PLANAR FUNCTIONS AND PERFECT NONLINEAR MONOMIALS OVER FINITE FIELDS

MICHAEL E. ZIEVE

ABSTRACT. The study of finite projective planes involves planar functions, namely, functions $f\colon \mathbb{F}_q \to \mathbb{F}_q$ such that, for each $a \in \mathbb{F}_q^*$, the function $c \mapsto f(c+a) - f(c)$ is a bijection on $\mathbb{F}_q$. Planar functions are also used in the construction of DES-like cryptosystems, where they are called perfect nonlinear functions. We determine all planar functions on $\mathbb{F}_q$ of the form $c \mapsto c^t$, under the assumption that $q \geq (t-1)^4$. This resolves two conjectures of Hernando, McGuire and Monserrat. Our arguments also yield a new proof of a conjecture of Segre and Bartocci about monomial hyperovals in finite Desarguesian projective planes.

1. INTRODUCTION

Let $q = p^r$ where p is prime and r is a positive integer. A *planar function* is a function $f\colon \mathbb{F}_q \to \mathbb{F}_q$ such that, for every $a \in \mathbb{F}_q^*$, the function $c \mapsto f(c+a)-f(c)$ is a bijection on $\mathbb{F}_q$. Planar functions can be used to construct finite projective planes, and they have been studied by finite geometers since 1968 [6]. They arose more recently in the cryptography literature where they are called *perfect nonlinear functions* [22], the idea being that these functions are optimally resistant to linear and differential cryptanalysis when used in DES-like cryptosystems. Many authors have investigated the planarity of monomial functions $f(x) = x^t$ with $t > 0$. Since x^t is planar on $\mathbb{F}_q$ if and only if x^{t+q-1} is planar, and likewise if and only if x^{tp} is planar, the study of planar monomials reduces at once to the case that $t < q$ and $p \nmid t$.

The only known examples of planar monomials x^t over $\mathbb{F}_{p^r}$ with $p \nmid t$ and $t < p^r$ are

(1.1) $t = p^i + 1$ if $0 \leq i < r$ and $p^{\frac{r}{\gcd(i,r)}}$ is odd; and

(1.2) $t = \frac{3^i+1}{2}$ if $p = 3$ and $2 < i < r$ and $\gcd(i, 2r) = 1$.

A folk conjecture in the subject asserts that there are no further examples. This is known to be true for $r = 1$ [14], $r = 2$ [4], and $r = 4$ [5]. However, as noted in [5, 3], the methods used in these papers will likely not extend to much larger values of r. In this paper we prove this conjecture for all large r:

2010 *Mathematics Subject Classification.* 51E20, 11T06, 11T71, 05B05.

The author thanks Elodie Leducq and the referees for helpful remarks, and also thanks Gary McGuire and Peter Mueller for their interest. The author was partially supported by NSF grant DMS-1162181.

Theorem 1.4. *If $c \mapsto c^t$ is a planar function on $\mathbb{F}_{p^r}$, where $p^r \geq (t-1)^4$ and $p \nmid t$, then either (1.1) or (1.2) holds.*

Note that each of the known planar monomials over $\mathbb{F}_q$ has the property that it is also planar over $\mathbb{F}_{q^k}$ for infinitely many integers k. One consequence of our result is that no other planar monomials have this property:

Corollary 1.5. *For any prime p and any positive integer t, the function $c \mapsto c^t$ is a planar function on $\mathbb{F}_{p^k}$ for infinitely many k if and only if either*

- *$t = p^i + p^j$ where p is odd and $i \geq j \geq 0$; or*
- *$t = \frac{3^i+3^j}{2}$ where $p = 3$ and $i > j \geq 0$ with $i \not\equiv j \pmod 2$.*

This corollary resolves two conjectures of Hernando, McGuire and Monserrat [13, Conjectures PN2 and PN3]. It is the first known characterization of the known planar monomials among all planar monomials.

Corollary 1.5 was proved in the case $t \equiv 1 \pmod p$ by Leducq [16]. Thus, the bulk of our effort addresses the case $t \not\equiv 1 \pmod p$. In this case, Corollary 1.5 was proved in [13] if t and p satisfy any of eight different conditions. We show that none of these extra conditions are needed. Our approach is completely different from that of [16] and [13]. Whereas those papers rely on dozens of pages of computations involving the singularities of an associated (possibly singular and reducible) plane curve, we focus on the functional decomposition of a certain univariate polynomial. In particular, our most novel contribution is a method for testing whether a polynomial can be written as a function of a Dickson polynomial.

