Counting Irreducibility-Preserving Substitutions for Polynomials over Finite Fields

Paul Pollack

Abstract

Let n be a positive integer and let $f_1(T), \dots, f_r(T)$ be pairwise nonassociated irreducible polynomials over a finite field $\mathbf{F}_q$ with the degree of $f_1 \cdots f_r$ bounded by B. We show that the number of univariate monic polynomials h of degree n for which all of $f_1(h(T)), \dots, f_r(h(T))$ are irreducible over $\mathbf{F}_q$ is $q^n/n^r + O_{n,B}(q^{n-1/2})$ provided $\gcd(q, 2n) = 1$. As an application, fix an infinite arithmetic progression $a \bmod m$ and fix pairwise nonassociated irreducibles $f_1(T), \dots, f_r(T)$ over $\mathbf{F}_p$ with the degree of $f_1 \cdots f_r$ bounded by B. If p is sufficiently large depending only on m, r, and B, then there are infinitely many monic polynomials $h(T)$ with $\deg h \equiv a \pmod{m}$ and all of $f_1(h(T)), \dots, f_r(h(T))$ irreducible over $\mathbf{F}_p$.

1. Introduction

Are there infinitely many primes of the form $n^2 + 1$? Questions of this type, where one inquires about the prime values of a polynomial (or the simultaneous prime values of a finite collection of polynomials) have received considerable attention, especially since the development of sieve methods in the early 20th century. Yet we still cannot prove the existence a single polynomial of degree > 1 that assumes prime values infinitely often.

In 1923, Hardy & Littlewood [HL23] formulated quantitative predictions for the number of simultaneous prime values assumed on integers $n \leqslant x$ for several specific families of polynomials. A general prediction for all finite collections of polynomials was later given by Bateman & Horn [BH62]; roughly speaking, the number of such n is conjectured to be governed by a global factor predicted by the density of primes, multiplied by a local factor depending on the number of solutions of our polynomials modulo p for all primes p.

In light of the strong analogies between the ring of integers and the ring of polynomials in one variable over a finite field, it is natural to wonder if similar conjectures can be formulated in the polynomial context. This is indeed the case: the following is one plausible analogue of the Hardy-Littlewood/Bateman-Horn conjectures:

Conjecture 1 (A Hardy-Littlewood Conjecture for Polynomials over $\mathbf{F}_q$). *Let $f_1, \dots, f_r$ be nonassociated irreducible one-variable polynomials over $\mathbf{F}_q$. Suppose that there is no prime π of $\mathbf{F}_q[T]$ for which the map*

$$h(T) \mapsto f_1(h(T)) \cdots f_r(h(T)) \bmod \pi$$

is identically zero. Then there are infinitely many monic $h(T)$ for which all of $f_1(h(T)), \dots, f_r(h(T))$

2000 Mathematics Subject Classification Primary: 11T55, Secondary: 11N32

Keywords: Finite fields, Hardy-Littlewood conjectures, Irreducible polynomials, Twin prime polynomials

The author is supported by an NSF Graduate Research Fellowship.

are simultaneously irreducible over $\mathbf{F}_q$. *Moreover,*

$$\#\{h(T) : h \text{ monic}, \;\deg h = n, \;\text{and } f_1(h(T)), \dots, f_r(h(T)) \text{ are all prime}\} \sim \mathfrak{S}(f_1, \dots, f_r)\frac{1}{\prod_{i=1}^{r}\deg f_i}\frac{q^n}{n^r} \quad \text{as } n \to \infty.$$

Here the local factor $\mathfrak{S}(f_1, \dots, f_r)$ *is defined by*

$$\mathfrak{S}(f_1, \dots, f_r) := \prod_{n=1}^{\infty} \prod_{\substack{\deg \pi = n \\ \pi \text{ monic prime of } \mathbf{F}_q[T]}} \frac{1 - \omega(\pi)/q^n}{(1 - 1/q^n)^r},$$

where

$$\omega(\pi) := \#\{a \bmod \pi : f_1(a) \cdots f_r(a) \equiv 0 \pmod{\pi}\}.$$

Remarks. We make two remarks about the behavior of $\mathfrak{S}(f_1, \dots, f_r)$, deferring their proofs to §2.

i) Under the hypotheses of Conjecture 1, the product defining $\mathfrak{S}(f_1, \dots, f_r)$ converges to a nonzero constant.

ii) If the sum of the degrees of the f_i is bounded, then the ratio $\mathfrak{S}(f_1, \dots, f_r)/\prod_{i=1}^{r}\deg f_i$ tends uniformly to 1 as q tends to infinity. This observation will be useful in explaining the form of Theorem 2 below.

