Finite Fields and Their Applications 54 (2018) 366–375

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Carlitz–Wan conjecture for permutation polynomials and Weil bound for curves over finite fields ☆,☆☆

Jasbir S. Chahal [a], Sudhir R. Ghorpade [b,*]

[a] *Department of Mathematics, Brigham Young University, Provo, UT 84602, USA*
[b] *Department of Mathematics, Indian Institute of Technology Bombay, Powai, Mumbai 400076, India*

ARTICLE INFO

Article history:
Received 27 September 2013
Received in revised form 1 June 2018
Accepted 5 June 2018
Available online 23 August 2018
Communicated by Rudolf Lidl

MSC:
11T06
11G20
12E20

Keywords:
Permutation polynomial
Exceptional polynomial
Separable polynomial
Weil bound

ABSTRACT

The Carlitz–Wan conjecture, which is now a theorem, asserts that for any positive integer n, there is a constant C_n such that if q is any prime power $> C_n$ with $\mathrm{GCD}(n, q-1) > 1$, then there is no permutation polynomial of degree n over the finite field with q elements. From the work of von zur Gathen, it is known that one can take $C_n = n^4$. On the other hand, a conjecture of Mullen, which asserts essentially that one can take $C_n = n(n-2)$ has been shown to be false. In this paper, we use a precise version of Weil bound for the number of points of affine algebraic curves over finite fields to obtain a refinement of the result of von zur Gathen where n^4 is replaced by a sharper bound. As a corollary, we show that Mullen's conjecture holds in the affirmative if $n(n-2)$ is replaced by $n^2(n-2)^2$.

☆ This is a republication, with minor changes, of the article published earlier in Vol. 28 (July 2014), pp. 282–291. The original article was wrongly retracted by the journal on July 8, 2015 for which the publisher apologizes to the authors.

☆☆ The second named author was partially supported during the course of this work by the Indo-Russian project INT/RFBR/P-114 from the Department of Science & Technology, Govt. of India and the IRCC Award grant 12IRAWD009 from IIT Bombay.

* Corresponding author.
E-mail addresses: jasbir@math.byu.edu (J.S. Chahal), srg@math.iitb.ac.in (S.R. Ghorpade).

https://doi.org/10.1016/j.ffa.2018.07.006
1071-5797/

1. Introduction

Let $\mathbb{F}_q$ denote the finite field with q elements and $\mathbb{F}_q[x]$ (resp: $\mathbb{F}_q[x, y]$) the ring of polynomials in one variable x (resp: two variables x and y) with coefficients in $\mathbb{F}_q$. A permutation polynomial over $\mathbb{F}_q$ is an element of $\mathbb{F}_q[x]$ such that the corresponding function from $\mathbb{F}_q$ to $\mathbb{F}_q$ is bijective. For example, if n is a positive integer relatively prime to $q-1$, then x^n is a permutation polynomial over $\mathbb{F}_q$. A closely related notion is that of an exceptional polynomial, which by definition, is a univariate polynomial $f \in \mathbb{F}_q[x]$ such that the corresponding bivariate polynomial

$$f^*(x, y) = \frac{f(x) - f(y)}{x - y} \tag{1}$$

has no absolutely irreducible factor in $\mathbb{F}_q[x, y]$. The following result was proved in special cases by MacCluer [12] and Williams [22], and unconditionally, by Cohen [4, Theorem 5].

Theorem 1.1. *Every exceptional polynomial in $\mathbb{F}_q[x]$ is a permutation polynomial.*

The converse is not true, in general. For example, if p is the characteristic of $\mathbb{F}_q$ and $f(x) = x^p$, then f is a permutation polynomial, but not an exceptional polynomial. On the other hand, if we require f to be a separable polynomial, then as we shall see, f is necessarily an exceptional polynomial provided q is large enough. In fact, a result such as this and indeed much of the development concerning permutation polynomials, was motivated by a conjecture of Carlitz (1966), which states that for any even positive integer n, there is a constant C_n such that if q is any odd prime power with $q > C_n$, then there is no permutation polynomial in $\mathbb{F}_q[x]$ of degree n. This was subsequently generalized by Wan [19] in 1993 to what became known as Carlitz–Wan Conjecture, the statement of which has already been given in the abstract of this article. In the meantime, the use of fundamental inequalities concerning the number of points of algebraic curves over finite fields led to the following converse to Theorem 1.1.