After reviewing some background material in the next section, we prove Theorem 1.4 and Corollary 1.5 in Sections 3 and 4, respectively. Then in Section 5 we show that our techniques yield a simple proof of the Segre–Bartocci conjecture about hyperovals in Desarguesian projective planes, and in Section 6 we discuss how generally our techniques will apply to related problems.

2. Background results

In this section we present the known results about exceptional polynomials, Dickson polynomials, and functional decomposition which will be used in our proofs. We begin with some definitions.

Definition 2.1. A polynomial $F(x) \in \mathbb{F}_q[x]$ is *linear* if it has degree one.

Remark. What we call linear polynomials are sometimes called affine polynomials.

Definition 2.2. A polynomial $F(x) \in \mathbb{F}_q[x]$ of degree at least 2 is *indecomposable* if there do not exist nonlinear $G, H \in \mathbb{F}_q[x]$ such that $F(x) = G(H(x))$.

Definition 2.3. A polynomial $F(x) \in \mathbb{F}_q[x]$ is *exceptional* if there are infinitely many k for which the function $c \mapsto F(c)$ is a bijection on $\mathbb{F}_{q^k}$.

Plainly every polynomial in $\mathbb{F}_q[x]$ of degree at least 2 can be written as the composition of indecomposable polynomials in $\mathbb{F}_q[x]$. Moreover, for $G, H \in \mathbb{F}_q[x]$, if $G(H(x))$ is exceptional then both G and H are exceptional (in fact the converse holds as well [25], but it will not be used in this paper). Thus, every nonlinear exceptional polynomial is the composition of indecomposable exceptional polynomials. Much difficult mathematics has been used in the study of indecomposable exceptional polynomials (see e.g. [9, 11, 25]), and much remains to be done. However, we will not need any deep results about exceptional polynomials. Instead we will only rely on the following two known results.

Proposition 2.4. *If $F(x) \in \mathbb{F}_q[x]$ has degree at most $q^{1/4}$, and the function $c \mapsto F(c)$ induces a bijection on $\mathbb{F}_q$, then F is exceptional.*

Proposition 2.5. *If $F(x) \in \mathbb{F}_q[x]$ is an indecomposable exceptional polynomial of degree coprime to q, then there are linear $\mu, \nu \in \mathbb{F}_q[x]$ such that $\mu \circ F \circ \nu$ is one of the following polynomials:*

- *x^m for some prime m which is coprime to $q-1$, or*
- *$D_n(x, a)$ for some $a \in \mathbb{F}_q^*$ and some prime n which is coprime to $q^2 - 1$.*

In this result, $D_n(x, a)$ denotes the degree-n Dickson polynomial of the first kind with parameter a. This is a polynomial in $\mathbb{F}_q[x]$ which satisfies the functional equation

$$D_n(x + \frac{a}{x}, a) = x^n + \left(\frac{a}{x}\right)^n.$$

These polynomials are closely related to the Chebyshev polynomials of the first kind. Here we note only that, in light of the above functional equation, $D_n(x, a)$ has degree n and satisfies $D_n(-x, a) = (-1)^n D_n(x, a)$. Thus, if n is odd then $D_n(x, a)$ is an odd polynomial, in the sense that all of its terms have odd degree. For more information about Dickson polynomials, see [1, 17].

Remark. Proposition 2.4 follows easily from Weil's bound on the number of rational points on a curve over a finite field, combined with a quick argument using either Galois theory [10] or the fundamental theorem of symmetric polynomials [24]. See [25, Rem. 8.4.20] for the history of this result. Proposition 2.5 is a slight variant of a result from [15]; see [20] for a proof in the stated form. The proof of this result only depends on Weil's bound, group-theoretic results due to Burnside and Schur, and a quick and easy genus computation. Weil's bound follows from the Riemann-Roch theorem, and the two group-theoretic results are proved in a few pages in [17, 21]. So, although deep tools have been used in the study of exceptional polynomials, Propositions 2.4 and 2.5 do not depend on such tools.

The next result is well-known, but we include a proof for the reader's convenience.

