ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 26, Number 3, Summer 1996

NONSINGULAR ZEROS OF QUINTIC FORMS OVER FINITE FIELDS

DAVID B. LEEP AND CHARLES C. YEOMANS

ABSTRACT. Let f be a nondegenerate homogeneous polynomial of degree 5 defined over the finite field $\mathbf{F}_q$ in at least six variables. We show that if $q > 101$, then f has a nonsingular $\mathbf{F}_q$-rational zero.

1. Introduction. Let $f \in \mathbf{F}_q[x_1, \dots, x_n]$ be a homogeneous form of degree d, where $\mathbf{F}_q$ is the finite field with q elements. If $n > d$, then one knows (see Lemma 2.2) that f has a nontrivial $\mathbf{F}_q$-rational zero. It is also useful to know under what conditions one can guarantee the existence of a *nonsingular* $\mathbf{F}_q$-rational zero of f.

To cite one example, suppose F is a polynomial defined over a p-adic field K with coefficients in the ring A of integers of K, and let $\overline{F}$ denote the reduction of F modulo the maximal ideal of A. Then $\overline{F}$ is defined over some finite field. If $\overline{F}$ has a nonsingular zero over this finite field, then Hensel's lemma allows one to construct a nonsingular K-rational zero of F.

A theorem of Lang-Weil [**4**, p. 824, Corollary 3] says that if f is absolutely irreducible and q is sufficiently large (depending on n and d), then f has a nonsingular zero over $\mathbf{F}_q$. But other than for the well-known and easy cases of a quadratic or cubic form (see the end of Lemma 3.5 for the cubic case), the only other effective general result comes from Deligne's solution of the Weil conjectures, from which one can obtain a bound on q for nonsingular f (see [**2**, p. 276, Theorem 6.1]).

Our main result is the following (Corollary 4.5):

Let f be a nondegenerate quintic form in at least six variables over the finite field $\mathbf{F}_q$. If $q > 101$, then f has a nonsingular $\mathbf{F}_q$-rational zero.

Received by the editors on November 3, 1994.

While our result is specific to forms of degree 5, it does not require that the form be nonsingular, or even absolutely irreducible. Furthermore, the techniques of the proof can be applied more generally, at least to forms of low degree.

For some quintic forms in 3 to 5 variables, we also obtain the same bound of 101 in Theorem 4.4. Unfortunately, we must require in advance that the form has a singular $\mathbf{F}_q$-rational zero. Thus, for nonsingular quintic forms in less than six variables, we can do no better than the theorems of Weil and Deligne.

We now give a summary of notation and terminology.

We denote by $\mathbf{F}_q$ the finite field of cardinality q. For a field K, $\mathbf{P}^n(K)$ denotes n-dimensional projective space over K.

Let f be a nonzero homogeneous polynomial (or form) with coefficients in a field K. We define the order of f as follows. Let $f \in K[x_1, \dots , x_n]$ be a homogeneous polynomial, and let $\gamma(f)$ be the number of variables occurring in the monomials in f with nonzero coefficient. Define the order of f to be $\min\{\gamma(f(Ax)) \mid A \in GL_n(K)\}$. This is the number of variables upon which f actually depends. A polynomial for which $\gamma(f) >$ order (f) is said to be degenerate; otherwise, it is said to be nondegenerate. By definition, every polynomial can be made nondegenerate by a linear change of variables. We note that any absolutely irreducible homogeneous polynomial of degree greater than 1 has order at least 3.

Let $f \in K[x_1, \dots , x_n]$, and let L be a field containing K. If there exist $z_1, \dots , z_n \in L$ satisfying $f(z_1, \dots , z_n) = 0$, then $z = (z_1, \dots , z_n)$ is said to be an L-rational zero of f. If at least one of the $z_i \neq 0$, then the zero is said to be nontrivial. Suppose $z = (z_1, \dots , z_n)$ is an L-rational zero of f. By a linear change of variables defined over L, we may assume that $z = (1, 0, \dots , 0)$. Thus, we may write $f = \sum_{k=0}^{d} x_1^{d-k} A_k(x_2, \dots , x_n)$, where A_k is a homogeneous form of degree k or the zero polynomial. Since $f(1, 0, \dots , 0) = 0$, $A_0 = 0$. The minimum degree of the nonvanishing A_k is said to be the multiplicity of z. Clearly the multiplicity of z is at least 1 and at most d. If f is nondegenerate, then the multiplicity of z is at most $d - 1$.

