PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 110, Number 2, October 1990

PERMUTATION POLYNOMIALS AND RESOLUTION OF SINGULARITIES OVER FINITE FIELDS

DAQING WAN

(Communicated by William Adams)

ABSTRACT. A geometric approach is introduced to study permutation polynomials over a finite field. As an application, we prove that there are no permutation polynomials of degree $2l$ over a large finite field, where l is an odd prime. This proves that the Carlitz conjecture is true for $n = 2l$. Previously, the conjecture was known to be true only for $n \leq 16$.

1. INTRODUCTION

Let F_q be a finite field with $q = p^k$ elements where p is a prime. A polynomial $f(x)$ over F_q is called a permutation polynomial over F_q if $f(x)$ induces a one-one map of F_q onto itself. A well-known open problem [5, 6] in this connection is the following conjecture raised by L. Carlitz in 1966:

Conjecture. For any positive even integer n, there are no permutation polynomials of degree n over F_q if q is sufficiently large compared to n.

The conjecture is easily shown to be true for all $n = 2^a$. Dickson's list [2] of permutation polynomials shows the conjecture is true for $n = 6$. Hayes [4] proved the conjecture for $n = 10$. The author recently settled the cases $n = 12$ and $n = 14$ [9]. In this paper, we shall relate the above conjecture to the study of resolution of singularities of a plane algebraic curve over a finite field. As an application, we shall prove the conjecture for $n = 2l$, where l is an odd prime. That is,

Theorem 1. *The Carlitz conjecture holds for all $n = 2l$, where l is an odd prime.*

Remark. S. D. Cohen [1] has obtained a different and independent proof of Theorem 1. He also proves the conjecture for $n < 1000$.

Our approach to attack the conjecture is as follows: Let $f(x) = x^n + a_1 x^{n-1} + \cdots + a_n$ be a separable polynomial of degree n over F_q, where n is even and p is odd. Consider the projective plane curve C defined by the affine polynomial equation $\phi(x, y) = (f(x) - f(y))/(x - y) = 0$. In the study of the Carlitz

Received by the editors August 22, 1989 and, in revised form, November 15, 1989.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 11T99; Secondary 14H20.

conjecture, it is well known that one can suppose that p is a factor of n. In this case, the points $P = (-1, 1, 0)$ and $Q = (1, 1, 0)$ are two F_q-rational singular points on C at infinity. If one can resolve over F_q one of the two singular points P and Q to get another plane curve with a nonsingular point rational over F_q, then the Riemann Hypothesis for curves over a finite field implies that C must have a lot of F_q-rational points. This means that $f(x)$ can not be a permutation polynomial over F_q if q is large.

In the case $n = 2l$, where l is an odd prime, we can resolve over F_q one of the singularities by explicitly constructing a sequence of birational maps (blowing up). Thus, the Carlitz conjecture is proved in this case. It is conceivable that the same method could be used to study the conjecture in some other cases. However, the concrete case by case construction of the desired resolution seems rather difficult to generalize to give a complete solution of the conjecture. It might be instructive to use the modern machinery of abstract algebraic geometry, where rich results are available. Due to lack of knowledge, however, we are unable to say anything more here.

2. Permutation polynomials and exceptional polynomials

Here we briefly recall the connection between permutation polynomials and exceptional polynomials. If $f(x) = g(x^p)$, it is clear that $f(x)$ is a permutation polynomial if and only if $g(x)$ is a permutation polynomial. Thus, without loss of generality, we shall always assume that $f(x)$ is separable.

A polynomial $\phi(x, y) \in F_q[x, y]$ of positive degree is called absolutely irreducible over F_q if $\phi(x, y)$ is irreducible over the algebraic closure $\overline{F}_q$ of F_q. For any separable $f(x) \in F_q[x]$, if the associated polynomial $\phi(x, y) = (f(x) - f(y))/(x - y)$ has no absolutely irreducible factors over F_q, $f(x)$ is called exceptional over F_q. The relationship between permutation polynomials and exceptional polynomials is provided by the following result [9, Theorem 2.4].

Lemma 2. *Let $f(x) \in F_q[x]$ be a separable polynomial of degree n. For q sufficiently large compared to n, $f(x)$ is a permutation polynomial over F_q if and only if $f(x)$ is an exceptional polynomial over F_q.*

3. Equations over finite fields

In this section, we prove a useful simple result on hypersurfaces defined over F_q. This is more general than what we shall need in this paper. However, it seems interesting in its own right.