Lemma 2.6. *For $G, H \in \mathbb{F}_q[x]$, if $G \circ H$ is an odd polynomial and $\deg(G)$ is coprime to q then $H(x) - H(0)$ is odd.*

Proof. Suppose otherwise. Let ax^α and bx^β be the leading terms of G and H, respectively, and let cx^γ be the highest-degree term of H having even degree. Then α and β are odd, and γ is both even and positive. Writing $\delta := (\alpha-1)\beta + \gamma$, and noting that δ is even, it follows that the coefficient of x^δ in $G \circ H$ is $a\alpha b^{\alpha-1}c$. Since this is nonzero, $G \circ H$ has a term of even degree, which contradicts our hypothesis. □

Remark. The above lemma has been rediscovered many times. It is not true without the hypothesis on $\deg(G)$; one counterexample from [2] is $G = (x+1)^s(x-1)^{q-s}$ and $H = x^q + (x+1)^{q-s}(x-1)^s$ with q odd and $0 < s < q$.

Lemma 2.7. *Let $\mu, \nu \in \mathbb{F}_q[x]$ be linear, and let $G \in \mathbb{F}_q[x]$ have degree larger than 1 and coprime to q. If both G and $\mu \circ G \circ \nu$ are odd, then $\nu(0) = 0$.*

Proof. Write $\nu(x) = cx + d$, and let ax and bx^β be the leading terms of μ and G. Then the coefficient of $x^{\beta-1}$ in $\mu \circ G \circ \nu$ is $ab\beta c^{\beta-1}d$. But this coefficient is zero by hypothesis, so $d = 0$. □

One of the nice features of the polynomials $f(x) = x^t$ is the following well-known criterion for planarity of $c \mapsto f(c)$, which we will often use without explicit mention.

Lemma 2.8. *For any positive integer t, the function $c \mapsto c^t$ is planar on $\mathbb{F}_q$ if and only if the function $c \mapsto (c+1)^t - c^t$ is bijective on $\mathbb{F}_q$.*

Proof. Planarity asserts that $c \mapsto (c+a)^t - c^t$ is bijective for each $a \in \mathbb{F}_q^*$; composing on the right with $c \mapsto ac$ and on the left with $c \mapsto c/a^t$ yields the stated criterion. □

Finally, we recall Lucas's theorem about binomial coefficients mod p (see e.g. [19, 8]):

Lemma 2.9. *Let p be prime and let m and n be positive integers. Write $m = m_0 + m_1 p + m_2 p^2 + \cdots + m_s p^s$ and $n := n_0 + n_1 p + n_2 p^2 + \cdots + n_s p^s$ where $0 \le m_i, n_i \le p-1$ for each i. Then*

$$\binom{n}{m} \equiv \binom{n_0}{m_0}\binom{n_1}{m_1}\cdots\binom{n_s}{m_s} \pmod{p}.$$

3. Proof of Theorem 1.4

We now prove Theorem 1.4. Suppose that x^t is a planar function on $\mathbb{F}_{p^r}$ where $p^r \ge (t-1)^4$ and $t > 2$ and $p \nmid t$. Planarity implies that, for $\hat{F}(x) := (x+1)^t - x^t$, the function $c \mapsto \hat{F}(c)$ is a bijection on $\mathbb{F}_{p^r}$. By Proposition 2.4, $\hat{F}$ is an exceptional polynomial over $\mathbb{F}_{p^r}$ (and hence over $\mathbb{F}_p$), so there are infinitely many k for which $\hat{F}$ induces a bijection on $\mathbb{F}_{p^k}$; equivalently, there are infinitely many k for which x^t is a planar function on

$\mathbb{F}_{p^k}$. If $t \equiv 1 \pmod{p}$ then [16, Cor. 1.7] implies that (1.1) holds. Henceforth assume that $t \not\equiv 1 \pmod{p}$.

Since $\hat{F}(-1-x) = (-1)^{t+1}\hat{F}(x)$, bijectivity of $\hat{F}$ on $\mathbb{F}_{p^r}$ implies that p is odd and t is even. Thus also $c \mapsto F(c)$ is a bijection on $\mathbb{F}_{p^r}$, where