Conjecture 1 is the expected translation of the Hardy-Littlewood/Bateman-Horn prediction into the polynomial setting, except that we have been a bit conservative in our formulation by restricting ourselves to polynomials with coefficients from $\mathbf{F}_q$. A complete analogue of the Hardy-Littlewood conjectures would address prime specializations of polynomials with coefficients from $\mathbf{F}_q[u]$ (predicting, e.g., the frequency of polynomials h for which $h(u)$ and $h(u)^q + u$ are both prime in $\mathbf{F}_q[u]$). However, formulating a plausible conjecture in complete generality requires some care; simply translating the classical conjectures into the language of polynomials is no longer adequate. Indeed, the number of prime specializations of a single irreducible polynomial in $\mathbf{F}_q[u][T]$ may already display unexpected behavior if the polynomial is inseparable over $\mathbf{F}_q(u)$. The underlying issues here were brought to light and vigorously explored by Conrad, Conrad & Gross ([CCG06]; see also the survey [Con05]). We restrict our attention in this paper to Conjecture 1.

Let B denote an upper bound on the degree of the product $f_1 \cdots f_r$. Then Conjecture 1 provides a (predicted) asymptotic formula for fixed q and B valid as $n \to \infty$. It makes equally good sense to ask for asymptotics in other ranges of (q, n, B)-space, perhaps for a uniform conjecture. In this paper we make some progress in this direction by proving asymptotic results when q is large compared to n and B, subject to mild restrictions on the characteristic of $\mathbf{F}_q$. Our main result is as follows:

Theorem 2. *Let n be a positive integer. Let $f_1(T), \dots, f_r(T)$ be pairwise nonassociated irreducible polynomials over $\mathbf{F}_q$ with the degree of the product $f_1 \cdots f_r$ bounded by B. The number of univariate monic polynomials h of degree n for which all of $f_1(h(T)), \dots, f_r(h(T))$ are irreducible over $\mathbf{F}_q$ is* $q^n/n^r + O_{n,B}(q^{n-1/2})$ *provided* $\gcd(q, 2n) = 1$.

The dependence of the $O_{n,B}$-term here is explicit but unpleasant, and it would be interesting to improve this. Observe that there is no coefficient appearing in front of q^n/n^r in the estimate of Theorem 2. Referring to Remark (ii) above, we see that this is exactly what we would expect if a uniform version of Conjecture 1 holds.

Example. The polynomial $T^2 + 1$ is irreducible over $\mathbf{F}_q$ if and only if $q \equiv 3 \pmod 4$. By Theorem 2 (with $r = 1$) the number of h of a fixed degree $n \geqslant 1$ for which $h^2 + 1$ is irreducible is asymptotic to q^n/n, provided $q \to \infty$ through prime powers $3 \pmod 4$ satisfying $\gcd(q, 2n) = 1$. This prediction may be initially surprising: if h has degree n, then h^2+1 has degree $2n$, and a random polynomial of degree $2n$ is irreducible with probability roughly $1/(2n)$. So we obtain from Theorem 2 twice as many irreducible specializations as we might expect. But this naive expectation fails to take the local data into account; as remarked above, a uniform version of Conjecture 1 would explain the discrepancy. Alternatively, one can convince oneself that the estimate of Theorem 2 is reasonable by realizing that for $q \equiv 3 \pmod 4$, the polynomial h^2+1 is irreducible over $\mathbf{F}_q$ exactly when $h+i$ is irreducible over $\mathbf{F}_{q^2}$, and it is plausible that the latter should happen with probability about $1/n$.