Let f be a polynomial in n variables, and let $\bar{f}$ be the restriction of f to a linear subspace V. If $z \in V$ is a zero of f and a nonsingular zero of $\bar{f}$, then z is a nonsingular zero of f.

We shall require some basic definitions and facts about algebraic curves, for which we take [**3**] as a reference.

2. Known results.

We list for reference some results which we shall use throughout this paper.

Lemma 2.1. *For $n \geq 2$, let H_n be the homogeneous ideal in $\mathbf{F}_q[x_1, \dots, x_n]$ (i.e., generated by homogeneous polynomials) of polynomials vanishing at every point of $\mathbf{F}_q^n$. Then H_n is generated by the forms $x_i^q x_j - x_i x_j^q$, where i and j satisfy $1 \leq i < j \leq n$. In particular, if f is nonzero and $f \in H_n$, then* $\deg(f) \geq q+1$.

Lemma 2.2 (Chevalley's theorem). *Let f be a homogeneous form of degree d in n variables over $\mathbf{F}_q$. If $n > d$, then f has a nontrivial $\mathbf{F}_q$-rational zero.*

This result was originally proved in [**1**].

We shall make use of the Weil estimate for the number of rational points on a curve over a finite field. From [**6**], Corollary 1 we recall a version which applies to plane curves with singularities.

Proposition 2.3. *Let C be an absolutely irreducible projective plane curve defined over $\mathbf{F}_q$ of degree d and genus g. Let N be the number of $\mathbf{F}_q$-rational points of C. Then N satisfies*

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

If C is nonsingular, then $g = (1/2)(d-1)(d-2)$ and one recovers the usual estimate of Weil, as enhanced by Serre in [**8**].

3. Reducible forms.

In this section we consider forms of degree 5 which are not absolutely irreducible. First we need to consider forms of lower degree.

Lemma 3.1. *Let $f = x_0 A(x_1, \dots, x_n) - B(x_1, \dots, x_n)$ be a form of degree d over $\mathbf{F}_q$, with $A \neq 0$. If $q \geq d - 1$, then f has a nonsingular $\mathbf{F}_q$-rational zero.*

Proof. Since $q \geq d-1$, there exist $a_1, \dots, a_n$ such that $A(a_1, \dots, a_n) \neq 0$. One then checks easily that $(B(a_1, \dots, a_n)/A(a_1, \dots, a_n), a_1, \dots, a_n)$ is a nonsingular $\mathbf{F}_q$-rational zero of f. □

Lemma 3.2. *Let $f = x_0 A(x_1, \dots, x_n) - B(x_1, \dots, x_n)$ and $g(x_0, \dots, x_n)$ be homogeneous forms over $\mathbf{F}_q$-rational of degrees d and e, respectively, with $A \neq 0$. Assume that f does not divide g, f is irreducible and that $q \geq de$. Then there is a nontrivial $\mathbf{F}_q$-rational zero of f which is not a zero of g.*

If $q \geq d(d - 1 + e)$, then there is a nonsingular $\mathbf{F}_q$-rational zero of f which is not a zero of g.

Proof. Assume that every zero of f is a zero of g. We have

$$(*) \quad \begin{aligned}(A(x_1, \dots, x_n))^e g(x_0, \dots, x_n) &= g(x_0 A(x_1, \dots, x_n), \dots, x_n A(x_1, \dots, x_n)) \\ &\equiv g(B(x_1, \dots, x_n), x_1 A(x_1, \dots, x_n), \dots, \\ &\qquad x_n A(x_1, \dots, x_n)) \bmod f.\end{aligned}$$