$$F(x) := 4^t \hat{F}\Big(\frac{x}{4} - \frac{1}{2}\Big) = (x+2)^t - (x-2)^t.$$

Since $\hat{F}$ is an exceptional polynomial over $\mathbb{F}_{p^r}$ and $\mathbb{F}_p$, also F is exceptional over these fields. Since $p \nmid t$, we have $\deg(F) = t-1$, so $\deg(F) > 1$. Hence F can be written as the composition of indecomposable polynomials over $\mathbb{F}_p$. Write $F = \hat{F}_1 \circ \hat{F}_2$ with $\hat{F}_i \in \mathbb{F}_p[x]$ and $\hat{F}_2$ indecomposable. Put $F_1(x) := \hat{F}_1(x + \hat{F}_2(0))$ and $F_2(x) := \hat{F}_2(x) - \hat{F}_2(0)$, so that $F_1, F_2 \in \mathbb{F}_p[x]$ are such that $F = F_1 \circ F_2$ and $F_2(0) = 0$ and F_2 is indecomposable. Since F is exceptional, it follows that F_2 is exceptional. Since $\deg(F) = t-1$ is coprime to p, by Proposition 2.5 there are linear $\mu, \nu \in \mathbb{F}_p[x]$ such that either

$$F_2 = \mu \circ x^m \circ \nu \text{ for some prime } m \text{ which is coprime to } p-1 \tag{3.1}$$

or

$$F_2 = \mu \circ D_n(x,a) \circ \nu \text{ for some } a \in \mathbb{F}_p^* \text{ and some prime } n \text{ which is coprime to } p^2-1. \tag{3.2}$$

In particular, since p is odd and $\deg(F)$ is coprime to p, it follows that in (3.1) we have $m \geq 3$ and $(m, 2p) = 1$, and in (3.2) we have $n \geq 5$ and $(n, 6p) = 1$.

Since t is even, F is an odd polynomial. Now Lemma 2.6 implies that $F_2(x) - F_2(0) = F_2(x)$ is odd. Recall that $F_2 = \mu \circ H \circ \nu$ where $\mu, \nu \in \mathbb{F}_p[x]$ are linear and H is either x^m or $D_n(x,a)$. Since $\deg(H)$ is odd, we know that H is odd. By Lemma 2.7, we must have $\nu(x) = c_0 x$ with $c_0 \in \mathbb{F}_p^*$. Thus $F = G \circ H(c_0 x)$ where $G := F_1 \circ \mu$ is in $\mathbb{F}_p[x]$. If $H = x^m$ with $m \geq 3$ then $F \in \mathbb{F}_p[x^m]$, which is false since the coefficient of x in F is $t(2^{t-1} - (-2)^{t-1})$ which (since t is even and coprime to p) equals $t2^t$, and in particular is nonzero. Thus we must have $H(x) = D_n(x,a)$ where $n \geq 5$ is odd and $a \in \mathbb{F}_p^*$. Now put

$$A(x) := F \circ \frac{1}{c_0}\Big(x + \frac{a}{x}\Big).$$

Then

$$A(x) = G \circ \Big(x^n + \Big(\frac{a}{x}\Big)^n\Big)$$

is an element of $\mathbb{F}_p[x^n, x^{-n}]$. But also

$$A(x) = \Big(\frac{x}{c_0} + \frac{a}{c_0 x} + 2\Big)^t - \Big(\frac{x}{c_0} + \frac{a}{c_0 x} - 2\Big)^t.$$

Now pick $b \in \mathbb{F}_{p^2}^*$ such that $b^2 = a$, and put $c = 2c_0/b$ and

$$B(x) := \frac{1}{2}\Big(\frac{c_0}{b}\Big)^t A(bx).$$

Then $B \in \mathbb{F}_{p^2}[x^n, x^{-n}]$ and

$$B(x) = \frac{1}{2}\Big((x + x^{-1} + c)^t - (x + x^{-1} - c)^t\Big).$$

The coefficient of x^{t-1} in $B(x)$ is tc, which is nonzero, so $n \mid (t-1)$. Since B is a Laurent polynomial all of whose terms have degree divisible by n, and $n \geq 5$ is odd, it follows that the coefficients of x^{t-3}, x^{t-5}, and x^{t-7} in B must be zero. We now compute these coefficients.

The coefficient of x^{t-3} in B is

$$tc(t-1) + \binom{t}{3}c^3,$$

which equals

$$ct(t-1)\Big(\frac{t-2}{6}c^2 + 1\Big).$$

Since this coefficient is zero, we must have

$$\frac{t-2}{6}c^2 = -1. \tag{3.3}$$

Here, if $p = 3$, we first interpret $\frac{t-2}{6}$ as a rational number, and then view this rational number as an element of $\mathbb{F}_p$; in particular, if $p = 3$ then $t \equiv 2 \pmod 3$ but $t \not\equiv 2 \pmod 9$.