Theorem 2 was inspired by the result of Effinger, Hicks, and Mullen [EHM02] that for each fixed $n \geqslant 1$ and every large enough finite field $\mathbf{F}_q$, one can find a pair of distinct monic irreducibles of degree n over $\mathbf{F}_q$ which differ only in their constant term. To see this, let $h(T)$ range over the polynomials of degree n with vanishing constant term, and let N_h denote the number of $a \in \mathbf{F}_q$ for which $h(T)-a$ is irreducible over $\mathbf{F}_q$. By Gauss's formula for the number of monic irreducibles of degree n (see, for example, [LN97, Theorem 3.25]), we have

$$\sum_h N_h = q^n/n + O(q^{n/2}/n),$$

so that by the Cauchy-Schwarz inequality,

$$\sum_h 1^2 \sum_h N_h^2 \geqslant \left(\sum_h N_h\right)^2 = q^{2n}/n^2 + O(q^{3n/2}/n^2),$$

and hence

$$\sum_h N_h^2 \geqslant q^{n+1}/n^2 + O(q^{n/2+1}/n^2).$$

But the left-hand side counts the number of ordered pairs of monic degree n irreducibles which differ at most in their constant term. Since the lower bound exceeds the number of trivial pairs once q is large enough compared to n, the result follows.

An averaging argument of this kind does not appear sufficient for the proof of Theorem 2. Instead we employ an explicit form of the Chebotarev density theorem. Our argument is similar in strategy to that used by Cohen [Coh70] and Ree ([Ree71], [Ree72]) to settle Chowla's conjecture [Cho66] on the existence of prime polynomials of the form $T^n + T + a$ modulo p for $p > p_0(n)$.

Under the hypotheses of Conjecture 1 we expect infinitely many irreducibility-preserving specializations. Surprisingly, this qualitative version of Conjecture 1 can be rigorously confirmed in many special cases, even if the asymptotic appears out of reach. The first to make significant progress in this direction was Hall [Hal06], who showed that there are infinitely many monic twin prime pairs $f, f+1$ over all finite fields $\mathbf{F}_q$ with more than two elements (excepting $\mathbf{F}_3$, which was later treated by the present author [Pol06, Theorem 1]). Generalizing the work of Hall, the author recently established the following result (cf. [Pol06, Theorem 2]):

Theorem A. *Let $f_1(T), \dots, f_r(T)$ be pairwise nonassociated irreducible polynomials over $\mathbf{F}_q$ with the degree of $f_1 \cdots f_r$ bounded by B. If $q \geqslant 2^{2r}(1+B)^2$, then there is a prime l dividing $q-1$ and an element $\beta \in \mathbf{F}_q$ for which every substitution*

$$T \mapsto T^{l^k} - \beta \quad \text{with} \quad k = 1, 2, 3, \dots$$

leaves all of $f_1, \dots, f_r$ irreducible. In particular, there are infinitely many h as in Conjecture 1.

In both Hall's original theorem and in Theorem A, the set of substitutions $T \mapsto h(T)$ leaving all the f_i irreducible form a sparse set. A weak consequence of Conjecture 1 is that there should be such irreducibility-preserving substitutions $h(T)$ of every sufficiently large degree. Here we establish that the degrees of the permissible substitutions are "dense" with respect to arithmetic progressions, in the following sense:

Theorem 3. *Let $f_1(T), \dots, f_r(T)$ be pairwise nonassociated irreducibles over $\mathbf{F}_q$ with the degree of $f_1 \cdots f_r$ bounded by B. Let $a \bmod m$ be an arbitrary infinite arithmetic progression of integers. If the finite field $\mathbf{F}_q$ is sufficiently large, depending just on m, r, and B, and if q is prime to $2\gcd(a,m)$, then there are infinitely many univariate monic polynomials h over $\mathbf{F}_q$ with*

$$\deg h \equiv a \pmod m \quad \text{and} \quad f_1(h(T)), \dots, f_r(h(T)) \text{ all irreducible over } \mathbf{F}_q.$$

This result is most satisfactory in the case of prime fields, since the restriction that q be coprime to $2\gcd(a,m)$ is satisfied for all sufficiently large primes q. Probably Theorem 3 remains true without any restriction on the characteristic of $\mathbf{F}_q$, but we have not been able to show this.

Our proof of Theorem 3 is completely effective. We illustrate our methods with the following result, the first half of which settles a problem posed by Hall [Hal06, p. 140]:

Theorem 4. *Let $\mathbf{F}_q$ be any finite field with more than two elements. Then there are infinitely many monic prime pairs $f, f+1$ of odd degree over $\mathbf{F}_q$. The same holds for the case of even degree.*

Even for large q this is not immediate from Theorem 3, since that theorem says nothing about prime specializations over fields of characteristic 2.