Theorem 1.2. *If $f \in \mathbb{F}_q[x]$ is a separable polynomial of degree n such that f is a permutation polynomial, then f is an exceptional polynomial, provided $q \geq n^4$.*

Initially, this was proved by Hayes [9, Thm. 3.1] in 1969 with an additional hypothesis that $\mathrm{GCD}(q, n) = 1$ and with the explicit constant n^4 replaced by an abstract constant C_n. The latter stems from the use of Lang–Weil inequality. The version stated above was proposed by von zur Gathen [18] in 1991 who directly used Weil's inequality for curves, or rather, an erroneous version of it given in the book of Lidl and Niederreiter [11, p. 331]. Applications of results such as Theorem 1.2 to establish Carlitz's conjecture in a number of special cases are given by several authors beginning with Hayes [9] who considered the cases when $n = 8$ or 10. Eventually, by passing to Galois covers of the projective line over (the algebraic closure of) $\mathbb{F}_q$ and using results from group theory

(that depend on the classification theorem for finite simple groups), Fried, Guralnick and Saxl [6] showed in 1993 that there is no exceptional polynomial of even degree over $\mathbb{F}_q$ when q is odd, thus proving Carlitz's conjecture in the affirmative. Subsequently, Lenstra proved the following more general result and his proof avoids the use of the classification theorem for finite simple groups.

Theorem 1.3. *Let n be a positive integer such that* $\mathrm{GCD}(n, q-1) > 1$. *Then there is no exceptional polynomial of degree n in $\mathbb{F}_q[x]$.*

For an elementary account of the proof of Theorem 1.3, we refer to [5]. Thanks to Theorems 1.2 and 1.3, we see that Carlitz–Wan conjecture holds in the affirmative. A question that arises naturally is whether $C_n = n^4$ is the best constant possible. This has manifested itself in a slightly different context motivated by the following result of Wan [20] (see Turnwald [17] for an elementary proof) concerning the cardinality of the value set of a polynomial over $\mathbb{F}_q$.

Theorem 1.4. *If $f \in \mathbb{F}_q[x]$ has degree n and is not a permutation polynomial, then*

$$|V_f| \leq q - \left\lceil \frac{q-1}{n} \right\rceil \quad \text{where} \quad V_f := \{f(a) : a \in \mathbb{F}_q\}.$$

In 1993, Mullen [14,15] has proposed the following conjecture.

Conjecture 1.5. *If n is an even positive integer and q is an odd prime power with $q > n(n-2)$, then*

$$|V_f| \leq q - \left\lceil \frac{q-1}{n} \right\rceil \quad \text{for every } f \in \mathbb{F}_q[x] \text{ with } \deg f = n.$$

Since $q - \lceil (q-1)/n \rceil < q$ and since f is a permutation polynomial if and only if $|V_f| = q$, in view of Theorem 1.3, Mullen's conjecture is equivalent to asserting that there is no even degree permutation polynomial in $\mathbb{F}_q[x]$ when q is odd and $q > n(n-2)$. Thus Mullen's conjecture would follow from Theorems 1.2 and 1.3 at least for separable polynomials if $n(n-2)$ is replaced by n^4. However, an example by Masuda and Zieve [13] (viz., $f(x) = x^{10} + 3x$ and $q = 343 = 7^3$) and a more recent one by Shallue and Wanless [16] (for instance, $f(x) = x^6 + x^5 - x^2$ and $q = 27 = 3^3$) shows that Mullen's conjecture is false as stated. Indeed, in both these cases $q > n(n-2)$, but the given $f(x)$ of degree n is a separable permutation polynomial. However q is much smaller than n^4 as is to be expected. Thus, Shallue and Wanless have remarked that it would be interesting to know whether n^4 in Theorem 1.2 can be replaced by some quadratic in n. While we do not believe that this is feasible, we show in this article that in Theorem 1.2, the constant n^4 can be replaced by the square of Mullen's constant, viz., $n^2(n-2)^2$, thereby showing that Conjecture 1.5 is valid if $n(n-2)$ is replaced by its square. To

