PACIFIC JOURNAL OF MATHEMATICS
Vol. 98, No. 1, 1982

POLYNOMIALS THAT REPRESENT QUADRATIC RESIDUES AT PRIMITIVE ROOTS

DANIEL J. MADDEN AND WILLIAM YSLAS VÉLEZ

In this paper the following result is obtained.

THEOREM. Let r be any positive integer; in all but finitely many finite fields k, of odd characteristic, for every polynomial $f(x) \in k[x]$ of degree r that is not of the form $\alpha(g(x))^2$ or $\alpha x(g(x))^2$, there exists a primitive root $\beta \in k$ such that $f(\beta)$ is a square in k.

As a result of this and some computation we shall see that for every finite field k of characteristic $\neq 2$ or 3, there exists a primitive root $\alpha \in k$ such that $-(\alpha^2+\alpha+1)=\beta^2$ for some $\beta \in k$; also every linear polynomial with nonzero constant term in the finite field k of odd characteristic represents both nonzero squares and nonsquares at primitive roots of k unless $k = GF(3)$, $GF(5)$ or $GF(7)$.

1. Introduction. This paper arose from a question posed by Moshe Rosenfeld. Alspach, Heinrich and Rosenfeld were attempting to decompose the complete symmetric digraph on n-vertices into n antidirected cycles of length $n-1$ with the property that any two cycles have exactly one undirected edge in common. (See [1] for definitions and results.) For $n=p^f$, p an odd prime, they were able to find such a decomposition provided the following question could be answered in the affirmative:

For $p^f \equiv 3 \pmod 4$, does there exist a primitive root $\alpha \in GF(p^f)$ such that $-(\alpha^2+\alpha+1)=\beta^2$ for some $\beta \in GF(p^f)$?

Experimental evidence seemed to indicate that this was true irrespective of the condition $p^f \equiv 3 \pmod 4$.

In subsequent study of this question a second problem arose naturally. If P is the set of all the primitive roots in a finite field, it is clear that P consists entirely of nonsquares. Is it possible to find an element a in the field such that the translation of P by a, $P+a$, consists of all squares or of all nonsquares?

These two questions are related in the context of the following theorem which is the main result of this paper.

THEOREM. *Let $F(x)$ be any polynomial with integer coefficients. Let $K(F(x))$ be the set of all prime numbers $p \neq 2$ such that $F(x)$ does not reduce to one of the forms modulo p:*

$$\alpha[g(x)]^2\,, \quad or \quad \alpha x[g(x)]^2\,.$$

Then, for all but finitely many primes in $K(F(x))$, $F(x)$ represents a quadratic residue at a primitive element modulo p. If $F(x)$ is square free, $F(x)$ represents both nonzero quadratic residues and quadratic nonresidues at the primitive elements.

As a result of this theorem, we will see that the question posed by Moshe Rosenfeld may be completely answered. Also, we will see that the primitive elements of a finite field can be linearly translated into the set of quadratic residues or the quadratic nonresidues only if the field is $GF(3)$, $GF(5)$ or $GF(7)$.

2. Let k be a finite field, if $f(x) \in k[x]$ and $f(x)$ is of one of the forms:

$$\alpha[g(x)]^2 \quad \text{or} \quad \alpha x[g(x)]^2\,,$$

then $\{f(\beta) \mid \beta \in k$ is a primitive root and $f(\beta) \neq 0\}$ is certainly contained either in the set of all quadratic residues or in the set of all quadratic nonresidues. Thus if we expect to prove that a polynomial $F(x)$ with integer coefficients represents both squares and nonsquares at the primitive roots of a finite field, we need first insist $F(x)$ does not reduce to one of these two forms. For this reason we must introduce the set $K(F(x))$ defined in the statement of the theorem in the first section. In this section, we will find sufficient conditions on the finite field k to assure that any polynomial $f(x) \in k[x]$ of fixed degree which does not have one of the two excluded forms represents a quadratic residue at a primitive element of k.

First we note that it is sufficient to establish conditions on the field k which guarantee that, given any polynomial $f(x)$ of fixed degree, there exists a primitive root $\alpha \in k$ such that $f(\alpha)$ is a nonzero quadratic residue, for, in this case, not only will the polynomial $f(x)$ represent a square at a primitive root but so will the polynomial $\beta f(x)$ where β is any nonresidue in k.

Let k be a finite field with $|k| = p^n$ where p is an odd prime. We begin with a simple result concerning the primitive roots of k.

LEMMA 1. *If s and t are relatively prime integers such that a prime q divides st if and only if q divides $p^n - 1$, then for any primitive root $\alpha \in k$, the element $\alpha^t\beta^s$ is also primitive exactly*

$$\frac{\phi(t)(p^n - 1)}{t}$$

times as β runs through all the non-zero elements of k. ($\phi(t)$ denotes *the Euler ϕ-function.)*

Proof. Since α is primitive and β is nonzero, we can write $\beta = \alpha^{\ell}$, with $0 \leqq \ell \leqq p^n - 1$. By the conditions on s and t, we see that $(t + s\ell, p^n - 1) = 1$ if and only if $(\ell, t) = 1$.

As ℓ runs through the integers $0 \leqq \ell < p^n - 1$, the number of times ℓ is relatively prime to t is exactly $\phi(t)(p^n - 1)t^{-1}$.