Theorem 4 is an analogue of Kornblum's result that every coprime residue class of polynomials over $\mathbf{F}_q$ contains infinitely many monic irreducibles of odd degree, as well as infinitely many of even degree. In the posthumously-published version of Kornblum's paper [Kor19], Landau proved the more general theorem that the degrees can be taken from an arbitrary arithmetic progression. Theorem 3 can be seen as an effort in the same direction.

2. Analysis of the Local Factor

Here we justify the remarks following Conjecture 1. Proposition 5 vindicates our first remark, and Proposition 6 establishes the second in a more precise form.

Proposition 5. *Let $f_1, \dots, f_r$ be pairwise nonassociated irreducibles over $\mathbf{F}_q$. Suppose that as in Conjecture 1 their product $f_1 \cdots f_r$ has no fixed prime divisor. Then the product defining $\mathfrak{S}(f_1, \dots, f_r)$ converges to a positive constant.*

Proposition 6. *Let $f_1, \dots, f_r$ be pairwise nonassociated irreducibles over $\mathbf{F}_q$ with the degree of $f_1 \dots f_r$ bounded by B. If $q \geqslant 2B^2$, then*

$$\frac{1}{\prod_{i=1}^r \deg f_i} \mathfrak{S}(f_1, \dots, f_r) = 1 + O(B/q^{1/2}),$$

where the implied constant is absolute.

The proofs of both propositions are based on the following technical lemma:

Lemma 7. *Let $f_1, \dots, f_r$ be pairwise nonassociated irreducibles over $\mathbf{F}_q$. For π a prime of $\mathbf{F}_q[T]$, let $\omega(\pi)$ denote the number of roots of $f_1 \cdots f_r$ modulo π, and for each $i = 1, 2, \dots, r$, let $\omega_i(\pi)$ denote the number of roots of f_i modulo π. Suppose that B is an upper bound for the degree of $f_1 \cdots f_r$. Then*

$$\log \prod_{n=N_0}^{N_1} \prod_{\deg \pi = n} \left(1 - \frac{1}{q^n}\right)^{-r} = r \sum_{n=N_0}^{N_1} \frac{1}{n} + O\left(\frac{B}{N_0 q^{N_0/2}}\right) \tag{1}$$

for all positive integers $N_0 < N_1$. Moreover, if $q^{N_0} \geqslant 2B$, then

$$\log \prod_{n=N_0}^{N_1} \prod_{\deg \pi = n} \left(1 - \frac{\omega(\pi)}{q^n}\right) = \\ - \left(\deg f_1 \sum_{\substack{n=N_0 \\ \deg f_1 \mid n}}^{N_1} \frac{1}{n} + \dots + \deg f_r \sum_{\substack{n=N_0 \\ \deg f_r \mid n}}^{N_1} \frac{1}{n}\right) + O\left(\frac{B}{N_0 q^{N_0/2}}\right) + O\left(\frac{B^2}{N_0 q^{N_0}}\right). \quad (2)$$

All implied constants here are absolute.

Proof. The left hand side of (1) is given by

$$-r \sum_{n=N_0}^{N_1} \sum_{\deg \pi = n} \log(1 - 1/q^n) = -r \sum_{n=N_0}^{N_1} \sum_{\deg \pi = n} \left(-\frac{1}{q^n} + O\left(\frac{1}{q^{2n}}\right)\right).$$

Inserting the estimate $q^n/n + O(q^{n/2}/n)$ for the number of monic irreducibles of degree n, this simplifies to

$$r \sum_{n=N_0}^{N_1} \frac{1}{n} + O\left(r \sum_{n=N_0}^{N_1} \frac{1}{nq^n} + r \sum_{n=N_0}^{N_1} \frac{1}{nq^{n/2}}\right).$$

The error term is $O(r/(N_0 q^{N_0/2}))$; since r is bounded by B, this proves (1).