Define $h(x_1, \dots, x_n) = g(B(x_1, \dots, x_n), x_1 A(x_1, \dots, x_n), \dots, x_n A(x_1, \dots, x_n))$; h is a homogeneous form of degree de. For all $a_1, \dots, a_n$ such that $A(a_1, \dots, a_n) \neq 0$, we have

$$\begin{aligned}h(a_1, \dots, a_n) &= g(B(a_1, \dots, a_n), a_1 A(a_1, \dots, a_n), \dots, a_n A(a_1, \dots, a_n)) \\ &= (A(a_1, \dots, a_n))^e g\left(\frac{B(a_1, \dots, a_n)}{A(a_1, \dots, a_n)}, a_1, \dots, a_n\right) = 0,\end{aligned}$$

since $(B(a_1, \dots, a_n)/A(a_1, \dots, a_n), a_1, \dots, a_n)$ is a zero of f and thus also a zero of g. Let $a_1, \dots, a_n$ be such that $A(a_1, \dots, a_n) = 0$. Then

$$\begin{aligned}h(a_1, \dots, a_n) &= g(B(a_1, \dots, a_n), a_1 A(a_1, \dots, a_n), \dots, a_n A(a_1, \dots, a_n)) \\ &= g(B(a_1, \dots, a_n), 0, \dots, 0) = 0,\end{aligned}$$

since $(a, 0, \dots, 0)$ is a zero of f for all a and hence a zero of g. We have shown that h vanishes on all of $\mathbf{F}_q^n$. Since, by assumption,

$q \geq de = \deg h$, Lemma 2.1 implies that h must be the zero polynomial. By $(*)$, we see that f divides $A^e g$. But $\gcd(A, f) = 1$, since f is irreducible. Thus f divides g.

To verify the second statement of the lemma, one applies the first part to the forms f and Ag. If every $\mathbf{F}_q$-rational zero of f is a zero of Ag, then f divides $A^{d+e}g$. As above, we see that f divides g. We conclude that if f does not divide g, then there is a zero of f which is not a zero of A or of g. The fact that A does not vanish implies that the zero is nonsingular. □

The bound $q \geq d(d-1+e)$ is not best possible. For example, if $d = 2$ and $e = 1$, then the second part of the lemma holds for $q \geq 2$.

Lemma 3.3. *Let f be a nondegenerate form of prime degree defined over a perfect field K which has a nontrivial K-rational zero. If f is not absolutely irreducible, then f is reducible over K.*

This is Lemma 3.3 of [**5**], in which a proof of this lemma is given.

Lemma 3.4. *Let Q be a nondegenerate quadratic form in n variables over $\mathbf{F}_q$. If $n \geq 3$, then Q is nonsingular and has an $\mathbf{F}_q$-rational zero. If $n = 2$, then Q factors into distinct linear factors. If Q factors over $\mathbf{F}_q$, then Q has a nonsingular zero. If Q is irreducible over $\mathbf{F}_q$, then Q has no nontrivial $\mathbf{F}_q$-rational zeros. If $n = 1$, then Q factors over $\mathbf{F}_q$ as the square of a linear form and has no nontrivial $\mathbf{F}_q$-rational zeros.*

Lemma 3.5. *Let f be a nondegenerate cubic form defined over $\mathbf{F}_q$ in n variables. Then f has no nontrivial $\mathbf{F}_q$-rational zeros if and only if*

(i) *f is the third power of a linear form*;

(ii) *f is irreducible over $\mathbf{F}_q$, but factors over $\mathbf{F}_{q^3}$ into conjugate linear factors.*

If f has a nontrivial $\mathbf{F}_q$-rational zero, then it must have a nonsingular $\mathbf{F}_q$-rational zero.

Proof. Assume first that f is reducible over $\mathbf{F}_q$. Then f has a linear factor. Either f is divisible by a simple linear factor L or f is divisible by the cube of a linear factor. In the first case, f clearly has a nontrivial $\mathbf{F}_q$-rational zero; in the second case, nondegeneracy of f implies that f has no nontrivial zero.

Now assume that f is irreducible over $\mathbf{F}_q$, but not absolutely irreducible. Since $\mathbf{F}_q$ is perfect, Lemma 3.3 implies that f has no nontrivial $\mathbf{F}_q$-rational zeros. One sees easily that f has a linear factor L over some extension of $\mathbf{F}_q$ of degree $d > 1$. The product of L and its conjugates is a form of degree d defined over $\mathbf{F}_q$ and which divides f. Since f is irreducible over $\mathbf{F}_q$, we conclude that $d = 3$.

