-b)\ (p-1-b)\ (p-2-b)\ (b-1)\ 1)_p \quad \text{for } 1 \leq b \leq p-2, \\ N_{(0,0)} &= (1\ 0\ (p-1)\ (p-3)\ (p-1)\ 1)_p, \\ N_{(0,p-1)} &= ((p-1)\ (p-1)\ (p-2)\ 1)_p. \end{aligned}$$

As $j_t[0] = 1+t > 1$ for $1 \le t \le p-2$, $j_{p-1}[2] = j_p[2] = p-2$, and $j_{p-1}[4] = 1$, then $\binom{N_{(0,b)}}{j_t} \equiv 0 \bmod p$ for all $(b,t) \neq (p-1,p)$. Since

$$\begin{aligned}\binom{N_{(0,p-1)}}{j_p} &\equiv \binom{1}{1}\binom{p-2}{0}\binom{p-1}{p-2}\binom{p-1}{p-1} \bmod p \\ &\equiv p-1 \bmod p,\end{aligned}$$

the claim is proved for $a = 0$.

If $a = p-1$, then $N_{(p-1,p-1)} = 0$, while for $0 \le b \le p-2$,

$$N_{(p-1,b)} = ((p-1-b)\ (p-1-b)\ (p-2-b)\ (1+b)\ 0)_p.$$

As $j_t[0] \ge 1$ for $t \neq p-1$, and

$$\begin{aligned}\binom{N_{(p-1,0)}}{j_{p-1}} &\equiv \binom{0}{0}\binom{1}{0}\binom{p-2}{p-2}\binom{p-1}{p-1}\binom{p-1}{1} \bmod p \\ &\equiv p-1 \bmod p,\end{aligned}$$

the claim is proved for $a = p-1$ also.

Therefore, in what follows, we may assume $1 \le a \le p-2$. This implies that $1 \le a+b \le 2p-3$. We first note that when $a+b \neq p-1$, it follows from (12) that

$$N_i[3] = \begin{cases} p-1-(a+b) & \text{when } 1 \le a+b \le p-3, \\ 0 \text{ or } 1 & \text{when } a+b = p-2, \\ 2p-2-(a+b) & \text{when } p \le a+b \le 2p-3. \end{cases}$$

In each of these cases, $j_t[3] = p-1 > N_i[3]$ for all t, and so $\binom{N_i}{j_t} \equiv 0 \bmod p$ as claimed.

The only case which we have not yet considered is $1 \le a \le p-2$ and $a+b = p-1$. Let $k = p-a$. Then $i = a+bp = p-k+(k-1)p = (p-1)k$, where $2 \le k \le p-1$. Now

$$\begin{aligned}N_i = N_{(p-1)k} &= (p-k+1)p^4 + (-2)p^2 + (2k-1)p^2 + (1-k) \\ &= (p-k)p^4 + (p-1)p^3 + (p-2)p^2 + (2k-2)p + (p+1-k).\end{aligned}$$

and writing $N_{(p-1)k}$ in base p we obtain

$$N_{(p-1)k} = \begin{cases} ((p-k)\ (p-1)\ (p-2)\ (2k-2)\ (p+1-k))_p & \text{if } 2 \le k \le \frac{p+1}{2}; \\ ((p-k)\ (p-1)\ (p-1)\ (2k-2-p)\ (p+1-k))_p & \text{if } \frac{p+1}{2} < k \le p. \end{cases}$$

Let $1 \le t \le p-2$. For $\binom{N_{(p-1)k}}{j_t} \not\equiv 0 \bmod p$, we must have $N_{(p-1)k}[0] = p+1-k \ge 1+t = j_t[0]$, and $N_{(p-1)k}[4] = p-k \ge p-t = j_t[4]$. These conditions give $p-k \ge t \ge k$, and so $k \le (p-1)/2$. This implies $N_{(p-1)k}[1] = 2k-2 < p-1 = j_t[1]$, and so $\binom{N_{(p-1)k}}{j_t} \equiv 0 \bmod p$ for all $1 \le t \le p-2$.