Proposition 3. *Let $f(x_1, \ldots, x_k)$, $k \geq 2$, be a polynomial over F_q of degree n in k variables. If the affine hypersurface H defined by $f = 0$ has a nonsingular point P rational over F_q, then the component of H containing P is defined by an absolutely irreducible polynomial g over F_q. Furthermore, g is a simple factor of f.*

It follows immediately from the Riemann Hypothesis over a finite field [7] that we have the following interesting corollary.

Corollary 4. *Let* $N_q(f)$ (resp. $M_q(f)$) *be the number of* F_q*-rational solutions* (resp. F_q*-rational nonsingular solutions*) *of the equation* $f(x_1, \ldots, x_k) = 0$. *If* $M_q(f) \geq 1$, *then*

$$N_q(f) \geq q^{k-1} + O(q^{k-3/2}),$$
$$M_q(f) \geq q^{k-1} + O(q^{k-3/2}).$$

Note that Corollary 4 should be compared with a well-known theorem of Warning [7] which asserts that if $N_q(f) \geq 1$, then $N_q(f) \geq q^{k-n}$. It is easy to see that results similar to Proposition 3 and Corollary 4 hold if one consider a projective hypersurface.

Proof of Proposition 3. Let

$$f(x_1, \ldots, x_k) = \prod_{i=1}^{r} g_i(x_1, \ldots, x_k)$$

be the complete factorization of f over the algebraic closure $\overline{F}_q$ of F_q. Since $M_q(f) \geq 1$, $f = 0$ has a nonsingular solution P. Without loss of generality, we may suppose that $g_1(P) = 0$. If the hypersurface $g_1 = 0$ is not defined over F_q, then there is an automorphism $\sigma \in \mathrm{Gal}(\overline{F}_q/F_q)$ such that $\sigma(g_1) = g_j$ (up to a nonzero constant factor) for some $j > 1$. This implies that $g_j(P) = 0$ and P is a singular point of $f = 0$. Thus, g_1 (up to a nonzero constant) is an absolutely irreducible polynomial over F_q. Furthermore, g_1 is a simple factor of f since P is a nonsingular point of $f = 0$. □

4. Permutation polynomials and resolution of singularities

We first describe the general method to use resolution of singularities to attack the Carlitz conjecture. As above, we assume that $f(x)$ is separable.

Let

$$f(x) = x^n + a_1 x^{n-1} + \cdots + a_n \tag{1}$$

be a monic polynomial of degree n over a large finite field F_q. Consider the projective curve defined by

$$\begin{aligned} \phi(x, y, z) &= z^n \left(f\left(\frac{x}{z}\right) - f\left(\frac{y}{z}\right) \right) / (x - y) \\ &= \frac{x^n - y^n}{x - y} + a_1 \frac{(x^{n-1} - y^{n-1})}{x - y} z + \cdots + a_{n-1} z^{n-1} = 0. \end{aligned} \tag{2}$$

If there is an absolutely irreducible factor of $\phi(x, y, z)$ over F_q, then, setting $z = 1$, we get an absolutely irreducible factor over F_q of

$$\phi(x, y) = (f(x) - f(y))/(x - y).$$

This is true because $\phi(x, y, z)$ has no factors involving only the variable z.

Now, if n is even, then $P = (-1, 1, 0)$ is an F_q-rational point on the curve $\phi = 0$. If P is nonsingular, i.e., p does not divide n or $a_1 \neq 0$, then Proposition 3 shows that ϕ has an absolutely irreducible factor over F_q. Thus, f is not exceptional. Lemma 2 shows that the Carlitz conjecture is true in this case.

If P is a singular point, one naturally wants to resolve the singularity by a birational transformation. Suppose that there is a birational transformation B defined over F_q between the plane curve $\phi = 0$ and another plane curve $\psi = 0$ defined over F_q such that the plane curve $\psi = 0$ has a nonsingular point rational over F_q. Then, by Proposition 3, the component of $\psi = 0$ containing the nonsingular point is absolutely irreducible over F_q. Since $\phi = 0$ and $\psi = 0$ are birationally isomorphic, it follows that ϕ has an absolutely irreducible factor over F_q. Lemma 2 shows that the Carlitz conjecture holds.

Assume P is singular, then p is a factor of n. In this case, $Q = (1, 1, 0)$ is an F_q-rational singular point on the curve $\phi = 0$. Similarly, if one can resolve the singularity at Q in the above way, the same argument implies that the Carlitz conjecture is true.