this end, we follow the arguments of von zur Gathen in his proof of Theorem 1.2, but manage to refine some of his bounds mainly by using a simple observation concerning linear factors (Lemma 2.1) and a precise version of the Weil bound for singular plane curves (Lemma 2.4). For the sake of completeness, we provide detailed arguments that lead to a version of Theorem 1.2 with n^4 replaced by $n^2(n-2)^2$ (and in fact, a slightly better, albeit complicated, bound) even though there is a significant overlap with the work of von zur Gathen [18]. In the next section some preliminary results are collected, while the main theorem is proved in Section 3.

2. Preliminaries

Throughout this section q denotes a power of a prime number and $\mathbb{F}_q$ the finite field with q elements. For a finite set E, we denote by $|E|$ the cardinality of E.

Since linear polynomials in $\mathbb{F}_q[x,y]$ are absolutely irreducible, the following observation may be viewed as a first step toward proving Theorem 1.2 with the added advantage that it holds for all q.

Lemma 2.1. *Let $f \in \mathbb{F}_q[x]$ be a separable permutation polynomial and let $f^*(x,y)$ in $\mathbb{F}_q[x,y]$ be as in (1). Then $f(x)-f(y)$ is squarefree. In particular, $x-y$ does not divide $f^*(x,y)$. More generally, $f^*(x,y)$ does not have a linear factor in $\mathbb{F}_q[x,y]$.*

Proof. If $f(x)-f(y)$ were divisible by h^2 for some $h \in \mathbb{F}_q[x,y]$, then taking partial derivatives, we find that h divides both $f'(x)$ and $f'(y)$, and since f is separable, this implies that h must be a constant polynomial. Now suppose a linear polynomial $ax+by+c$ divides $f^*(x,y)$, where $a,b,c \in \mathbb{F}_q$ with $a \neq 0$ or $b \neq 0$. First, suppose $a \neq 0$. Then in case $c \neq 0$, we find $f^*(-c/a, 0) = 0$, i.e., $f(-c/a) = f(0)$, which contradicts the assumption that f is a permutation polynomial. In case $c = 0$ and $a \neq -b$, we find $f^*(-b,a) = 0$, i.e., $f(-b) = f(a)$, which is again a contradiction. Finally, if $a = -b \neq 0 = c$, then $x-y$ divides $f^*(x,y)$ and this has already been ruled out. In a similar manner, we are led to a contradiction if $b \neq 0$. □

The next two results are variants of elementary bounds used by von zur Gathen [18] without proof. In fact, one of the assertions in [18, p. 144], which states that a sum of the form $\sum_{1\le i\le j\le s} n_i n_j$, where $n_1,\dots,n_s$ are positive integers with $\sum n_i \le n-1$, reaches its maximum at $(n_1,\dots,n_s) = (n-s,1,\dots,1)$ is incorrect (take, e.g., $n=5$ and $s=2$). With this in view, we include complete proofs here.

Lemma 2.2. *Let s,d be positive integers and let $\mathbb{R}_+^s := \{(x_1,\dots,x_s) \in \mathbb{R}^s : x_i \ge 0$ for all $i = 1,\dots,s\}$. Also let $f : \mathbb{R}_+^s \to \mathbb{R}$ and $D \subset \mathbb{R}^s$ be defined by*

$$f(x_1,\dots,x_s) := \sum_{1\le i<j\le s} x_i x_j \quad \text{and} \quad D := \{(x_1,\dots,x_s) \in \mathbb{R}_+^s : \sum_{i=1}^{s} x_i \le d\}.$$

Then the maximum value of f on the set D is $d^2(s-1)/2s$, attained at $x_1 = \cdots = x_s = d/s$. Moreover, if $1 \leq s \leq d/2$, then $d^2(s-1)/2s \leq d(d-2)/2$.