LEMMA 2. *If $f(x) \in k[x]$ is square free with nonzero constant term, and if s and t are chosen as in Lemma 1, then $f(\alpha^t x^s)$ is also square free.*

Proof. Consider the formal derivative of $g(x) = f(\alpha^t x^s)$, viz., $g'(x) = \alpha^t s x^{s-1} f'(\alpha^t x^s)$. Since s divides $p^n - 1$, $g'(x)$ is not identically 0. Also, since x does not divide $f(x)$, we have $(g(x), g'(x)) = (f(\alpha^t x^s), f'(\alpha^t x^s))$. However, if this is not one, then there exists a common root $\gamma \in \bar{k}$, the algebraic closure of k. This in turn implies $\alpha^t \gamma^s$ is a common root $f(x)$ and $f'(x)$. This contradicts the assumption that $f(x)$ is square free.

As an immediate consequence of this lemma, we see that the polynomial $y^2 - f(\alpha^t x^s)$ is irreducible over the rational function field $\bar{k}(x)$. Thus we know that the algebraic function field K, where

$$K = k(x, y) \; ; \qquad y^2 = f(\alpha^t x^s) \; ,$$

has k for its exact field of constants. That is, K is a hyperelliptic function field of genus

$$g = \begin{cases} \dfrac{rs}{2} - 1 \; , & \text{if } rs \text{ is even} \\[2ex] \dfrac{rs - 1}{2} \; , & \text{if } rs \text{ is odd} \; , \end{cases}$$

where $r = \deg f(x)$.

Our next task is to find bounds on the number of prime divisors of degree one in K. The first bound is obtained by Weil's theorem (the Riemann hypothesis for congruence function fields). This famous result states that N_1, the number of primes of degree one in a congruence function field of genus g over a field of constants with p^n elements, satisfies

$$|N_1 - (p^n + 1)| \leqq 2gp^{n/2} \; .$$

Thus in our case, the number of primes of degree one in K satisfies

$$|N_1 - (p^n + 1)| \leqq \begin{cases} (rs - 2)p^{n/2} \; , & \text{if } rs \text{ is even} \\ (rs - 1)p^{n/2} \; , & \text{if } rs \text{ is odd} \; . \end{cases}$$

On the other hand, a prime of degree one in K must lie over a prime of degree one in $k(x)$. The prime divisors of degree one in $k(x)$ are those divisors associated with linear polynomials $x - \beta$, $\beta \in k$, and the divisor associated with the degree map. The factorization of primes in a quadratic extension of $k(x)$ is exactly analogous to the factorization of rational primes in quadratic extensions of the rational numbers [2]. Thus we have:

A The prime divisor of $k(x)$ associated with $x - \beta$:

(i) ramifies in $K \Leftrightarrow f(\alpha^t \beta^s) = 0$.

(ii) splits in $K \Leftrightarrow f(\alpha^t \beta^s)$ is a nonzero square in k.

(iii) remains inert in $K \Leftrightarrow f(\alpha^t \beta^s)$ is a nonsquare.

B The prime divisor of $k(x)$ associated with the degree map (the infinite prime):

(i) ramifies in $K \Leftrightarrow \deg f(\alpha^t x^s)$ is odd.

(ii) splits in $K \Leftrightarrow \deg f(\alpha^t x^s)$ is even and has a square as the leading coefficient.

(iii) remains inert in $K \Leftrightarrow \deg f(\alpha^t x^s)$ is even and has a nonsquare as the leading coefficient.

A prime of degree one of k lies over a prime of degree one in $k(x)$ which does not remain inert. We may now give conditions under which a polynomial $f(x)$ represents a square at a primitive element of k.

THEOREM 1. *Let k be a field with p^n elements. If s and t are integers such that:*

(i) $(s, t) = 1$,

(ii) *the prime q divides $p^n - 1 \Leftrightarrow q$ divides st, and*

(iii) $2\phi(t)/t > 1 + (rs - 2)p^{n/2}/(p^n - 1) + 2/(p^n - 1)$,

then, given any polynomial $f(x) \in k[x]$ of degree r, square free, and with nonzero constant term, there exists a primitive root $\gamma \in k$ such that $f(\gamma)$ is either zero or a perfect square in k.

Proof. By Lemma 1 we see that $\alpha^t \beta^s$ is *not* a primitive root exactly

$$\ell = (p^n - 1) - \frac{\phi(t)(p^n - 1)}{t}$$

times as β runs through the nonzero elements of k. Let $\{\beta_1, \beta_2, \cdots, \beta_\ell\}$ be those β such that $\alpha^t \beta^s$ is not primitive. Now if all the prime divisors $x - \beta_i$ associated with these elements of k were to split in K, then this would account for exactly 2ℓ primes of degree one in K. Further, if the primes associated with x and the infinite prime were also split in K, they would account for four more primes of degree one in K. If we knew that $N_1 > 2\ell + 4$, then K would have more primes of degree one than could possibly lie over the infinite prime, the prime x and the primes $x - \beta_i$ alone. That is, there must be a $\beta \in k$ such that $\gamma = \alpha^t \beta^s$ is primitive and $x - \beta$ splits or ramifies in K. Thus γ is a primitive root in k and $f(\gamma)$ is either zero or a square in k.