The proof of (2) is similar but a bit more involved. Since $q^{N_0} \geqslant 2B$, we have $\omega(\pi)/q^n \leqslant 1/2$ for any prime π of $\mathbf{F}_q[T]$ of degree $n \geqslant N_0$. As a consequence, we may write the left hand side of (2) as

$$-\sum_{n=N_0}^{N_1} \sum_{\deg \pi = n} \left(\frac{\omega(\pi)}{q^n} + O\left(\frac{B^2}{q^{2n}}\right)\right).$$

The O-term here is

$$\ll \sum_{n=N_0}^{N_1} \frac{B^2}{q^{2n}} \frac{q^n}{n} \ll B^2 \frac{1}{N_0 q^{N_0}}. \quad (3)$$

To evaluate the main term, we observe that since the f_i are pairwise coprime, we have $\omega(\pi) = \omega_1(\pi) + \dots + \omega_r(\pi)$. Moreover, $\omega_i(\pi)$ vanishes unless the degree of f_i, say d_i, divides the degree of π, in which case $\omega_i(\pi) = d_i$. With this information in hand, we can write the main term as

$$-\sum_{n=N_0}^{N_1} \sum_{\deg \pi = n} \frac{\omega(\pi)}{q^n} = -\left(d_1 \sum_{\substack{n=N_0 \\ d_1 \mid n}}^{N_1} \frac{1}{q^n} \sum_{\deg \pi = n} 1 + \dots + d_r \sum_{\substack{n=N_0 \\ d_r \mid n}}^{N_1} \frac{1}{q^n} \sum_{\deg \pi = n} 1\right).$$

For each $1 \leqslant i \leqslant r$, we have

$$\begin{aligned} d_i \sum_{\substack{n=N_0 \\ d_i \mid n}}^{N_1} \frac{1}{q^n} \sum_{\deg \pi = n} 1 &= d_i \sum_{\substack{n=N_0 \\ d_i \mid n}}^{N_1} \frac{1}{n} + O\left(d_i \sum_{n=N_0}^{N_1} \frac{1}{nq^{n/2}}\right) \\ &= d_i \sum_{\substack{n=N_0 \\ d_i \mid n}}^{N_1} \frac{1}{n} + O\left(\frac{d_i}{N_0 q^{N_0/2}}\right). \end{aligned}$$

Adding all these estimates (and keeping in mind the prior error term (3)) we obtain the main term of (2) with an error that is $\ll B/(N_0 q^{N_0/2}) + B^2/(N_0 q^{N_0})$, as claimed. $\square$

Proof of Proposition 5. Suppose that q and the f_i are fixed, and let d_i denote the degree of f_i as above. By (1) and (2), if $N_1 > N_0$ and N_0 is large enough to satisfy $q^{N_0} \geqslant 2B$, then we have

$$\log \prod_{n=N_0}^{N_1} \prod_{\deg \pi = n} \frac{(1-\omega(\pi)/q^n)}{(1-1/q^n)^r} = \\ -\left(d_1\left(\frac{1}{d_1}\sum_{N_0/d_1 \leqslant n \leqslant N_1/d_1} \frac{1}{n}\right) + \cdots + d_r\left(\frac{1}{d_r}\sum_{N_0/d_r \leqslant n \leqslant N_1/d_r} \frac{1}{n}\right)\right) + \\ r\sum_{n=N_0}^{N_1} \frac{1}{n} + O\left(\frac{B}{N_0 q^{N_0/2}} + \frac{B^2}{N_0 q^{N_0}}\right). \quad (4)$$

Since we have $\sum_{N_0/d_i \leqslant n \leqslant N_1/d_i} \frac{1}{n} = \log(N_1/N_0) + O(d_i/N_0)$ while $\sum_{N_0 \leqslant n \leqslant N_1} \frac{1}{n} = \log(N_1/N_0) + O(1/N_0)$, this simplifies to

$$-r\log(N_1/N_0) + r\log(N_1/N_0) + O\left(B/N_0 + r/N_0 + \frac{B}{N_0 q^{N_0/2}} + \frac{B^2}{N_0 q^{N_0}}\right) = O(B^2/N_0).$$

But in our situation B is fixed. It follows that (4) tends to zero as N_0 tends to infinity. This verifies that the sequence of logarithms of the partial products for the expression defining $\mathfrak{S}(f_1, \dots, f_r)$ is Cauchy, hence convergent. Consequently, the product defining $\mathfrak{S}(f_1, \dots, f_r)$ converges to a positive real number, as claimed. (Note that in order to know that the sequence of logarithms of the partial products is well-defined, we are implicitly using the condition that $f_1 \cdots f_r$ has no fixed prime divisor.) □