Proof. Induct on s. The case $s = 1$ is trivial since f is given in this case by an empty sum, which is zero. Suppose $s > 1$ and the result holds for smaller values of s. For each $i = 1, \ldots, s$, let $D_i := \{(x_1, \ldots, x_s) \in D : x_i = 0\}$. Note that the restriction of f to D_i is a function just like f, but in $s-1$ variables; hence by induction hypothesis f is bounded above on D_i by $d^2(s-2)/2(s-1)$, which is strictly smaller than $d^2(s-1)/2s$. To show that f is bounded above by $d^2(s-1)/2s$ on all of D we proceed as follows. Clearly, D is compact and f is continuous. Moreover, f is an increasing function in each of the s variables. Hence the maximum of f on D is attained at some $(x_1, \ldots, x_s) \in D$ satisfying $g(x_1, \ldots, x_s) = 0$, where $g : \mathbb{R}_+^s \to \mathbb{R}$ is given by $g(x_1, \ldots, x_s) := \sum_{i=1}^s x_i - d$. We may thus employ the Lagrange multiplier method (see, e.g., [8, §4.2]). The above argument shows that the maximum of f on $\mathbb{R}_+^s$ subject to the constraint $g = 0$ cannot be attained at a boundary point of $\mathbb{R}_+^s$ (where some $x_i = 0$). Moreover the minimum of f on $\mathbb{R}_+^s$ is evidently 0. Thus the constrained maximum of f is attained at some interior point $(x_1, \ldots, x_s)$ of $\mathbb{R}_+^s$ at which $g = 0$ and $\nabla f = \lambda \nabla g$ for some $\lambda \in \mathbb{R}$. This implies that $d - x_i = \lambda$ for all $i = 1, \ldots, s$, and hence $\lambda = (ds - d)/s$ and $x_1 = \cdots = x_s = d/s$, as desired. To prove the last assertion, observe that the function $h : (0, \infty) \to \mathbb{R}$ defined by $h(s) := d^2(s-1)/2s$ is differentiable and $h'(s) > 0$ for $s \in (0, \infty)$, and hence $h(s) \leq h(d/2) = d(d-2)/2$ if $1 \leq s \leq d/2$. □

Lemma 2.3. *Let s, d be positive integers and let $n_1, \ldots, n_s$ be integers such that $n_i \geq 2$ for all $i = 1, \ldots, s$ and $n_1 + \cdots + n_s = d$. Then $s \leq d/2$ and*

$$\sum_{i=1}^{s} (n_i - 1)(n_i - 2) \leq (d - 2s)(d - 2s + 1). \tag{2}$$

Moreover, $(d-2s)(d-2s+1) \leq (d-1)(d-2)$.

Proof. It is clear that $s \leq d/2$. We prove (2) by induction on s. The case $s = 1$ is trivial. Suppose $s > 1$ and the result holds for smaller values of s. Fix $n_s \geq 2$ and apply the induction hypothesis to obtain

$$\sum_{i=1}^{s} (n_i - 1)(n_i - 2) \leq (d - n_s - 2s + 2)(d - n_s - 2s + 3) + (n_s - 1)(n_s - 2).$$

An easy calculation shows that the expression on the right is equal to

$$(d - 2s)(d - 2s + 1) - \epsilon \quad \text{where} \quad \epsilon = 2(n_s - 2)\left[(n_1 - 2) + \cdots + (n_{s-1} - 2)\right].$$

Since $n_i \geq 2$ for all $i = 1, \ldots, s$, we find $\epsilon \geq 0$, and this yields the desired inequality. Moreover, the quadratic function $q(s) := (d - 2s)(d - 2s + 1)$ is readily seen to be decreasing in s for $1 \leq s \leq d/2$, and hence it is bounded above by $q(1)$. □