It remains to consider the cases $t = p-1, p$. For $2 \le k \le (p+1)/2$, we obtain

$$\begin{aligned}\binom{N_{(p-1)k}}{j_{p-1}} &\equiv \binom{p+1-k}{0}\binom{2k-2}{0}\binom{p-2}{p-2}\binom{p-1}{p-1}\binom{p-k}{1} \bmod p \\ &\equiv p-k \bmod p, \\ \binom{N_{(p-1)k}}{j_p} &\equiv \binom{p+1-k}{1}\binom{2k-2}{0}\binom{p-2}{p-2}\binom{p-1}{p-1}\binom{p-k}{0} \bmod p \\ &\equiv p+1-k \bmod p,\end{aligned}$$

while for $(p+1)/2 < k \leq p$, we find

$$\begin{aligned}\binom{N_{(p-1)k}}{j_{p-1}} &\equiv \binom{p+1-k}{0}\binom{2k-2-p}{0}\binom{p-1}{p-2}\binom{p-1}{p-1}\binom{p-k}{1} \bmod p \\ &\equiv k \bmod p, \\ \binom{N_{(p-1)k}}{j_p} &\equiv \binom{p+1-k}{1}\binom{2k-2-p}{0}\binom{p-1}{p-2}\binom{p-1}{p-1}\binom{p-k}{0} \bmod p \\ &\equiv k-1 \bmod p,\end{aligned}$$

as claimed. This ends the proof of Claim 2. □

We are ready to finish our proof for $n = p^3 + p^2 + p - 1$ by showing that $C \not\equiv 0 \bmod p$. By Claim 2,

$$\begin{aligned}C = \sum_{t=1}^{p} C_t &\equiv C_{p-1} + C_p \bmod p \\ &\equiv \sum_{i=0}^{p^2-1} \binom{N_i}{j_{p-1}} + \sum_{i=0}^{p^2-1} \binom{N_i}{j_p} \bmod p \\ &\equiv 4 \sum_{k=2}^{(p+1)/2} (p-k+1) - 1 \bmod p \\ &\equiv 4\left(\frac{p-1+(p+1)/2}{2}\right)\left(\frac{p-1}{2}\right) - 1 \bmod p \\ &\equiv \frac{3p^2-1}{2} \bmod p \\ &\not\equiv 0 \bmod p.\end{aligned}$$

Hence, by Lemma 2, $f(X)$ is not a permutation polynomial and X^n is not planar over $\mathbb{F}_{p^4}$. □

References

[1] R.S. Coulter. The classification of planar monomials over fields of prime square order. *Proc. Amer. Math. Soc.*, 134:3373–3378, 2006.

[2] R.S. Coulter and R.W. Matthews. Planar functions and planes of Lenz-Barlotti class II. *Des. Codes Cryptogr.*, 10:167–184, 1997.

[3] P. Dembowski and T.G. Ostrom. Planes of order n with collineation groups of order n^2. *Math. Z.*, 103:239–258, 1968.

[4] 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. of Math.*, 11:65–120, 161–183, 1897.

[5] D. Gluck. Affine planes and permutation polynomials. In *Coding Theory and Design Theory, part II (Design Theory)*, volume 21 of *The IMA Volumes in Mathematics and its Applications*, pages 99–100. Springer-Verlag, 1990.

[6] C. Hermite. Sur les fonctions de sept lettres. *C.R. Acad. Sci. Paris*, 57:750–757, 1863.

[7] Y. Hiramine. A conjecture on affine planes of prime order. *J. Combin. Theory Ser. A*, 52:44–50, 1989.

[8] N.L. Johnson. Projective planes of order p that admit collineation groups of order p^2. *J. Geometry*, 30:49–68, 1987.

[9] E. Lucas. Théorie des fonctions numériques simplement périodiques. *Amer. J. Math*, 1:184–240, 289–321, 1878.

[10] L. Rónyai and T. Szőnyi. Planar functions over finite fields. *Combinatorica*, 9:315–320, 1989.