Suppose for the moment that neither of the following holds:

$$p > 3 \quad \text{and} \quad t \equiv \frac{1}{2} \pmod p, \quad \text{or} \tag{3.4}$$

$$p = 3 \quad \text{and} \quad t \equiv \frac{1}{2} \pmod 9. \tag{3.5}$$

We will obtain a contradiction from the fact that the coefficients of x^{t-5} and x^{t-7} in B are zero. The coefficient of x^{t-5} in B is

$$tc\binom{t-1}{2} + \binom{t}{3}c^3(t-3) + \binom{t}{5}c^5;$$

in light of (3.3), we can rewrite this expression as

$$-\frac{t-2}{6}c^2 \cdot tc\binom{t-1}{2} + \binom{t}{3}c^3(t-3) - \frac{6}{t-2}c^{-2} \cdot \binom{t}{5}c^5$$

which simplifies to

$$c^3 \frac{t(t-1)}{2} \frac{(t-\frac{1}{2})(t-4)}{15}.$$

Since this equals zero, but neither (3.4) nor (3.5) holds, we must have either

$$p > 5 \quad \text{and} \quad t \equiv 4 \pmod p, \quad \text{or} \tag{3.6}$$

$$p = 5 \quad \text{and} \quad t \equiv 4 \pmod{25}. \tag{3.7}$$

In particular, $p > 3$ and $t \equiv 4 \pmod p$. Since (3.4) does not hold, we have $t \not\equiv \frac{1}{2} \pmod p$. Next, the coefficient of x^{t-7} in B is

$$tc\binom{t-1}{3} + \binom{t}{3}c^3\binom{t-3}{2} + \binom{t}{5}c^5(t-5) + \binom{t}{7}c^7;$$

again using (3.3), we can simplify this expression to

$$-2c^5t(t-1)\frac{(t+1)(t-\frac{1}{2})(t-3)(t-5)}{3^3 \cdot 5 \cdot 7}.$$

Since this equals zero, and $4 \equiv t \not\equiv \frac{1}{2} \pmod p$, we must have $4 \equiv t \equiv -1 \pmod p$, whence $p = 5$. But since $p = 5$, the vanishing of the coefficient of x^{t-7} implies that $t \equiv -1 \pmod{25}$, which contradicts (3.7). This contradiction shows that in fact either (3.4) or (3.5) must hold.

Now assume that either (3.4) or (3.5) holds. In either case, (3.3) implies that $c^2 = 4$, so $c = 2\epsilon$ with $\epsilon \in \{1, -1\}$. Hence

$$2B(x) = (x + x^{-1} + 2\epsilon)^t - (x + x^{-1} - 2\epsilon)^t.$$

Since $B(x) \in \mathbb{F}_p[x^n, x^{-n}]$, it follows that $B(x^2) \in \mathbb{F}_p[x^{2n}, x^{-2n}]$. But we compute

$$2B(x^2) = \left(x + \frac{\epsilon}{x}\right)^{2t} - \left(x - \frac{\epsilon}{x}\right)^{2t} = 2\sum_{\substack{0<i<2t \\ i \text{ odd}}} \binom{2t}{i}\epsilon^i x^{2t-2i}.$$

Since $n \mid (t-1)$, we see that $2n \mid (2t-2i)$ if and only if $n \mid (i-1)$. Thus, the condition $B(x^2) \in \mathbb{F}_p[x^{2n}, x^{-2n}]$ asserts that

$$\text{if } i \text{ is odd and } i \not\equiv 1 \pmod n \text{ then } \binom{2t}{i} \equiv 0 \pmod p.$$