For the number of $\mathbb{F}_q$-rational points of smooth projective curves defined over $\mathbb{F}_q$, there is a well-known bound due to A. Weil. The following result is a version of this Weil bound for affine plane curves that are absolutely irreducible, but possibly singular. The inequality (3) below has been ascribed to Weil [21] in [3, eq. (1), p. 2], but it seems more appropriate to ascribe it to Leep and Yeomans [10], Aubry and Perret [1], and Bach [2], where a version of the Weil bound for singular projective curves is proved. In fact, [10, Cor. 2] gives a version for singular curves (projective as well as affine) of Serre's improvement of the Weil bound. Also, [1, Cor. 2.5] gives a bound for absolutely irreducible projective curves that are complete intersections (and in particular, absolutely irreducible projective plane curves), while [7, Cor. 7.4] contains a more precise version of this result. For the convenience of the reader, we state below the version that we require in this article and outline a quick proof.

Lemma 2.4. *Let $f(x, y)$ be an absolutely irreducible polynomial in $\mathbb{F}_q[x, y]$ of degree d and let ν be the number of zeros of f, i.e., $\nu = |\{(a, b) \in \mathbb{F}_q^2 : f(a, b) = 0\}|$. Then*

$$|\nu - q| \leq (d-1)(d-2)\sqrt{q} + d + 1. \tag{3}$$

In fact, we have a slightly better version of (3), namely,

$$q + 1 - (d-1)(d-2)\sqrt{q} - d \leq \nu \leq q + 1 + (d-1)(d-2)\sqrt{q}. \tag{4}$$

Proof. Let $F(x, y, z) \in \mathbb{F}_q[x, y, z]$ be the homogenization of f so that F is homogeneous of degree d and $f(x, y) = F(x, y, 1)$. Then F is absolutely irreducible and hence so is the projective algebraic variety in $\mathbb{P}^2$ given by F. Thus if N denotes the number of $\mathbb{F}_q$-rational points of this projective variety, then on the one hand $\nu \leq N \leq \nu + d$ and on the other hand, by Corollary 7.4 of [7],

$$|N - (q+1)| \leq (d-1)(d-2)\sqrt{q}.$$

This yields (4), which implies (3). □

3. Main Theorem

In this section we prove the following improved version of Theorem 1.2. Throughout this section n denotes a positive integer and q a prime power.

Theorem 3.1. *Let $f \in \mathbb{F}_q[x]$ be a separable polynomial of degree n such that f is a permutation polynomial. Then f is an exceptional polynomial if $q \geq n^2(n-2)^2$.*

Proof. Suppose $f \in \mathbb{F}_q[x]$ satisfies the hypothesis of the theorem, but f is not an exceptional polynomial. Let $f^* \in \mathbb{F}_q[x, y]$ be as in (1). By Lemma 2.1, f^* does not have a linear factor and in particular we must have $n \geq 3$. Also since f is not an

exceptional polynomial, there are integers s, t such that $t \geq s \geq 1$ and irreducible polynomials $g_1, \ldots, g_t \in \mathbb{F}_q[x, y]$ of degrees $n_1, \ldots, n_t$ respectively such that $f^* = g_1 \cdots g_t$ and $g_1, \ldots, g_s$ are absolutely irreducible while $g_{s+1}, \ldots, g_t$ are not absolutely irreducible. Note that $n_i \geq 2$ for $1 \leq i \leq t$, thanks to Lemma 2.1, and hence $s \leq t \leq (n-1)/2$. Let $\overline{\mathbb{F}}_q$ denote an algebraic closure of $\mathbb{F}_q$ and for $i = 1, \ldots, t$, let

$$\overline{X}_i := \{(a, b) \in \overline{\mathbb{F}}_q^2 : g_i(a, b) = 0\} \quad \text{and} \quad X_i = \overline{X}_i \cap \mathbb{F}_q^2$$

denote the affine curves defined by g_i over $\overline{\mathbb{F}}_q$ and $\mathbb{F}_q$ respectively. Also let

$$\overline{X} = \bigcup_{i=1}^{t} \overline{X}_i, \quad X = \bigcup_{i=1}^{t} X_i, \quad \overline{\Delta} = \{(a, b) \in \overline{\mathbb{F}}_q^2 : a = b\}, \quad \text{and} \quad \Delta = \overline{\Delta} \cap \mathbb{F}_q^2.$$