Proof of Proposition 6. We appeal to estimates (1) and (2) with $N_0 = 1$. Since $q \geqslant 2B^2$, the condition $q^{N_0} \geqslant 2B$ of Lemma 7 is certainly satisfied. Proceeding as in the proof of Proposition 5, we find

$$\log \prod_{n=1}^{N} \prod_{\deg \pi = n} \frac{(1-\omega(\pi)/q^n)}{(1-1/q^n)^r} = -\left(\sum_{n \leqslant N/d_1} \frac{1}{n} + \cdots + \sum_{n \leqslant N/d_r} \frac{1}{n}\right) + r\sum_{n \leqslant N} \frac{1}{n} + O\left(\frac{B}{q^{1/2}} + \frac{B^2}{q}\right).$$

Since $\sum_{n \leqslant N/d_i} \frac{1}{n} = \log(N/d_1) + \gamma + O(d_i/N)$ while $\sum_{n \leqslant N} \frac{1}{n} = \log N + \gamma + O(1/N)$, the last expression can be estimated as

$$-\log \frac{N^r}{d_1 \cdots d_r} + r\log N - r\gamma + r\gamma + O(B/N + r/N + B/q^{1/2} + B^2/q) = \\ \log d_1 \cdots d_r + O(B/N + B/q^{1/2}).$$

(Note that $B/q^{1/2} \geqslant B^2/q$ since $q \geqslant B^2$.) Letting N tend to infinity and exponentiating now gives the result. □

3. Preparation for the Proof of Theorem 2

3.1 Notation

We fix once and for all an algebraically closed field Ω_q of infinite transcendence degree over $\mathbf{F}_q$ and assume for the remainder of the paper that all extensions of $\mathbf{F}_q$ which appear are subfields of Ω_q. We use an overline to denote the operation of taking an algebraic closure; in particular, $\overline{\mathbf{F}}_q$ denotes the algebraic closure of $\mathbf{F}_q$ inside Ω_q.

We use res and disc to denote the polynomial resultant and discriminant, respectively. Our work also requires variants of these quantities, which we define as follows: If $f = \sum_{i=0}^{n} a_i u^i$ and

$g = \sum_{j=0}^{m} b_j u^j$ are polynomials in u of degrees *at most* n and m respectively over a domain R (so that a_n and b_m may vanish), we define

$$\mathrm{res}_u^{n,m}(f,g) := \mathrm{res}_u\left(\sum_{i=0}^{n} A_i u^i, \sum_{j=0}^{m} B_j u^j\right)\Bigg|_{A_0=a_0,\ldots,A_n=a_n,B_0=b_0,\ldots,B_m=b_m},$$

where the right-hand resultant is computed over the ring of polynomials $R[A_0,\ldots,A_n,B_0,\ldots,B_m]$ obtained by adjoining the indeterminates A_i and B_j to R. Similarly, if $f = \sum_{i=0}^{n} a_i T^i$ is a polynomial in T of degree at most n, we define

$$\mathrm{disc}_T^n(f) := \mathrm{disc}_T\left(\sum_{i=0}^{n} A_i T^i\right)\Bigg|_{A_0=a_0,\ldots,A_n=a_n},$$

the right-hand discriminant being taken over $R[A_0,\ldots,A_n]$. If n and m represent the actual degrees of f and g, respectively, then $\mathrm{res}_u^{n,m}(f,g) = \mathrm{res}_u(f,g)$, and similarly for $\mathrm{disc}_T^n(f)$. We work with $\mathrm{res}_u^{n,m}$ and disc_T^n rather than the usual resultant and discriminant in order to obtain uniform formulas without needing to worry about "degree-dropping" in intermediate calculations. The fundamental property of $\mathrm{res}_u^{n,m}$ that we need is that $\mathrm{res}_u^{n,m}(f,g)$ is an $R[u]$-linear combination of f and g. (This follows from our definitions above and the analogous result for the usual resultant.) In particular, if R is a field and $\mathrm{res}_u^{n,m}(f,g)$ is a nonzero constant, then f and g have no common roots in R.

We use $\mathrm{Sym}(S)$ to denote the symmetric group on the set S.