Now assume that f is absolutely irreducible, in which case f has order at least 3. If f has order at least 4, then Chevalley's theorem implies the existence of an $\mathbf{F}_q$-rational zero. If f has order 3, then f defines a curve of genus 1, if f is nonsingular, or a curve of genus 0, if f is singular. Then the existence of an $\mathbf{F}_q$-rational zero of f follows from Proposition 2.3.

Now suppose that f has a nontrivial $\mathbf{F}_q$-rational zero, which we may assume to be $(1, 0, \dots, 0)$. If this zero is singular, then we may write $f = x_1 A(x_2, \dots, x_n) + B(x_2, \dots, x_n)$, where A is not the zero polynomial and has degree 2. It follows that $A(z_2, \dots, z_n) \neq 0$ for some choice of $z_2, \dots, z_n \in \mathbf{F}_q$. It follows easily that $(-B(z_2, \dots, z_n)/A(z_2, \dots, z_n), z_2, \dots, z_n)$ is a nonsingular $\mathbf{F}_q$-rational zero of f. □

Lemma 3.6. *Let C be a nondegenerate cubic form in n variables and H a linear form in the same n variables. If $q \geq 8$ and C has a nontrivial $\mathbf{F}_q$-rational zero, then either there is a nonsingular $\mathbf{F}_q$-rational zero of C which is not a zero of H or $C = HQ$, where Q has no nonsingular $\mathbf{F}_q$-rational zeros*; *in particular, Q has order at most* 2.

Proof. Suppose first that C is not absolutely irreducible. Since C has a nontrivial $\mathbf{F}_q$-rational zero, it is reducible over $\mathbf{F}_q$ by Lemma 3.3 and thus has a linear factor. The proof of Lemma 3.5 shows that in fact f has a simple linear factor L. Write $C = LQ$. If $L \neq H$ and $q \geq 3$, then we may apply Lemma 3.2 to the forms L and QH to find a nonsingular rational zero z of L which is not a zero of QH. Application of the product rule shows that z is a nonsingular zero of C which is not a zero of H.

Otherwise, $C = HQ$. If Q has a nonsingular rational zero, using Lemma 3.2 we see that Q has a nonsingular rational zero which is not a zero of H; such a zero is then easily seen to be a nonsingular zero of C. Otherwise, Q has no nonsingular $\mathbf{F}_q$-rational zeros and thus by Lemma 3.4, Q has order at most 2.

We now assume that C is absolutely irreducible. Suppose first that $n = 3$. In this case, one knows that C defines a curve of genus 1 if it is nonsingular; if C is singular, then it defines a curve of genus 0 which has exactly one singular point, and that point is defined over $\mathbf{F}_q$. Bézout's theorem tells us that C and H intersect in at most three distinct points. When C is nonsingular, it suffices to choose q large enough so that C has at least four rational points. When C is singular, it suffices to choose q large enough so that C has at least five rational points. From Proposition 2.3, we obtain the following information: if C is nonsingular and $q \geq 8$, then C has at least four rational points. If C is singular and $q \geq 5$, then C has at least five rational points.

Now suppose that $n \geq 4$. Chevalley's theorem implies that C has a nontrivial zero; thus, by Lemma 3.5 C has a nonsingular rational zero, which we may assume to be $(1, 0, \dots, 0)$. Then we may write $C = x_1^2 L(x_2, \dots, x_n) + x_1 g(x_2, \dots, x_n) + h(x_2, \dots, x_n)$, with $L \neq 0$. Since C is absolutely irreducible, H does not divide C. Thus, if $q \geq 3$, by Lemma 3.2 there is a point w satisfying $H(w) = 0$, $C(w) \neq 0$. Let p be a point such that $H(p)L(p) \neq 0$. Let Π be a plane containing $(1, 0, \dots, 0)$, p and w. The restriction of C to this plane has a nonsingular rational zero because L, restricted to Π, is not the zero polynomial. Since $H(w) = 0$, $C(w) \neq 0$, we see that H does not divide C after restriction to Π. Since H does not vanish identically on Π, $H|_\Pi$ is not the zero polynomial. Since $C|_\Pi$ has a nonsingular rational zero, $C|_\Pi$ has order 2 or 3 and the previous cases give a nonsingular $\mathbf{F}_q$-rational zero of $C|_\Pi$ which is not a zero of $H|_\Pi$, and thus there is a nonsingular $\mathbf{F}_q$-rational zero of C which is not a zero of H. □