Now for any $i, j = 1, \ldots, t$ with $i \neq j$, by Lemma 2.1 and Hilbert's Nullstellensatz, we see that $\overline{X}_i \neq \overline{\Delta}$ and $\overline{X}_i \neq \overline{X}_j$; consequently, by Bézout's theorem,

$$|X \cap \Delta| \leq \left|\overline{X} \cap \overline{\Delta}\right| \leq (\deg f^*)(\deg \overline{\Delta}) = n - 1 \text{ and } |X_i \cap X_j| \leq \left|\overline{X}_i \cap \overline{X}_j\right| \leq n_i n_j.$$

Next, by Lemma 2.4,

$$|X_i| > q - (n_i - 1)(n_i - 2)\sqrt{q} - n_i \quad \text{for } i = 1, \ldots, s.$$

Also note that $(n_1 + \cdots + n_s) \leq (n_1 + \cdots + n_t) = n - 1$. It follows that

$$\begin{aligned} |X| \geq \left|\bigcup_{i=1}^{s} X_i\right| &\geq \sum_{i=1}^{s} |X_i| - \sum_{1 \leq i < j \leq s} |X_i \cap X_j| \\ &> sq - \sum_{i=1}^{s} (n_i - 1)(n_i - 2)\sqrt{q} - (n - 1) - \sum_{1 \leq i < j \leq s} n_i n_j. \end{aligned}$$

We now invoke Lemmas 2.2 and 2.3 with $d = n - 1$ to obtain

$$|X| > sq - (n-2)(n-3)\sqrt{q} - (n-1) - \frac{(n-1)(n-3)}{2}. \tag{5}$$

On the other hand, if Δ^c denotes the complement of Δ in $\mathbb{F}_q^2$, then

$$|X| \leq |X \cap \Delta| + |X \cap \Delta^c| \leq (n-1) + |X \cap \Delta^c|. \tag{6}$$

Moreover, for any $v \in \mathbb{F}_q$, the equation $f(x) = v$ has at most n solutions in $\mathbb{F}_q$ and so the value set of f can be partitioned as follows.

$$V_f = \coprod_{i=1}^{n} E_i \quad \text{where} \quad E_i := \left\{v \in \mathbb{F}_q : \left|f^{-1}\{v\}\right| = i\right\} \text{ for } i = 0, 1, \ldots, n,$$

where $\coprod$ denotes disjoint union (of sets). Also it is clear that

$$\mathbb{F}_q = \coprod_{v \in V_f} f^{-1}\{v\} = \coprod_{i=1}^{n} \coprod_{v \in E_i} f^{-1}\{v\}.$$

This implies that

$$q - |V_f| = \sum_{i=1}^{n} i|E_i| - \sum_{i=1}^{n} |E_i| = \sum_{i=2}^{n} (i-1)|E_i|.$$

Looking at the fibers of the map $\pi : X \cap \Delta^c \to V_f$ defined by $(a, b) \mapsto f(a)$, we find

$$|X \cap \Delta^c| = \sum_{v \in V_f} \left|\pi^{-1}\{v\}\right| = \sum_{i=1}^{n} \sum_{v \in E_i} \left|\pi^{-1}\{v\}\right| = \sum_{i=2}^{n} i(i-1)\,|E_i| \le n\,(q - |V_f|)\,.$$

Using the last inequality together with (5) and (6), we see that

$$n\,(q - |V_f|) \ge |X| - (n-1) > q - (n-2)(n-3)\sqrt{q} - 2(n-1) - \frac{(n-1)(n-3)}{2}.$$