The above discussion reduces the Carlitz conjecture to the study of resolution of singularity with certain properties. This suggests the following more general question for hypersurfaces.

Rational resolution question at a point. Given a hypersurface H and a singular point P on H, both defined over a large finite field F_q, what conditions are required on P and q to insure that H is birationally isomorphic (over F_q) to a hypersurface with an F_q-rational nonsingular point?

By Proposition 3 and the Riemann Hypothesis over a finite field, one sees that this question is equivalent to ask when a rational singular point on a polynomial equation $f(x_1, \ldots, x_n) = 0$ over a large finite field F_q insures the existence of an absolutely irreducible factor of f over F_q. The last question frequently occurs in the study of finite fields. It is therefore useful to have a good knowledge of the above resolution question.

5. The Carlitz conjecture for $n = 2l$

We now turn to prove the Carlitz conjecture for $n = 2l$, where l is an odd prime. The following result on finite fields [7, p. 200] will be needed in our proof.

Lemma 5. *Let a and b be two elements of F_q. If a is not a $(p-1)$th power in F_q, then the equation $x^p - ax - b = 0$ has a solution in F_q. In fact, let $q = p^k$, $\alpha = a^{1+p+\cdots+p^{k-1}}$ and $\beta = ba^{p+p^2+\cdots+p^{k-1}} + b^p a^{p^2+\cdots+p^{k-1}} + \cdots + b^{p^{k-1}}$. Then $\beta/(1-\alpha)$ is a root of $x^p - ax - b = 0$ in F_q.*

Proof of Theorem 1. Let $f(x)$ be given as in (1). Let p be odd and $n = 2l$, where l is an odd prime. If $l \neq p$, the characteristic of F_q, the argument of

§4 shows that the Carlitz conjecture is true. Thus, we assume that $l = p$ in the following. As before, we may also suppose that $f(x)$ is separable. Let h be the smallest positive integer such that $a_h \neq 0$ $1 \leq h \leq 2p-1$. If $h = p$, then $f(x) = x^{2p} + a_p x^p + \cdots$. The linear transform $x \to x - (1/2)a_p^{q/p}$ removes the a_p-term. Thus, we can suppose that $h \neq p$. Now $f(x) = x^{2p} + a_h x^{2p-h} + \cdots$. To be simple, we work in the affine (x, z) plane and set $y = 1$ in (2), obtaining

$$\phi(x, 1, z) = \frac{x^{2p} - 1}{x - 1} + a_h \frac{(x^{2p-h} - 1)}{x - 1} z^h + \cdots = 0. \tag{3}$$

Case I. $h = p-1$ and $a_p \neq 0$. In this case, $f(x) = x^{2p} + a_{p-1}x^{p+1} + a_p x^p + \cdots$. We first suppose that $(-1/2)a_{p-1}$ is not a $(p-1)$th power in F_q. Lemma 5 implies that there is an element $c \in F_q$ such that $c^p + (1/2)a_{p-1}c + (1/2)a_p = 0$. Then the linear transformation $x \to x + c$ removes the a_p-term. Thus, we have $a_p = 0$ and the present case is reduced to Case II. Next, we suppose that $(-1/2)a_{p-1}$ is a $(p-1)$th power in F_q. We move the point $Q = (1, 1, 0)$ to the origin, i.e., make the transformation $x \to x - 1$. Then (3) takes the form

$$2\left(x^{p-1} + \frac{a_{p-1}}{2} z^{p-1}\right) + \cdots = 0, \tag{4}$$

where the omitted terms all have higher order of vanishing at the origin than one of the written terms (this agreement is used throughout the following). Now, since $(-1/2)a_{p-1}$ is a $(p-1)$th power in F_q, $x^{p-1} + (a_{p-1}/2)z^{p-1}$ splits into linear factors over F_q. Thus, blowing up the origin in (4) $(x \to xz)$, we get $p-1$ nonsingular points rational over F_q (corresponding to the zeros of $x^{p-1} + a_{p-1}/2 = 0$) of the new plane curve (the strict transform, see [3]). This shows that we can exclude the case: $h = p-1$ and $a_p \neq 0$.

Case II. h is even. If $f(x) = g(x^2)$ for some polynomial $g(x) \in F_q[x]$, then $(x+y)$ is already an absolutely irreducible factor of $\phi(x, y, z)$ over F_q. Lemma 2 shows that we are done. If $f(x) \neq g(x^2)$ for any polynomial $g(x)$, there is a smallest odd positive integer t such that $a_{h+t} \neq 0$. We move the point $P = (-1, 1, 0)$ to the origin $(x \to x + 1)$, then (3) takes the form (up to a nonzero constant)

$$x^p + axz^h + bz^{h+t} + \cdots = 0, \tag{5}$$

where a and b are nonzero elements of F_q.