Lemma 3.6 first appeared in [**7**] as their Theorem 2. They stated that the result was true for $q \geq 7$, but this is incorrect. The mistake occurred on p. 298, line 7 of [**7**], where a formula for the number of points on a curve was applied incorrectly.

A counterexample is given over $\mathbf{F}_7$ by the nonsingular curve defined by $y^2z = x^3 + 4z^3$ and the hyperplane defined by $x = 0$. One can check that the curve has exactly three $\mathbf{F}_7$-rational zeros, all of which lie on $x = 0$.

In addition, the theorem is slightly misstated. In the case where $C = HQ$, their condition "...Q has no k-zero off $H = 0$..." should be modified to our statement, "...Q has no nonsingular $\mathbf{F}_q$-rational zeros...". To see this, one considers the example $C = xQ(y, z)$, $H = x$, where Q is a rank 2 quadratic form having only singular rational zeros. Then $(1, 0, 0)$ is a rational zero of Q and is the only rational zero of C not lying on H, but it is singular. The point of possible confusion is that the ambient space is $\mathbf{P}^2$, and Q must be considered as defining a variety in $\mathbf{P}^2$, not $\mathbf{P}^1$.

Proposition 3.7. *Let f be a nondegenerate quintic form over $\mathbf{F}_q$, and assume that f is not absolutely irreducible.*

If f has no nontrivial $\mathbf{F}_q$-rational zeros, then f is one of the following:

(i) *the fifth power of a linear form*;

(ii) *the product of linear forms defined over $\mathbf{F}_{q^5}$ and conjugate over $\mathbf{F}_q$.*

(iii) *$f = QC$, where* (*after an appropriate linear change of variables*) *$Q = Q(x, y)$, $C = C(x, y)$, Q and C have order exactly* 2 *and neither form has a nontrivial $\mathbf{F}_q$-rational zero.*

If f has a nontrivial $\mathbf{F}_q$-rational zero, but no nonsingular rational zeros, and $q \geq 8$, then $f = QC$, where Q has degree 2, *C has degree* 3, *and neither Q nor C has an $\mathbf{F}_q$-rational nonsingular zero. In particular, Q has order at most* 2, *C has order at most* 3, *and f has order at most* 5.

Proof. Assume first that f has no $\mathbf{F}_q$-rational zero, and that f is neither the fifth power of a linear form nor the product of linear factors conjugate over $\mathbf{F}_q$. Since f is not absolutely irreducible, it has an absolutely irreducible factor g of degree $d < 5$ defined over the extension of $\mathbf{F}_q$ of degree r. The product of g and its conjugates is a factor of f defined over $\mathbf{F}_q$ of degree rd. If $rd = 5$, then $d = 1$ (since $d < 5$) and $r = 5$. But this case was ruled out above by the assumption at the beginning of the proof. Thus $rd < 5$, and we conclude that f must be reducible over $\mathbf{F}_q$.

The assumption that f have no nontrivial $\mathbf{F}_q$-rational zero easily implies that F cannot have a linear factor defined over $\mathbf{F}_q$. Thus, f must factor as QC, where Q and C are irreducible over $\mathbf{F}_q$. If Q has order at least 3, then it has a rational zero by Lemma 3.4. We conclude that Q has order exactly 2; irreducibility of Q then implies that it has no nontrivial rational zero. After a linear change of variables, we may assume that $Q = Q(x, y)$. If any variable appears nontrivially in C other than x or y, then $(0, 0, 1, \dots, 1)$ would be a nontrivial rational zero of f. Thus $C = C(x, y)$. Since C is irreducible over $\mathbf{F}_q$, it has no nontrivial rational zero and has order exactly 2.