Write $2t = \sum_{j=0}^{s} e_j p^j$ where e_j is an integer satisfying $0 \le e_j \le p-1$. Since either (3.4) or (3.5) holds, we have $2t \equiv 1 \pmod p$, so $e_0 = 1$. First consider $i = 1 + 2p^j$ for any $1 \le j \le s$. Clearly i is odd, and since the only prime factors of $i - 1$ are 2 and p, neither of which divides n, we also have $i \not\equiv 1 \pmod n$. Thus we must have $\binom{2t}{i} \equiv 0 \pmod p$, so Lucas's theorem (Lemma 2.9) implies $e_j < 2$. Hence every e_j is either 0 or 1. Next, for any $0 < j < k \le s$, consider the three values $i_1 = p^j$, $i_2 = p^k$, and $i_3 = 1 + p^j + p^k$. Each of these values is odd, but since $i_3 = 1 + i_1 + i_2$ we cannot have $i_1 \equiv i_2 \equiv i_3 \equiv 1 \pmod n$. Thus there is some $i \in \{p^j, p^k, 1 + p^j + p^k\}$ for which $\binom{2t}{i} \equiv 0 \pmod p$, so (again by Lucas's theorem) we must have either $e_j = 0$ or $e_k = 0$. Since $2t > 1$, the only remaining possibility is that $2t = 1 + p^s$ for some $s > 0$. Writing $q := p^s$, we compute

$$\begin{aligned} F \circ (x^2 + x^{-2}) &= (x^2 + x^{-2} + 2)^t - (x^2 + x^{-2} - 2)^t \\ &= (x + x^{-1})^{1+q} - (x - x^{-1})^{1+q} \\ &= 2(x^{q-1} + x^{1-q}). \end{aligned}$$

But also $D(x) := D_{\frac{q-1}{2}}(x,1)$ satisfies

$$D \circ (x^2 + x^{-2}) = x^{q-1} + x^{1-q},$$

so $F(x) = 2D(x)$. Since $F(x)$ is exceptional over $\mathbb{F}_{p^r}$, it follows that $D(x)$ is exceptional over $\mathbb{F}_{p^r}$ as well. By an easy classical result (see e.g. [7, Thm. 54]), $D(x)$ is exceptional over $\mathbb{F}_{p^r}$ if and only if $\frac{q-1}{2}$ is coprime to $p^{2r}-1$. But both of these numbers are divisible by $(p^{\gcd(s,2r)}-1)/2$, so we must have $p=3$ and $\gcd(s,2r)=1$. This concludes the proof.

4. Proof of Corollary 1.5

We now prove Corollary 1.5. The "if" direction is known and easy: for, if p is odd and $i \geq j \geq 0$ then

$$(x+1)^{p^i+p^j} - x^{p^i+p^j} - 1 = x^{p^i} + x^{p^j}$$

induces a homomorphism from the additive group of $\mathbb{F}_{p^k}$ to itself, and therefore induces a bijection on $\mathbb{F}_{p^k}$ if and only if it has no nonzero roots in $\mathbb{F}_{p^k}$. But its nonzero roots are the $(p^{i-j}-1)$-th roots of -1, and there are no such roots of -1 in $\mathbb{F}_{p^k}$ if either $i=j$ or $k=(i-j)u$ with u odd. Thus $x^{p^i+p^j}$ is planar on $\mathbb{F}_{p^k}$ for infinitely many k. Next, for $t = \frac{3^i+3^j}{2}$ where $p=3$ and $i > j \geq 0$ and $i \not\equiv j \pmod 2$, the argument at the end of the previous section shows that

$$(x+1)^t - x^t = 2D_s(x-1,1)$$

where $s := \frac{3^i-3^j}{2}$. Since s is coprime to 3^2-1, Dickson's result [7, Thm. 54] implies that $D_s(x,1)$ is exceptional over $\mathbb{F}_3$, so x^t is planar on $\mathbb{F}_{3^k}$ for infinitely many k.

Conversely, fix a prime p and a positive integer s, and suppose that $c \mapsto c^s$ is a planar function on $\mathbb{F}_{p^k}$ for infinitely many k. Writing $s = p^j t$ with $p \nmid t$, it follows that $c \mapsto c^t$ is planar on $\mathbb{F}_{p^k}$ for infinitely many k. In particular, $c \mapsto c^t$ is planar on $\mathbb{F}_{p^r}$ for some r such that $p^r \geq (t-1)^4$, so Theorem 1.4 implies that either (1.1) or (1.2) holds. The result follows.

5. The Segre–Bartocci conjecture

We now show how a simple modification of our argument yields a new proof of the Segre–Bartocci conjecture about monomial hyperovals in finite Desarguesian projective planes. This conjecture was only proved for the first time quite recently, by Hernando and McGuire [12], by means of a lengthy calculation involving singularities of a certain plane curve. Our proof is vastly shorter and simpler.