3.2 Further Preliminaries for the Proof of Theorem 2

Since the case $n = 1$ of Theorem 2 is trivial, we always suppose that $n \geqslant 2$. We also suppose the following setup:

$f_1,\ldots,f_r$	pairwise nonassociated irreducible univariate polynomials over $\mathbf{F}_q$,
$d_1,\ldots,d_r$	degrees of $f_1,\ldots,f_r$ respectively,
$\theta_1,\ldots,\theta_r$	fixed roots of $f_1,\ldots,f_r$, respectively, from $\overline{\mathbf{F}}_q$,
$\theta_i^{(j)}$	jth conjugate of θ_i with respect to Frobenius, i.e., $\theta_i^{(j)} := \theta_i^{q^j}$.

If h is a fixed polynomial of degree $n \geqslant 2$ over $\mathbf{F}_q$, we define the function fields $K_{i,j}/\mathbf{F}_q, L_{i,j}/\mathbf{F}_q$ and $M_i/\mathbf{F}_q$ (for $1 \leqslant i \leqslant r, 1 \leqslant j \leqslant d_i$) as follows, suppressing in our notation the dependence on h:

$K_{i,j}$	field obtained by adjoining a fixed root of $h(T) - u - \theta_i^{(j)}$ to $\mathbf{F}_{q^{d_i}}(u)$,
$L_{i,j}$	Galois closure of $K_{i,j}$ over $\mathbf{F}_{q^{d_i}}(u)$,
M_i	compositum of the fields $L_{i,j}$ for $j = 1, 2\ldots, d_i$.

We let D be the least common multiple of $d_1,\ldots,d_r$ and denote with a tilde the corresponding fields obtained by extending the constant field by $\mathbf{F}_{q^D}$. (That is, we set $\widetilde{K}_{i,j} := K_{i,j}\mathbf{F}_{q^D}, \widetilde{L}_{i,j} := L_{i,j}\mathbf{F}_{q^D}$ and $\widetilde{M}_i := M_i\mathbf{F}_{q^D}$.) Finally, we let $\widetilde{M}$ denote the compositum of $\widetilde{M}_1,\ldots,\widetilde{M}_r$. The inclusion relations between these fields are illustrated in Figures 1 and 2.

Lemma 8. *Assume that $h(T)$ is a polynomial of degree $n \geqslant 2$ over $\mathbf{F}_q$ which is not a polynomial in T^p, where p is the characteristic of $\mathbf{F}_q$. Then the extensions $M_i/\mathbf{F}_q(u)$ are Galois for each $i = 1, 2, \ldots, r$. The same assertion holds for the extensions $\widetilde{M}_i/\mathbf{F}_q(u)$ and $\widetilde{M}/\mathbf{F}_q(u)$.*

Proof. Observe that M_i is the splitting field over $\mathbf{F}_q(u)$ of $f_i(h(T) - u)$, so that the first half of the lemma follows immediately once we show that the irreducible factors of $f_i(h(T) - u)$ are separable

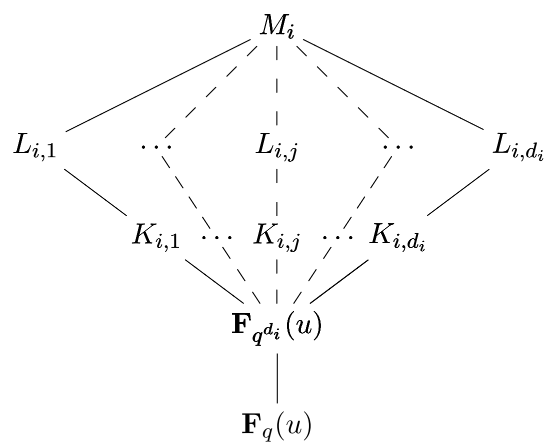

Figure 1: Tower of fields illustrating the inclusion relations between $\mathbf{F}_q(u), \mathbf{F}_{q^{d_i}}(u)$, the $K_{i,j}$, the $L_{i,j}$ and M_i.