Now assume that f has no nontrivial rational zero, but no $\mathbf{F}_q$-rational nonsingular zero. Since f is not absolutely irreducible, f is reducible over $\mathbf{F}_q$ by Lemma 3.3. Suppose that $f = Lg$, where L is linear and L and g are relatively prime. If $q \geq 4$, then the second part of Lemma 3.2 implies that there is a nonsingular zero of L which is not a zero of g. The product rule then shows that this gives a nonsingular zero of f. Thus f must factor as QC, where Q and C are relatively prime and neither has a simple linear factor. If Q has a nonsingular zero, then after a change of variables we may suppose that $Q = x_1 L + Q'$ and we may again apply Lemma 3.2, if $q \geq 8$. Thus, by Lemma 3.4 we see that Q has order at most 2 and no $\mathbf{F}_q$-rational nonsingular zeros.

Suppose now that C has an $\mathbf{F}_q$-rational nonsingular zero. We may assume that all of the $\mathbf{F}_q$-rational zeros of Q are singular and thus lie in a proper linear space. Let H be a hyperplane defined over $\mathbf{F}_q$ containing this linear space. If $H|C$, then, since C does not have a simple linear factor by assumption, $H^3|C$; but this would imply that C does not have a nonsingular zero. Thus, H does not divide C.

Since $q \geq 8$, then by Lemma 3.6 there is a nonsingular $\mathbf{F}_q$-rational zero of C which is not a zero of H and therefore not a zero of Q. This gives a nonsingular rational zero of f. Since we assume at the outset that f has no such zeros, we conclude that C has no nonsingular rational zeros and thus has order at most 3. □

Corollary 3.8. *Let f be a quintic form of order at least 6 defined over $\mathbf{F}_q$ which is not absolutely irreducible, and assume that $q \geq 8$. Then f has a nonsingular $\mathbf{F}_q$-rational zero.*

4. Absolutely irreducible quintic forms.

Lemma 4.1. *Let C be an absolutely irreducible projective plane curve of degree* 5 *over $\mathbf{F}_q$, and suppose that z is an $\mathbf{F}_q$-rational singular point of f. Then C has a nonsingular zero in the following cases*:

(1) *the multiplicity of z is* 2 *and* $q > 101$;

(2) *the multiplicity of z is* 3 *and* $q > 37$;

(3) *the multiplicity of z is* 4 *and* $q > 3$.

Proof. The first two cases follow, with a little work, from Proposition 2.3. The last case follows immediately from Lemma 3.1. □

Lemma 4.2. *Let $f, g, h \in \mathbf{F}_q[x_1, \ldots, x_n]$ be homogeneous forms of positive degrees a, b and c, respectively. Assume that f and g are relatively prime and that $q \geq \max\{ab, a+b+c\}$. Then there exists a line $L \subset \mathbf{P}^{n-1}$ defined over $\mathbf{F}_q$ such that $f|_L$ and $g|_L$ are relatively prime and such that h does not vanish identically on L.*

Proof. Since $q \geq a+b+c$, there exists a point in $\mathbf{P}^{n-1}(\mathbf{F}_q)$ at which none of f, g, h vanish. After possibly changing variables, we may assume that none of f, g and h vanishes at $(1, 0, \ldots, 0)$. This also implies that the leading x_1-coefficients of f and g have degree 0 and thus lie in $\mathbf{F}_q$.

Let $R(f, g)$ denote the resultant of f and g with respect to the variable x_1. Since f and g have no common factor of positive x_1-degree, $R(f, g)$ is not the zero polynomial. By [**9**, p. 30, Theorem 10.9], $R(f, g)$ is a nonzero homogeneous form of degree ab in $x_2, \ldots, x_n$. Since $q \geq ab$, $R(f, g)$ does not vanish identically, so we may assume, after a linear change of variables which fixes x_1, that $R(f, g)$ does not vanish at $x_2 = 1$, $x_3 = \cdots = x_n = 0$. Now choose L to be the line $x_3 = \cdots = x_n = 0$. Then $R(f|_L, g|_L) = R(f, g)(x_2, 0, \ldots, 0)$. By arrangement, $R(f|_L, g|_L)$ does not vanish on all of L and thus is not the zero polynomial. The leading x_1-coefficients of $f|_L$ and $g|_L$ continue to have degree 0. Thus it follows from [**9**, p. 29, Theorem 10.7] that $f|_L$ and $g|_L$ have no common nonconstant factor, and thus they remain relatively prime. Finally, we see that $h|_L(1, 0) \neq 0$. □