A *hyperoval* in $\mathbb{P}^2(\mathbb{F}_q)$ is a set of $q+2$ points in $\mathbb{P}^2(\mathbb{F}_q)$ which does not contain three collinear points. It turns out that such an object can only exist if q is even. It is easy to see that, for a suitable choice of coordinates on $\mathbb{P}^2(\mathbb{F}_q)$, any hyperoval can be written in the form

$$\{(1:c:H(c)) \colon c \in \mathbb{F}_q\} \cup \{(0:0:1),(0:1:0)\}$$

for some $H(x) \in \mathbb{F}_q[x]$. Denote this set by $D(H(x), q)$. Segre and Bartocci conjectured in 1971 [23] that the values $t = 6$ and $t = 2^i$ (with $i > 0$) are the only positive integers t for which there are infinitely many k such that $D(x^t, 2^k)$ is a hyperoval. By considering slopes of lines between two points, one can reformulate this conjecture as asserting that $t = 6$ and $t = 2^i$ are the only positive integers t for which the polynomial $\hat{F}(x) := x^{t-1} + x^{t-2} + \cdots + 1$ is exceptional over $\mathbb{F}_2$ (see, for instance, [18, p. 505]). Assume $\hat{F}$ is exceptional. Then $\hat{F}(0) \neq \hat{F}(1)$, so t is even. Assume $t > 2$, so that $\deg(F) = t - 1 > 1$. Put $F(x) := \hat{F}(x + 1)$, so

$$F(x) = \frac{(x+1)^t + 1}{x}.$$

Then F is an odd polynomial, so the first part of the proof of Theorem 1.4 shows that $F = G \circ H$ where H is either x^m (with $m > 1$ odd) or $D_n(x, 1)$ (with $n > 1$ coprime to 6). If $F = G(x^m)$ with $m > 1$ odd then t must be a power of 2: for, if 2^j and 2^k are distinct terms in the binary expansion of t, then F has terms of degrees $2^j - 1$ and $2^k - 1$ and $2^j + 2^k - 1$, and the gcd of these three degrees is 1. Finally, suppose $F = G \circ D_n(x, 1)$. Then we have $F(x + x^{-1}) = G(x^n + x^{-n}) \in \mathbb{F}_2[x^n, x^{-n}]$. In order to compute the coefficients of the Laurent polynomial $F(x + x^{-1})$, we write

$$F(x + x^{-1}) = \sum_{i=1}^{t} \binom{t}{i} (x + x^{-1})^{i-1}.$$

Since the coefficient of x^{t-1} in $F(x+x^{-1})$ is nonzero, we see that $n \mid (t-1)$, so that the coefficients of x^{t-3} and x^{t-7} must be zero. But one easily checks that this only occurs when $t = 6$, which implies the Segre–Bartocci conjecture.

6. Final remarks

We conclude with some remarks about how generally our techniques will apply to related questions. In our proof of Theorem 1.4, we applied the result of [16] to handle the case $t \equiv 1 \pmod{p}$. This played a crucial role, since if $t \equiv 1 \pmod{p}$ then $f(x) := (x + 1)^t - x^t$ has degree divisible by p, which is problematic because there is no known classification of indecomposable exceptional polynomials of degree divisible by p. There are partial results in this direction (see e.g. [9, 11, 25]), but most of them depend on the classification of finite simple groups, and so cannot be considered to be elementary. But even if we were willing to use consequences of this classification, we do not know how to avoid the use of [16] in the proof of Theorem 1.4 or Corollary 1.5. It seems strange that in our approach the case $t \not\equiv 1 \pmod{p}$ is so much easier than the case $t \equiv 1 \pmod{p}$, whereas in the approach of [13, 16] these two cases are of comparable difficulty. Might this suggest that there should be a simple proof of the case $t \equiv 1 \pmod{p}$ from the perspective of exceptional polynomials?

In the case that $t \not\equiv 0, 1 \pmod{p}$, we used known results about exceptional polynomials to reduce Theorem 1.4 to the question of whether $(x+1)^t - x^t$ is the composition of linear polynomials with polynomials of the form x^m or $D_n(x,a)$ for values of m and n satisfying certain constraints. We then introduced a method for determining which polynomials from some infinite collection can be written as a function of either $(bx+c)^m$ or $D_n(bx+c,a)$. This method seems to apply very generally: for instance, it applied at once to the polynomials arising in the Segre–Bartocci conjecture, and we do not see any special feature of the polynomials $(x+1)^t - x^t$ and $x^{t-1}+x^{t-2}+\cdots+1$ which would make the method better suited to these polynomials than to any others.