To complete the proof, it suffices to observe that if $q \ge n^2(n-2)^2$, then

$$q - (n-2)(n-3)\sqrt{q} - 2(n-1) - \frac{(n-1)(n-3)}{2} \ge n^2(n-2)^2 - n(n-2)^2(n-3) - \frac{n^2-1}{2}$$

and the expression on the right simplifies to $\frac{1}{2}(6n^3 - 25n^2 + 24n + 1)$, which is readily seen to be positive if $n \ge 3$. This implies that $|V_f| < q$, which contradicts the assumption that f is a permutation polynomial. □

The following result proves a slightly more general version of a conjecture of Mullen, provided the conjectured bound $n(n-2)$ is replaced by its square.

Corollary 3.2. *Assume that* $\mathrm{GCD}(n, q-1) > 1$ *and* $q \ge n^2(n-2)^2$. *Then*

$$|V_f| \le q - \left\lceil \frac{q-1}{n} \right\rceil \quad \textit{for every } f \in \mathbb{F}_q[x] \textit{ with } \deg f = n.$$

Proof. Let $f \in \mathbb{F}_q[x]$ with $\deg f = n$. The desired inequality will follow from Theorem 1.4 if we show that f is not a permutation polynomial. Let p denote the characteristic of $\mathbb{F}_q$. Note that $f(x) = g(x^{p^e})$ for some nonnegative integer e and a separable polynomial $g \in \mathbb{F}_q[x]$ of degree m (say). Thus $n = mp^e$ and hence $\mathrm{GCD}(m, q-1) = \mathrm{GCD}(n, q-1) > 1$ and $m^2(m-2)^2 \le n^2(n-2)^2 \le q$. Also since $a \mapsto a^{p^e}$ gives a bijection of $\mathbb{F}_q$ onto itself, we see that f is a permutation polynomial if and only if g is a permutation polynomial. Hence replacing f by g if necessary, we may assume without loss of generality that f

is a separable polynomial. Now if f were a permutation polynomial, then the condition on q together with Theorem 3.1 ensures that f is an exceptional polynomial. But this contradicts Theorem 1.3. □

Another corollary is that the Carlitz–Wan conjecture holds with a slight improvement in the bound appearing therein.

Corollary 3.3. *Assume that* $\mathrm{GCD}(n, q-1) > 1$ *and* $q \geq n^2(n-2)^2$. *Then there is no permutation polynomial in* $\mathbb{F}_q[x]$ *of degree* n.

Proof. Suppose there is a permutation polynomial $f \in \mathbb{F}_q[x]$ of degree n. As in the proof of Corollary 3.2, we may assume without loss of generality that f is a separable polynomial. Now apply Theorems 3.1 and 1.3 to arrive at a contradiction. □

Remark 3.4. A closer look at the proof of Theorem 3.1 shows that we can replace $n^2(n-2)^2$ by a slightly better, albeit more complicated, bound B_n given by

$$B_n = \left(\frac{(n-2)(n-3) + \sqrt{(n-2)^2(n-3)^2 + 2(n^2-1)}}{2} \right)^2 .$$

Indeed the quadratic polynomial

$$q - (n-2)(n-3)\sqrt{q} - 2(n-1) - \frac{(n-1)(n-3)}{2} = q - (n-2)(n-3)\sqrt{q} - \frac{(n^2-1)}{2}$$

in $\sqrt{q}$ would take nonnegative values if $\sqrt{q}$ is greater than or equal to the largest of the two roots. This leads to the bound B_n stated above. Evidently, we can use the bound B_n in place of $n^2(n-2)^2$ in Corollaries 3.2 and 3.3 as well. For instance, in the counterexample to Mullen's conjecture by Masuda and Zieve [13] (viz., $f(x) = x^{10} + 3x$ and $q = 343 = 7^3$), we have $n^4 = 10000$, $n^2(n-2)^2 = 6400$ and $B_n \approx 3235$, whereas in the case of $f(x) = x^6 + x^5 - x^2$ and $q = 27 = 3^3$ (which is a counterexample by Shallue and Wanless [16]), we have $n^4 = 1296$, $n^2(n-2)^2 = 576$ and $B_n \approx 178$.