Corollary 4.3. *Let $f, g \in \mathbf{F}_q[x_1, \dots, x_n]$ be homogeneous forms of degrees a and b, respectively. Assume that f does not divide g and that $q \geq \max\{ab, a+b\}$. Then there exists a line $L \subset \mathbf{P}^{n-1}$ defined over $\mathbf{F}_q$ such that $f|_L \neq 0$ and $f|_L$ does not divide $g|_L$.*

Proof. To verify the corollary, we apply the preceding lemma to the forms $f/\gcd(f,g)$, $g/\gcd(f,g)$ and $\gcd(f,g)$. We may assume that $a \leq b$. Let $c = \deg(\gcd(f,g))$. Since f does not divide g, we have $0 \leq c \leq a-1$. Then $a-c+b-c+c = a+b-c \leq \max\{ab, a+b\}$. Now the preceding lemma implies that the restrictions of $f/\gcd(f,g)$ and $g/\gcd(f,g)$ to some line L remain relatively prime and that $\gcd(f,g)$ does not vanish identically, and thus is not the zero polynomial. We conclude that $f|_L$ does not divide $g|_L$. □

Theorem 4.4. *Let $f \in \mathbf{F}_q[x_0, \dots, x_n]$ be an absolutely irreducible nondegenerate form of degree 5 with a nontrivial $\mathbf{F}_q$-rational zero. Then f has a nonsingular $\mathbf{F}_q$-rational zero if $q > 101$.*

Proof. We may assume that $(1, 0, \dots, 0)$ is a zero of f. If this zero is nonsingular, we are finished, so assume that it is singular. Since f is nondegenerate, $(1, 0, \dots, 0)$ has multiplicity 2, 3 or 4. If the multiplicity of this zero is 4, then the existence of a nonsingular zero of f follows immediately from Lemma 3.1.

Since f is absolutely irreducible, it has order at least 3. If f has order 3, then f defines an absolutely irreducible projective plane curve and the theorem follows in this case from Lemma 4.1. Henceforth we shall assume that f has order at least 4 and that $(1, 0, \dots, 0)$ is a zero of f of multiplicity 2 or 3.

Let A be the leading x_0-coefficient of f. It follows from the absolute irreducibility of f that there is another nonzero x_0-coefficient B of f such that A does not divide B. We have $\deg(A) \leq 3$, $\deg(B) \leq 5$. Thus $\max\{\deg(A)\deg(B), \deg(A) + \deg(B)\} \leq 15$. Since $q \geq 15$, it follows from Corollary 4.3 that there is a line L such that the restriction of A to L does not divide the restriction of B to L.

By a linear change of variables which fixes x_0, we may suppose that L is the span of $(0, 1, 0, \dots, 0)$ and $(0, 0, 1, 0, \dots, 0)$. Now set $\bar{f} = f(x_0, x_1, x_2, 0, \dots, 0)$ and consider the curve defined by $\bar{f}$. Observe that $\bar{f}(1,0,0)=0$.

If $\bar{f}$ is absolutely irreducible and $q>101$, then it has a nonsingular $\mathbf{F}_q$-rational zero by Lemma 4.1, and thus so does f. Otherwise, since $\bar{f}$ has an $\mathbf{F}_q$-rational zero, it is reducible by Lemma 3.3. From above, we see that $A(x_1,x_2)\neq 0$, thus $2\leq \deg_{x_0}(\bar{f})\leq 3$. Note that $\bar{f}$ must have order at least 2, for if it had order 1, then it would be the fifth power of a linear form and would therefore satisfy either $\deg_{x_i}(\bar{f})=0$ or $\deg_{x_i}(\bar{f})=\deg(\bar{f})$ for all i.