If $h \leq p-1$, we make the birational transform $x \to xz$ $(z \to z)$ and remove the trivial factor z^{h+1}. Then (5) takes the form

$$x^p z^{p-1-h} + ax + bz^{t-1} + z(\cdots) = 0. \tag{6}$$

If $t > 1$, then $(0, 0)$ is a nonsingular point of (6) rational over F_q and we are done. If $t = 1$, by Case I we can suppose that $h < p-1$. Then $(-b/a, 0)$ is a desired nonsingular F_q-rational point on (6). Again, we are done.

If $2p-2 \geq h \geq p+1$, replacing x by xz in (5) and removing the factor z^p, we get

$$x^p + axz^{h+1-p} + bz^{h+t-p} + \cdots = 0. \tag{7}$$

Now this curve has the same form as (5) and satisfies that $h+1-p \leq p-1$. The above argument applies except for the following two cases: $h+1-p = p-1$ or $t = 1$. In the first case, $h = 2p-2$, thus $t = 1$ since $h+t \leq 2p$ and $h+t$ is odd. If $t = 1$, then we have $0 < h+1-p \leq p-1$. (7) has the form

$$x^p + bz^{h+1-p} + \cdots, \tag{8}$$

where p and $h+1-p$ are relatively prime since $h \leq 2p-2$. Then the following lemma applies.

Lemma 6. *Let e_1 and e_2 be two relatively prime positive integers. Let $a \in F_q^*$. Then, any plane curve over F_q of the form*

$$x^{e_1} + az^{e_2} + \cdots, \tag{9}$$

is birationally equivalent to a plane curve with an F_q-rational nonsingular point, where the omitted terms all have higher order of vanishing at the origin than one of the written terms.

Proof of Lemma 6. We may suppose that $e_1 \geq e_2$. If $e_2 = 1$, the origin is already an F_q-rational nonsingular point and we are done. If $e_2 > 1$, by the assumption on the e_i's, one can write $e_1 = d_1e_2 + e_3$, where $0 < e_3 < e_2$. We make the birational transformation $z \to x^{d_1}z$. Then (9) is birationally isomorphic to a plane curve of the form

$$x^{e_3} + az^{e_2} + \cdots. \tag{10}$$

(10) has the same form as (9) and satisfies the conditions of Lemma 6. By induction or the Euclidean algorithm, one sees that Lemma 6 holds.

Case III. h is odd. We move the point $(-1, 1, 0)$ to the origin $(x \to x+1)$. Then (3) has the form

$$x^p + az^h + \cdots. \tag{11}$$

Since $h \neq p$ and $0 < h < 2p$, p and h are relatively prime. The desired resolution follows from Lemma 6. The proof is complete. □

References

1. S. D. Cohen, *Permutation polynomials and primitive permutation groups*, University of Glasgow, Department of Mathematics, preprint series no. 89/41.
2. L. E. Dickson, *The analytic representation of substitutions on a prime power of letters with a discussion of the linear group*, Ann. of Math. **11** (1897), 65–120, 161–183.
3. R. Hartshorne, *Algebraic geometry*, Graduate Texts in Mathematics, no. 52, Springer-Verlag, Berlin and New York, 1977, 28–30.

4. D. R. Hayes, *A geometric approach to permutation polynomials over a finite field*, Duke Math. J. **34** (1967), 293–305.
5. R. Lidl and G. L. Mullen, *When does a polynomial over a finite field permute the elements of the field?*, Amer. Math. Monthly **95** (1988), 243–246.
6. R. Lidl and H. Niderreiter, *Finite fields*, Encyclopedia Math. Appl., vol. 20, Addison-Wesley, Reading, MA, 1983.
7. W. M. Schmidt, *Equations over finite fields*, Lecture Notes in Math., vol. 536, Springer-Verlag, Heidelberg, 1976.
8. B. Segre, *Arithmetische Eigenschaften von Galois-Raumen*, I, Math. Ann. **154** (1964), 195–256.
9. Daqing Wan, *On a conjecture of Carlitz*, J. Austral. Math. Soc. (Ser. A) **43** (1987), 375–384.

Department of Mathematics, The University of Washington, Seattle, Washington 98195