One can easily see that condition (iii) is equivalent to

$$(p^n + 1) - (rs - 2)p^{n/2} > 2\left[(p^n - 1) - \frac{\phi(t)(p^n - 1)}{t}\right] + 4 .$$

However, if s is chosen to be even (as it must be to satisfy all three conditions), the Riemann hypothesis states

$$N_1 \geqq (p^n + 1) - (rs - 2)p^{n/2} .$$

The theorem is proved.

We now note that if the polynomial $f(x)$ is known to have r_1 primitive roots as zeros, then these r_1 primitive roots account for at most sr_1 elements β such that $f(\alpha^t\beta^s) = 0$. The primes $x - \beta$ associated with these sr_1 elements must all ramify in K accounting for at most sr_1 primes of degree one in K. Thus, if condition (iii) in the theorem were changed to

$$\frac{2\phi(t)}{t} > 1 + \frac{(rs - 2)p^{n/2}}{p^n - 1} + \frac{(r_1 s + 2)}{p^n - 1} ,$$

then there would exist a primitive root $\gamma \in k$ such that $f(\gamma)$ is a nonzero square. In fact since $r_1 \leqq r$ we can state the following:

COROLLARY 1. *Let k be a field with p^n elements; if s and t are integers such that*

(i) $(s, t) = 1$.

(ii) *The prime q divides $p^n - 1 \Leftrightarrow q$ divides st, and*

(iii) $2\phi(t)/t > 1 + (rs - 2)p^{n/2}/(p^n - 1) + (rs + 2)/(p^n - 1)$,

then, given any polynomial $f(x) \in k[x]$ of degree r, square free and with nonzero constant term, there exists a primitive root $\gamma \in k$ such that $f(\gamma)$ is a nonzero square in k.

3. In this section we will prove that for all but finitely many fields k, one can find integers s and t satisfying the three conditions of the corollary to Theorem 1. To this end we prove a few technical lemmas.

Let $\{q_1, q_2, q_3, \cdots, q_n, \cdots\}$ be any increasing sequence of primes with $q_1 = 2$; we then define the following functions with respect to this sequence:

$$d(n, m) = 2\Big(1 - \frac{1}{q_n}\Big)\Big(1 - \frac{1}{q_{n+1}}\Big) \cdots \Big(1 - \frac{1}{q_m}\Big),$$

$$c_r(n, m) = 2r\Big[\frac{q_1 q_2 \cdots q_{n-1}}{q_n q_{n+1} \cdots q_m}\Big]^{1/2}.$$

Also, we will let $k(m)$ denote the unique integer such that

$$d(k(m) - 1, m) \leqq 1 < d(k(m), m).$$

We now state:

LEMMA 3. *If* $m \geqq 2k(m) + 2$ *and* $q_m > 8r^2$, *then*

$$d(k(m) + 1, m) - c_r(k(m) + 1, m) > 1.$$

Proof. Consider $d(k(m) + 1, m)$; by definition

$$\begin{aligned} d(k(m) + 1, m) &= (1 - q_{k(m)}^{-1})^{-1} d(k(m), m) \\ &= (1 + (q_{k(m)} - 1)^{-1}) d(k(m), m) \qquad (1) \\ &\geqq 1 + (q_{k(m)} - 1)^{-1}. \end{aligned}$$

Now, we may estimate $c_r(k(m) + 1, m)$ by noticing that the fractions:

$$\frac{q_2}{q_{k(m)+1}}, \frac{q_3}{q_{k(m)+2}}, \cdots, \frac{q_{k(m)}}{q_{2k(m)-1}}$$

are all less than one. Therefore, since $m \geqq 2k(m) + 2$,

$$c_r(k(m) + 1, m) < 2r\Big[\frac{2}{q_{m-2} q_{m-1} q_m}\Big]^{1/2}.$$

However, since the sequence of primes is increasing $q_{k(m)} - 1 \leqq q_{m-2}$ and $q_{k(m)} - 1 \leqq q_{m-1}$; so we have

$$c_r(k(m) + 1, m) < \Big[\frac{8r^2}{q_m}\Big]^{1/2} \frac{1}{q_{k(m)} - 1} < \frac{1}{q_{k(m)} - 1}.$$

This together with inequality (1) proves the lemma.

LEMMA 4. *If* $\{q_1, q_2, \cdots, q_m, \cdots\}$ *is a sequence of primes with* $q_1 = 2$, *and if* m *is chosen so that* $q_{k(m)-1} \geqq 7$ *then* $2k(m) + 2 \leqq m$.

Proof. First we notice that it is sufficient to prove the result for the sequence of all primes, since one easily sees that the function $k_p(m)$ as defined for the sequence of all primes has the property that $k_p(m) \geqq k(m)$ for the k-function defined for any other sequence of primes.

We will prove the result by induction on m. The smallest value for m for which $q_{k(m)-1} \geqq 7$ is $m = 18$. This is true since, by the definition of $k(m)$, $d(k(m) - 1, m) \leqq 1$. This is equivalent to

$$d(k(m), m) \leqq (1 - q_{k(m)-1}^{-1})^{-1} \leqq \frac{7}{6},$$

since $q_{k(m)-1} \geqq 7$ implies $k(m) = 5$; computations show that the smallest m for which $d(5, m) \leqq 7/6$ is $m = 18$. In this case $2k(m) + 2 \leqq m$.