Assume that $\bar{f}$ has a factor of x_0-degree 0. Let g be the product of all factors of $\bar{f}$ of x_0-degree 0 and write $\bar{f}=gh$. Easily one sees that $\gcd(g,h)=1$ and that g divides each x_0-coefficient of $\bar{f}$. Since $A(x_1,x_2)$ does not divide $B(x_1,x_2)$, we have $\deg(g)<\deg(A(x_1,x_2))$. It follows that $\deg(h)>\deg_{x_0}(h)=\deg_{x_0}(\bar{f})\geq 2$; that is, h has $(1,0,0)$ as a zero and has order at least 2 and degree at least 3. If g is linear and $q\geq 4$, then it follows from Lemma 3.2 that $\bar{f}$ has a nonsingular $\mathbf{F}_q$-rational zero. Otherwise, h is a cubic, and the existence of a nontrivial $\mathbf{F}_q$-rational zero implies that h has a nonsingular rational zero, by Lemma 3.5. Proposition 3.7 then shows that $\bar{f}$ has a nonsingular rational zero, if $q\geq 8$.

Now assume that $\bar{f}$ has no factor of x_0-degree 0. Since $2\leq \deg_{x_0}(\bar{f})\leq 3$ and $\bar{f}$ is reducible over $\mathbf{F}_q$, each irreducible factor of $\bar{f}$ has x_0-degree 1 or 2, and at least one of them has x_0-degree exactly 1. As before, it is easy to argue that $\bar{f}$ is not a power of a linear form. Thus we may write $\bar{f}=hk$, where $\deg_{x_0}(h)=1$ and $\gcd(h,k)=1$. If either h or k is linear and $q\geq 4$, then by Lemma 3.2 we see that $\bar{f}$ has a nonsingular $\mathbf{F}_q$-rational zero. Otherwise h is either quadratic or cubic. Since $\deg_{x_0}(h)=1$, $(1,0,0)$ is a nontrivial $\mathbf{F}_q$-rational zero of h. If h is quadratic, then we see easily that $(1,0,0)$ is a nonsingular zero of h. If h is cubic, then Lemma 3.5 implies that h has a nonsingular zero. It then follows from Proposition 3.7 that $\bar{f}$ has a nonsingular rational zero, if $q\geq 8$. □

Corollary 4.5. *Let f be a nondegenerate quintic form of order at least 6 over $\mathbf{F}_q$. If $q>101$, then f has a nonsingular $\mathbf{F}_q$-rational zero.*

Proof. If f is not absolutely irreducible, then the result follows from Corollary 3.8.

If f is absolutely irreducible, then Lemma 2.2 gives an $\mathbf{F}_q$-rational zero of f. The result then follows from Theorem 4.4. □

REFERENCES

1. C. Chevalley, *Démonstration d'une hypothèse de M. Artin*, Abh. Math. Sem. Hamburg **11** (1935), 73–75.

2. E. Freitag and R. Kiehl, *Etale cohomology and the Weil conjecture*, Springer, New York, 1988.

3. W. Fulton, *Algebraic curves*, Addison Wesley, Reading, 1989.

4. S. Lang and A. Weil, *Number of points of varieties in finite fields*, Amer. J. Math. **76** (1954), 819–827.

5. David B. Leep and Charles C. Yeomans, *Quintic forms over p-adic fields*, J. Number Theory **57** (1996), 231–241.

6. ———, *The number of points on a singular curve over a finite field*, Archiv der Mathematik **63** (1994), 420–426.

7. Donald J. Lewis and Susan E. Schuur, *Varieties of small degree over finite fields*, J. für die Reine Angew. Math. **240** (1973), 293–306.

8. J-P. Serre, *Sur le nombre des points rationelles d'une courbe algèbrique sur un corps fini*, C.R. Acad. Sci. Paris **296** (1983), 397–402.

9. R.J. Walker, *Algebraic curves*, Princeton University Press, Princeton, 1950.

Department of Mathematics, University of Kentucky, Lexington, KY 40506-0027
E-mail address: leep@ms.uky.edu

809 Cooper Drive, Lexington, KY 40502
E-mail address: cyeomans@ms.uky.edu