Acknowledgments

We are grateful to the Department of Mathematics at the Brigham Young University for supporting the visit of the second named author during May 2013 when some of this work was carried out.

References

[1] Y. Aubry, M. Perret, A Weil theorem for singular curves, in: Arithmetic, Geometry and Coding Theory, Luminy, 1993, De Gruyter, Berlin, 1996, pp. 1–7.
[2] E. Bach, Weil bounds for singular curves, Appl. Algebra Eng. Commun. Comput. 7 (1996) 289–298.

[3] A. Cafure, G. Matera, Improved explicit estimates on the number of solutions of equations over a finite field, Finite Fields Appl. 12 (2006) 155–185.
[4] S.D. Cohen, The distribution of polynomials over finite fields, Acta Arith. 17 (1970) 255–271.
[5] S.D. Cohen, M.D. Fried, Lenstra's proof of the Carlitz–Wan conjecture on exceptional polynomials: an elementary version, Finite Fields Appl. 1 (1995) 372–375.
[6] M.D. Fried, R. Guralnick, J. Saxl, Schur covers and Carlitz's conjecture, Isr. J. Math. 82 (1993) 157–225.
[7] S.R. Ghorpade, G. Lachaud, Étale cohomology, Lefschetz theorems, and number of points of singular varieties over finite fields, Mosc. Math. J. 2 (3) (2002) 589–631.
[8] S.R. Ghorpade, B.V. Limaye, A Course in Multivariable Calculus and Analysis, Springer, New York, 2010.
[9] D.R. Hayes, A geometric approach to permutation polynomials over a finite field, Duke Math. J. 34 (1967) 293–305.
[10] D. Leep, C. Yeomans, The number of points on a singular curve over a finite field, Arch. Math. 63 (1994) 420–426.
[11] R. Lidl, H. Niederreiter, Finite Fields, Encycl. Math. Appl., vol. 20, Cambridge University Press, Cambridge, 1983.
[12] C.R. MacCleur, On a conjecture of Davenport and Lewis concerning exceptional polynomials, Acta Arith. 12 (1967) 289–299.
[13] A.M. Masuda, M.E. Zieve, Permutation binomials over finite fields, Trans. Am. Math. Soc. 361 (2009) 4169–4180.
[14] G.L. Mullen, Permutation polynomials over finite fields, in: Finite Fields, Coding Theory and Advances in Communications and Computing, Marcel Dekker, New York, 1993, pp. 131–151.
[15] G.L. Mullen, Permutation polynomials: a matrix analogue of Schur's conjecture and a survey of recent results, Finite Fields Appl. 1 (1995) 242–258.
[16] C.J. Shallue, I.M. Wanless, Permutation polynomials and orthomorphism polynomials of degree six, Finite Fields Appl. 20 (2013) 84–92.
[17] G. Turnwald, A new criterion for permutation polynomials, Finite Fields Appl. 1 (1995) 64–82.
[18] J. von zur Gathen, Values of polynomials over finite fields, Bull. Aust. Math. Soc. 43 (1991) 141–146.
[19] D. Wan, A generalisation of the Carlitz conjecture, in: Finite Fields, Coding Theory and Advances in Communications and Computing, Marcel Dekker, 1993, pp. 431–432.
[20] D. Wan, A p-adic lifting lemma and its applications to permutation polynomials, in: Finite Fields, Coding Theory and Advances in Communications and Computing, Marcel Dekker, 1993, pp. 209–216.
[21] A. Weil, Sur les Courbes Algébriques et les Variétés qui s'en déduisent, Actual. Sci. Ind., vol. 1041, Hermann, Paris, 1948.
[22] K.S. Williams, On exceptional polynomials, Can. Math. Bull. 11 (1968) 279–282.