To provide the induction step we need only show that if $k(m + 1) = k(m) + 1$, then $k(m + 2) = k(m + 1)$. This would suffice since it would show that m would need to increase at least 2 in order to have $k(m)$ increase 1.

First we consider the assumption that $k(m + 1) = k(m) + 1$; by definition, we see that this implies $d(k(m), m + 1) \leqq 1$. But consider the following estimate of $d(k(m), m)$:

$$\begin{aligned} d(k(m), m) &= 2\Big(1 - \frac{1}{q_{k(m)}}\Big)\Big(1 - \frac{1}{q_{k(m)+1}}\Big) \cdots \Big(1 - \frac{1}{q_m}\Big) \\ &> 2\Big(1 - \frac{1}{q_{k(m)}}\Big)\Big(1 - \frac{1}{q_{k(m)} + 1}\Big) \cdots \Big(1 - \frac{1}{q_m}\Big), \end{aligned}$$

which we obtain by including all the integers between $q_{k(m)}$ and q_m. This in turn implies $d(k(m), m) > 2(q_{k(m)} - 1)/q_m$, or equivalently

$$d(k(m), m + 1) > \frac{2(q_{k(m)} - 1)}{q_m}\Big(1 - \frac{1}{q_{m+1}}\Big).$$

But we have assumed that $d(k(m), m + 1) \leqq 1$, so we have

$$2(q_{k(m)} - 1) < \Big(1 + \frac{1}{q_{m+1} - 1}\Big)q_m :$$

or equivalently,

$$2q_{k(m)} < q_m + \frac{q_m}{q_{m+1} - 1} + 2.$$

However, all the parts of this inequality are integers except the fraction which is positive and strictly less than one, so we may conclude,

$$2q_{k(m)} \leqq q_m + 2 \leqq q_{m+1}$$

since q_m and q_{m+1} are consecutive primes.

We have seen that the conditions of the lemma imply that $q_{m+1} \geqq 2q_{k(m)}$; we will use this to establish the inequality

$$(2) \qquad \Big(1 - \frac{1}{q_{k(m)}}\Big)^{-1}\Big(1 - \frac{1}{q_{m+1}}\Big)\Big(1 - \frac{1}{q_{m+2}}\Big) \geqq 1.$$

Suppose by way of contradiction that this were not true, then we would have

$$\left(1 - \frac{1}{q_{k(m)}}\right) > \left(1 - \frac{1}{q_{m+1}}\right)\left(1 - \frac{1}{q_{m+2}}\right) > \left(1 - \frac{1}{q_{m+1}}\right)^2 .$$

One easily sees that this implies

$$q_{m+1} < q_{k(m)} + \sqrt{q_{k(m)}^2 - q_{k(m)}} .$$

Of course this would imply $q_{m+1} < 2q_{k(m)}$, a contradiction.

Now we are assuming that $k(m+1) = k(m) + 1$, and we want to find $k(m+2)$. We know $k(m+1) = k(m) + 1$ implies $d(k(m), m+1) \leqq 1$, so clearly $d(k(m), m+2) \leqq 1$. So we need now show that $d(k(m)+1, m+2) > 1$;

$$\begin{aligned} d(k(m)+1, m+2) &= \left(1 - \frac{1}{q_{k(m)}}\right)^{-1} d(k(m), m)\left(1 - \frac{1}{q_{m+1}}\right)\left(1 - \frac{1}{q_{m+2}}\right) \\ &\geqq d(k(m), m) , \end{aligned}$$

by the inequality (2). However, by the definition of $k(m)$, we have $d(k(m)+1, m+2) > 1$; and this shows $k(m+2) = k(m) + 1$.

We shall find that those sequences $\{q_1, q_2, \cdots, q_m\}$ having the property that $m \leqq 2k(m) + 1$ will play an important role; for this reason we state:

LEMMA 5. *Let $\{2 = q_1, q_2, \cdots, q_m\}$ be a finite sequence of primes satisfying $m \leqq 2k(m) + 1$; then $m \leqq 9$ and $q_{k(m)-1} \leqq 5$. In fact it must satisfy one of the following*:

(i) $k(m) = 4$, $q_{k(m)-1} = 5$ *and* $m = 9$.
(ii) $k(m) = 3$, $q_{k(m)-1} = 5$ *and* $m \leqq 7$.
(iii) $k(m) = 3$, $q_{k(m)-1} = 3$ *and* $m \leqq 7$ *or*
(iv) $k(m) = 2$, $q_{k(m)-1} = 2$ *and* $m \leqq 5$.

Proof. By Lemma 4 and since $m \leqq 2k(m) + 1$, we must have $m \leqq 9$ and $q_{k(m)-1} \leqq 5$. This, of course, implies $k(m) \leqq 4$. It is an easy computation to verify that for the sequence of primes $k_p(m) = 2$, for $m \leqq 3$; $k_p(m) = 3$, for $4 \leqq m \leqq 8$ and $k_p(9) = 4$. As we have already pointed out $k(m) \leqq k_p(m)$. Thus if $k(m) = 4$, then $m = 9$ and $q_{k(m)} = 5$. Suppose $k(m) = 3$; since we have assumed $m \leqq 2k(m) + 1$, we have $m \leqq 7$. Similarly $k(m) = 2$ implies $m \leqq 5$.