References

[1] S. S. Abhyankar, S. D. Cohen and M. E. Zieve, *Bivariate factorizations connecting Dickson polynomials and Galois theory*, Trans. Amer. Math. Soc. **352** (2000), 2871–2887. 3

[2] R. M. Beals and M. E. Zieve, *Decompositions of polynomials*, preprint, 2007. 4

[3] S. D. Cohen, review of [5], Math. Reviews 2890555. 1

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

[5] R. S. Coulter and F. Lazebnik, *On the classification of planar monomials over fields of square order*, Finite Fields Appl. **18** (2012), 316–336. 1, 10

[6] P. Dembowski and T. G. Ostrom, *Planes of order n with collineation groups of order n^2*, Math. Z. **103** (1968), 239–258. 1

[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*, Annals of Math. **11** (1896–1897), 65–120. 8

[8] A. Granville, *Arithmetic properties of binomial coefficients. I. Binomial coefficients modulo prime powers*, in: Organic Mathematics, CMS Conf. Proc. 20, Amer. Math. Soc., Providence, RI (1997), 253–276. 4

[9] R. M. Guralnick, J. E. Rosenberg and M. E. Zieve, *A new family of exceptional polynomials in characteristic two*, Annals of Math. **172** (2010), 1367–1396. 3, 9

[10] R. M. Guralnick, T. J. Tucker and M. E. Zieve, *Exceptional covers and bijections on rational points*, Int. Math. Res. Not. **2007** article ID rnm004, 19 pages. 3

[11] R. M. Guralnick and M. E. Zieve, *Polynomials with* PSL(2) *monodromy*, Annals of Math. **172** (2010), 1321–1365. 3, 9

[12] F. Hernando and G. McGuire, *Proof of a conjecture of Segre and Bartocci on monomial hyperovals in projective planes*, Des. Codes Cryptogr. **65** (2012), 275–289. 8

[13] F. Hernando, G. McGuire and F. Monserrat, *On the classification of exceptional planar functions over $\mathbb{F}_p$*, arXiv:1301.4016v1, January 17, 2013. 40 pages. 2, 9

[14] N. L. Johnson, *Projective planes of order p that admit collineation groups of order p^2*, J. Geom. **30** (1987), 49–68. 1

[15] A. A. Klyachko, *Monodromy groups of polynomial mappings*, in: Studies in Number Theory, Saratov, (1975), 82–91. 3

[16] E. Leducq, *Functions which are PN on infinitely many extensions of $\mathbb{F}_p$, p odd*, arXiv:1006.2610v2, 3 May 2012. 20 pages. 2, 5, 9

[17] R. Lidl, G. L. Mullen, and G. Turnwald, Dickson Polynomials, Longman Scientific & Technical, Essex, England, 1993. 3

[18] R. Lidl and H. Niederreiter, Finite Fields, Addison-Wesley, Reading, 1983. 9

[19] É. Lucas, *Sur les congruences des nombres eulériens et des coefficients différentiels des fonctions trigonométriques, suivant un module premier*, Bull. Soc. Math. France **6** (1877–1878), 49–54. 4

[20] P. Müller, *A Weil-bound free proof of Schur's conjecture*, Finite Fields Appl. **3** (1997), 25–32. 3

[21] P. Müller, *Permutation groups of prime degree, a quick proof of Burnside's theorem*, Arch. Math. (Basel) **85** (2005), 15–17. 3

[22] K. Nyberg and L. R. Knudsen, *Provable security against differential cryptanalysis*, in: Advances in Cryptology (CRYPTO '92), Lecture Notes in Computer Science 740, Springer-Verlag (1992), 566–574. 1

[23] B. Segre and U. Bartocci, *Ovali ed altre curve nei piani di Galois di caratteristica due*, Acta Arith. **18** (1971), 423–449. 9

[24] G. Turnwald, *A new criterion for permutation polynomials*, Finite Fields Appl. **1** (1995), 64–82. 3

[25] M. E. Zieve, *Exceptional polynomials*, in: Handbook of Finite Fields, CRC Press (2013), 229–233. 3, 9

Department of Mathematics, University of Michigan, 530 Church Street, Ann Arbor, MI 48109-1043 USA

Mathematical Sciences Center, Tsinghua University, Beijing 100084, China
E-mail address: zieve@umich.edu
URL: http://www.math.lsa.umich.edu/∼zieve/