Next we relate these lemmas to the problem at hand.

LEMMA 6. *If p^n is a prime power, then for any fixed integers t and s such that $s \geqq 2$, s divides $p^n - 1$ and $4(p^n - 1) \geqq rs \geqq 3$, we have*

$$\frac{(rs-2)p^{n/2}}{p^n - 1} \leqq \frac{rs}{(p^n - 1)^{1/2}} .$$

Proof. In this proof we will denote the greatest integer in x by $[|x|]$. First we note that the inequality in the lemma is equivalent to

$$4p^n \geqq \frac{r^2s^2}{rs-1} = rs + 1 + \frac{1}{rs-1} .$$

Now because $4p^n$ is an integer this is equivalent to

$$4p^n \geqq \left[\left|rs + 1 + \frac{1}{rs-1}\right|\right] + 1 .$$

Since $rs > 2$, we have the equivalent form

$$4p^n \geqq rs + 2 .$$

However, by assumption $4p^n \geqq rs + 4 > rs + 2$. Thus we see that the inequality in the lemma is equivalent to $4(p^n - 1) \geqq rs$, and this proves the lemma.

We are now ready to prove the main result of the paper.

THEOREM 2. *Let r be any positive integer; in all but finitely many finite fields k, for every polynomial $f(x) \in k[x]$ of degree r which is not of the form:*

$$\alpha[g(x)]^2 \quad or \quad \alpha x[g(x)]^2 ,$$

there exists a primitive root $\beta \in k$ such that $f(\beta)$ is a quadratic residue in k. If $f(x)$ is square free, then β can be found so that $f(\beta) \neq 0$.

Proof. As we pointed out earlier, the two forms listed must be excluded. We may assume without loss of generality that $f(x)$ is square free, since leaving out a square factor does not affect the validity of the conclusion. Also we may assume $f(x)$ has a nonzero constant term since if $f(x) = xg(x)$, one may replace $f(x)$ with the polynomial $\alpha g(x)$ where α is any nonsquare. Since we are interested only in the value of $f(x)$ at primitive roots β, this will not change the result since $\alpha g(\beta)$ or $\beta g(\beta)$ are either both residues or both not. Finally, after these reductions are made the polynomial in question must be a nonconstant function, since otherwise the original would have been of an excluded form.

Now let k be a finite field with $|k| = p^n$, and let $p^n - 1 = q_1^{a_1} q_2^{a_2} \cdots q_m^{a_m}$ be the prime factorization. If $f(x)$ is a square free polynomial of degree less than or equal to r with nonzero constant term, and if we can find s and t such that

(i) $(s, t) = 1$,

(ii) $st = q_1 q_2 \cdots q_m$,

(iii) $2\phi(t)/t \geqq 1 + (rs - 2)p^{n/2}/(p^n - 1) + (rs + 2)/(p^n - 1)$,
then, by the corollary to Theorem 1, we know that $f(x)$ represents a nonzero square at some primitive root in k. Our object is to show that such s and t exist for all but finitely many prime powers p^n.

Consider the finite sequence of increasing primes $\{2 = q_1, q_2, \cdots, q_m\}$. If $q_m > 8r^2$ and, $m \geqq 2k(m) + 2$ we know by Lemmas 3, 4 and 5 that

$$d(k(m) + 1, m) > 1 + c_r(k(m) + 1, m) .$$

But if we let $s = q_1 q_2 \cdots q_{k(m)}$ and $t = q_{k(m)+1} \cdots q_m$ we have

$$\frac{2\phi(t)}{t} = d(k(m) + 1, m) ;$$

$$\begin{aligned} c_r(k(m) + 1, m) &= 2r\left[\frac{q_1 q_2 \cdots q_{k(m)}}{q_{k(m)+1} q_{k(m)+2} \cdots q_m}\right]^{1/2} \\ &= \frac{2rs}{(q_1 q_2 \cdots q_m)^{1/2}} \\ &\geqq \frac{2rs}{(p^n - 1)^{1/2}} . \end{aligned}$$

We now wish to use Lemma 6; since s is even the condition $s \geqq 2$ is satisfied; also we may assume that $sr \geqq 3$ without loss of generality since the only excluded case would be $r = 1$; however, we will show that the inequality (iii) is satisfied for $r = 2$ and this will imply it is also true for $r = 1$. Finally, we are assuming that $q_m > 8r^2$, and this imples

$$4(p^n - 1) \geqq 4st \geqq 4sq_m > 32sr^2 > sr .$$

Thus all of the conditions of Lemma 6 are satisfied and we have

$$\frac{rs}{(p^n - 1)^{1/2}} \geqq \frac{(rs - 2)p^{n/2}}{(p^n - 1)} .$$

One can easily see that, if $p^n \geqq 7$ (which is always the case when $q_m \geqq 8r^2$), then

$$\frac{rs}{(p^n - 1)^{1/2}} \geqq \frac{(rs + 2)}{p^n - 1} .$$

Summing this up we see that, if $2k(m) + 2 \leqq m$ and $q_m > 8r^2$, then for $s = q_1 q_2 \cdots q_{k(m)}$ and $t = q_{k(m)+1} \cdots q_m$,

$$\begin{aligned} \frac{2\phi(t)}{t} &= d(k(m) + 1, m) \\ &\geqq 1 + c_r(k(m) + 1, m) \\ &\geqq 1 + \frac{2rs}{(p^n - 1)^{1/2}} \end{aligned}$$

$$\geqq 1 + \frac{(rs-2)p^{n/2}}{p^n - 1} + \frac{rs+2}{p^n - 1} .$$

We must now study those sequences of primes where these conditions are not met.

Let $\{2 = q_1, q_2, q_3, \cdots, q_m\}$ be any sequence of primes such that $q_m < 8r^2$; there are only finitely many such sequences. Consider all those prime powers p^n such that $p^n - 1 = q_1^{\alpha_1} q_2^{\alpha_2} \cdots q_m^{\alpha_m}$. If $s = q_1 q_2 \cdots q_{m-1}$ and $t = q_m$, one easily sees that for p^n large enough

$$\frac{2\phi(t)}{t} > 1 + \frac{(rs-2)p^{n/2}}{p^n - 1} + \frac{rs+2}{p^n - 1} .$$

Let us now consider those sequences where $m \leqq 2k(m) + 1$. By Lemma 5, we see $m \leqq 9$ and $q_{k(m)-1} \leqq 5$. We shall consider each of the four cases separately. In each case we shall show $2\phi(t)/t > 1 + \alpha$, $\alpha > 0$. Then, since

$$\frac{(rs-2)p^{n/2} + (rs+2)}{p^n - 1}$$

goes to zero as p^n goes to infinity, for almost all prime powers p^n, there exist s and t which satisfy the conditions (i), (ii) and (iii).

Case 1. $k(m) = 4$, $q_4 \geqq 7$ and $m = 9$, then

$$\frac{2\phi(t)}{t} \geqq 2\Big(1 - \frac{1}{7}\Big)\Big(1 - \frac{1}{11}\Big) \cdots \Big(1 - \frac{1}{23}\Big) \cong 1.227 .$$

Cases 2 *and* 3. $k(m) = 3$, $q_3 \geqq 5$, $m \leqq 7$, then

$$\frac{2\phi(t)}{t} \geqq 2\Big(1 - \frac{1}{5}\Big)\Big(1 - \frac{1}{7}\Big) \cdots \Big(1 - \frac{1}{17}\Big) \cong 1.083 .$$

Case 4. $k(m) = 2$, $q_3 \geqq 3$, $m \leqq 5$, then if $q_2 = 3$ or 5 we will set $s = 2q_2$ and use the same bounds obtained in Cases 2 and 3. Otherwise $q_2 \geqq 7$ and

$$\frac{2\phi(t)}{t} \geqq 2\Big(1 - \frac{1}{7}\Big)\Big(1 - \frac{1}{11}\Big)\Big(1 - \frac{1}{13}\Big)\Big(1 - \frac{1}{17}\Big) \cong 1.354 .$$

This completes the proof of the main theorem.

4. In this section we apply these results to the cases $r = 1$ and $r = 2$. These are the cases necessary to resolve the questions posed in the introduction.

First we consider the case $r = 2$.

LEMMA 7. *If* $p^n - 1 = q_1^{a_1} q_2^{a_2} \cdots q_m^{a_m}$ *with* $q_m \geqq 8 \cdot 2^2$, *then there exist* s *and* t *satisfying conditions* (i), (ii) *and* (iii) *of the corollary to Theorem* 1 *with* $r = 2$.

Proof. In the previous section, we saw that if $m \geqq 2k(m) + 2$ then such s and t do indeed exist. Therefore, we will assume that $m \leqq 2k(m) + 1$; this leads to the four cases of Lemma 5. In each case we will use the same procedure; we will prescribe a choice for s and use the conditions of each case to find a bound α so that $(2\phi(t)t^{-1} - 1) \geqq \alpha$. We will then be able to use the assumption $q_m \geqq 32$ to show that

$$\alpha > \frac{(2s-2)p^{n/2} + 2s + 2}{p^n - 1} . \tag{3}$$

Thus we see that the chosen s and an appropriate t satisfy the necessary conditions.

First we will deal with Case 1; namely, $k(m) = 4$, $m = 9$ and $q_9 \geqq 37$. One easily sees that such a sequence of primes must begin with $q_1 = 2$, $q_2 = 3$ and $q_3 = 5$. We will choose $s = 2 \cdot 3 \cdot 5$ and $t = q_4 q_5 \cdots q_9$. Now we see that

$$\begin{aligned} 2\frac{\phi(t)}{t} - 1 &\geqq 2\Big(1 - \frac{1}{7}\Big)\Big(1 - \frac{1}{11}\Big)\Big(1 - \frac{1}{13}\Big)\Big(1 - \frac{1}{17}\Big)\Big(1 - \frac{1}{19}\Big)\Big(1 - \frac{1}{37}\Big) - 1 \\ &\geqq 0.24801 . \end{aligned}$$

Thus p^n satisfies inequality (3) with $\alpha = .24801$ and $s = 30$, if and only if $p^n > 55190$. Suppose there is a prime power $p^n \leqq 55190$ that satisfies the conditions of this case, we know that $2 \cdot 3 \cdot 4 \cdot q_9$ divides $p_n - 1$ with $q_9 \geqq 37$. However, this would require $q_4 q_5 q_6 q_7 q_8 < 55190/2 \cdot 3 \cdot 5 \cdot 37 \leqq 50$; This is clearly not possible.

In the remaining three cases $k(m) \leqq 3$. Since p is an odd prime we know $q_1 = 2$ and we now consider the various possibilities for q_2. First $q_2 = 3$; this is a possibility in either of the last two cases of Lemma 5, and therefore we see that $m \leqq 7$. We will set $s = 2 \cdot 3$ and $t = q_3 q_4 \cdots q_m$; thus

$$\begin{aligned} 2\frac{\phi(t)}{t} - 1 &\geqq 2\Big(1 - \frac{1}{5}\Big)\Big(1 - \frac{1}{7}\Big)\Big(1 - \frac{1}{11}\Big)\Big(1 - \frac{1}{13}\Big)\Big(1 - \frac{1}{37}\Big) - 1 \\ &\geqq 0.11974 . \end{aligned}$$

Now p^n satisfies inequality (3) with $\alpha = 0.31734$ and $s = 6$, if and only if $p^n > 7207$. If we suppose $p^n \leqq 7207$, we see that $q_3 q_4 \cdots q_{m-1} < 7207/2 \cdot 3 \cdot 37 < 33$. If more than two primes appear in the product, this is not possible; so we have $m \leqq 4$. This allows us to improve the value we have for α, since now $t = q_3$ or $t = q_3 q_4$;

$$2\frac{\phi(t)}{t}-1 \geqq 2\Big(1-\frac{1}{5}\Big)\Big(1-\frac{1}{37}\Big)-1=0.5567\,.$$

In this case p^n satisfies (3), if and only if $p^n > 373$. Again $6q_m$ divides $p^n - 1$ with $q_m \geqq 37$, and we see $q_3 < 2$. This is not possible.

We use the same technique to study the case $q_2 = 5$. We choose $s = 2\cdot 5$ and $t = q_3 q_4 \cdots q_m$. Here we have $2\phi(t)/t - 1 \geqq 0.31734$, and p^n satisfies inequality (3) if and only if $p^n \leqq 3356$. This implies either $m = 4$ and $q_3 = 7$, or $m = 3$, both of these possibilities are taken care of in the same way.

Finally we consider the case $q_2 \geqq 7$. This immediately places us in Case 4 of Lemma 5; namely; $k(m) = 2$, $m \leqq 5$. Here we choose $s = 2$ and use the same technique as above to complete the proof.

So we have seen that given any finite sequence of primes with $q_m > 32$, we can choose an n such that when $s = q_1 q_2 \cdots q_n$ and $t = q_{n+1} q_{n+2} \cdots q_m$

$$\frac{2\phi(t)}{t} > 1 + \frac{(2s+2)(st+1)^{1/2}}{st} + \frac{2s+2}{st}\,. \tag{4}$$

It is clear that, if k is a finite field with $|k| = p^n$ and some prime larger than 32 divides $p^n - 1$, there exist s and t satisfying the three conditions of the corollary to Theorem 1 with $r = 2$.

We are now interested in finding those sequence $\{2 = q_1, q_2, q_3 \cdots q_m\}$ with $q_m < 32$ for which one cannot choose $s = q_1 q_2 \cdots q_n$ and $t = q_{n+1} q_{n+2} \cdots q_m$ and satisfy (4). A simple computer search of these finitely many sequences yields the following exceptional sequences

$$\{2\}\,,\ \ \{2,3\}\,,\ \ \{2,5\}\,,\ \ \{2,7\}\,,\ \ \{2,3,5\}\,,\ \ \{2,3,7\}\,,\ \ \{2,3,11\}\,,$$
$$\{2,3,13\}\,,\ \ \{2,3,5,7\}\,,\ \ \{2,3,5,11\}\ \text{ and }\ \{2,3,5,13\}\,.$$

Thus the three conditions of the corollary may be satisfied for all finite fields k such that the set of primes dividing $|k| - 1$ is not one of the above 11 exceptional cases.

The next step is to consider all those prime powers p^n where the primes dividing $p^n - 1$ are one of the exceptional cases. We consider each sequence separately. First we fix $s = q_1 q_2 \cdots q_n$ and $t = q_{n+1} q_{n+2} \cdots q_m$; then the inequality

$$\frac{2\phi(t)}{t} > 1 + \frac{2(s-1)x^{1/2}}{x-1} + \frac{2s+2}{x-1} \tag{5}$$

has but one variable x and is quadratic in $x^{1/2}$. We see that there is a constant K such that $x > K$ implies the inequality (5). In this way we are able to limit the prime powers p^n for which proper s and t do not exist. The inequality (5) corresponds to the inequality in the corollary to Theorem 1 with $r = 2$; we also check the inequalities

$$\frac{2\phi(t)}{t} > 1 + \frac{2(s-1)x^{1/2}}{x-1} + \frac{2}{x-1}, \tag{6}$$

which corresponds to the inequality of Theorem 1 with $r = 2$, and

$$\frac{2\phi(t)}{t} > 1 + \frac{(s-2)x^{1/2}}{x-1} + \frac{s+2}{x-1} \tag{7}$$

which corresponds to the inequality of the corollary with $r = 1$.

As an example we will look at the sequence $\{2, 3, 5\}$. When $s = 6$ and $t = 5$, inequality (5) is satisfied when $x - 1 > 30\cdot(10.82)$; inequality (6) is satisfied when $x - 1 > 30\cdot(9.55)$; inequality (7) is satisfied when $x - 1 > 30\cdot(1.75)$. Choosing $s = 2$ and $t = 3\cdot 5$, these inequalities are satisfied when, respectively, $x - 1 > 30\cdot(35.80)$; $x - 1 > 30\cdot(32.033)$ and $x - 1 > 30\cdot(1.033)$. As we see the best results occur when $s = 6$ and $t = 5$. Since we are assuming that 30 divides $p^n - 1$ we see that only a few extra powers of the primes can be added with the result not satisfying the inequalities. Thus we see that the only possible exceptional factorizations of $p^n - 1$ are: $2\cdot 3\cdot 5$ which does not satisfy any inequality; $2^2\cdot 3\cdot 5$, $2^3\cdot 3\cdot 5$, $2^4\cdot 3\cdot 5$, $2\cdot 3^2\cdot 5$, $2^2\cdot 3^2\cdot 5$, $2\cdot 3^3\cdot 5$ and $2\cdot 3\cdot 5^2$ which do not satisfy (6) or (7), but do satisfy (5); and $2^2\cdot 3\cdot 5^2$ which does not satisfy (7) but does satisfy (5) and (6).

Analysing all 11 exceptional sequences in this way we obtain the following chart of possible factorizations of $p^n - 1$ that do not satisfy the inequality for any s and t:

TABLE 1

Factorizations that do not satisfy (5), (6) or (7)	$2\cdot 3\cdot 5$, $2\cdot 3$, 2^2, 2
Factorizations that do not satisfy (6) or (7)	$2\cdot 3\cdot 5\cdot 11$, $(2\cdot 3\cdot 4\cdot 13)$, $2\cdot 3\cdot 5\cdot 7$, $2^2\cdot 3\cdot 5\cdot 7$, $2\cdot 3^2\cdot 5\cdot 7$, $2\cdot 3\cdot 13$, $2\cdot 3\cdot 11$, $2\cdot 3\cdot 7$, $(2^2\cdot 3\cdot 7)$, $2^3\cdot 3\cdot 7$, $2\cdot 3^2\cdot 7$, $2^2\cdot 3\cdot 5$, $2^3\cdot 3\cdot 5$, $2^4\cdot 3\cdot 5$, $(2\cdot 3^2\cdot 5)$, $2^2\cdot 3^2\cdot 5$, $2\cdot 3^3\cdot 5$, $2\cdot 3\cdot 5^2$, $2\cdot 5$, $2^2\cdot 3$, $2^3\cdot 3$, $2^4\cdot 3$, $2^2\cdot 3^2$, $2\cdot 3^2$, 2^3
Factorizations that do not satisfy (7)	$(2^2\cdot 3\cdot 11)$, $(2^2\cdot 3\cdot 5^2)$, $(2^2\cdot 5)$, $(2\cdot 3^3)$, $(2\cdot 7)$.

Those factorizations in parenthesis are not prime powers minus 1. We may now state the following theorems and corollaries:

THEOREM 3. *If k is a finite field of odd characteristic with $|k| \notin A$, then every square free quadratic polynomial in $k[x]$ represents a nonzero square in k at some primitive root in k, where*

$$A = \{3, 5, 7, 9, 11, 13, 19, 25, 31, 37, 43, 49, 61, 67, 79, 121, \\ 127, 151, 169, 181, 211, 241, 271, 331, 421, 631\}\ .$$

REMARK. The set A consists of those prime powers for which the techniques of this paper do not work. There may be elements in A for which the result is valid.

COROLLARY. *If k is a finite field of odd characteristic with $|k| \notin A$, then every square free quadratic polynomial in $k[x]$ represents both nonzero squares and nonsquares at the primitive roots in k.*

COROLLARY. *If k is any finite field of characteristic $\neq 2$ or 3 then there exists a primitive root $\alpha \in k$ such that $-(\alpha^2 + \alpha + 1) = \beta^2$ for some $\beta \in k$.*

Proof. If char $k = 3$, then $-(x^2 + x + 1) = -(x - 1)^2$ which is an excluded form. For char $k \neq 2, 3$ one simply checks the fields $GF(p^n)$ with $p^n \in A$.

THEOREM 4. *If k is a finite field of odd characteristic with $|k| \neq 3$, 5 or 7 then every linear polynomial with nonzero constant term in $k[x]$ represents a square at a primitive root of k.*

COROLLARY. *If k is a finite field and P is the set of primitive roots in k, then only in the fields $k = GF(3)$, $GF(5)$ and $GF(7)$ can one find nonzero $a \in k$ such that $P + a$ consists entirely of squares or entirely nonsquares in k.*

The authors would like to thank Robert Dillon and Lee Appelbaum for their invaluable aid in doing the calculations necessary for this paper. In particular, Robert Dillon made an observation which was critical in the approximation of $d(n, m) - c_r(n, m)$.

REFERENCES

1. Alspach, Heinrich, and Rosenfeld, *Some graph decompositions and related designs*, submitted.

2. Helmut Hasse, *Theorie der relative-zyklischen algebraischen Funktionenkorper, insbesondere bei endlichem Konstanterkorper*, J. Reine Angew. Math., **172** (1935), 37–45.

Received May 10, 1980.

UNIVERSITY OF ARIZONA
TUSCON, AZ 85721