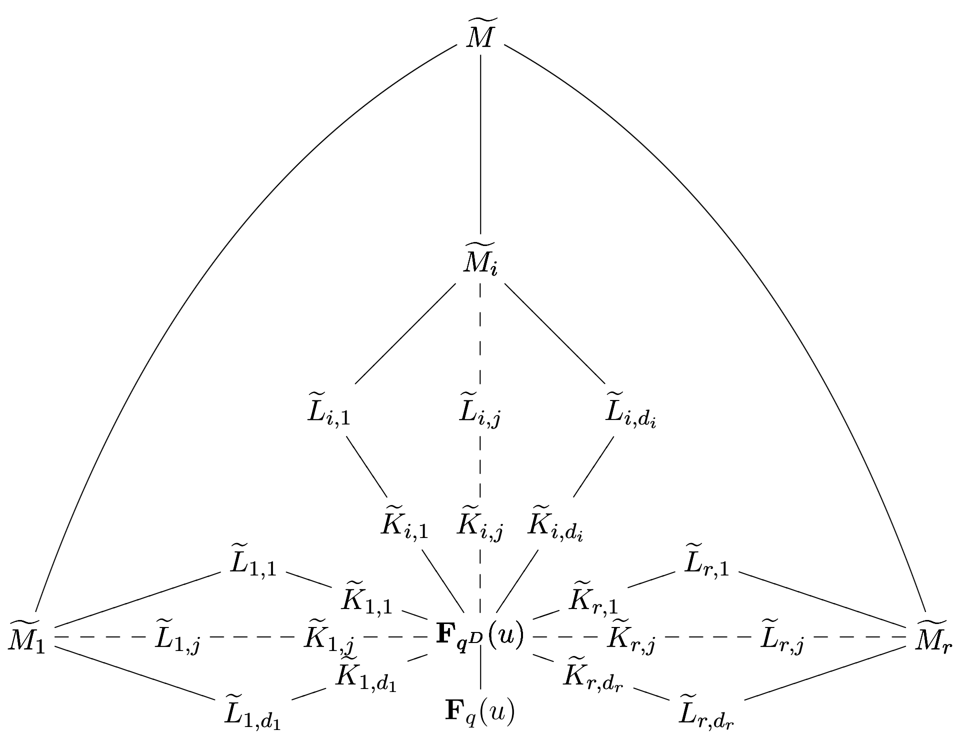

Figure 2: Field diagram illustrating the inclusion relations between $\mathbf{F}_q(u), \mathbf{F}_{q^D}(u)$, the $\widetilde{K}_{i,j}$, the $\widetilde{L}_{i,j}$, $\widetilde{M}_i$ and $\widetilde{M}$. Here moving to a larger field is signified by moving outward from $\mathbf{F}_q(u)$.

over $\mathbf{F}_q(u)$. Moving to the finite extension $\mathbf{F}_{q^{d_i}}(u)$ of $\mathbf{F}_q(u)$ we have

$$f_i(h(T)-u) = \prod_{j=1}^{d_i}(h(T)-u-\theta_i^{(j)}).$$

The d_i factors on the right-hand side are pairwise coprime (in $\overline{\mathbf{F}_q(u)}[T]$), so that it suffices to verify that each factor $h(T)-u-\theta_i^{(j)}$ has no repeated roots. Any such repeated root is also a root of $h'(T)$. But our hypothesis on h ensures that h' is not identically zero, so each root of $h'(T)$ is algebraic over $\mathbf{F}_q$, while $h(T)-u-\theta_i^{(j)}$ has no roots algebraic over $\mathbf{F}_q$.

The second half of the lemma is a consequence of the first. Indeed, since $\mathbf{F}_{q^D}(u)/\mathbf{F}_q(u)$ is Galois, what we have just proved implies that $\widetilde{M_i} = M_i\mathbf{F}_{q^D} = M_i\mathbf{F}_{q^D}(u)$ is also Galois over $\mathbf{F}_q(u)$, and thus so is the compositum of the $\widetilde{M_i}$. □

The groups $\mathrm{Gal}(\widetilde{M}/\mathbf{F}_q(u))$ and $\mathrm{Gal}(M_i/\mathbf{F}_q(u))$ will play an important role and so we study them in some detail. Let $S_{i,j}$ denote the full set of roots of $h(T)-u-\theta_i^{(j)}$ (thus $S_{i,j}$ depends only on $j \bmod d_i$). We begin by observing that under the hypothesis of Lemma 8, which assures that the extensions appearing below are Galois, we have for each $k=1,2,\dots,r$ a commutative diagram

$$\begin{array}{ccc} \mathrm{Gal}(\widetilde{M}/\mathbf{F}_q(u)) & \xrightarrow{\iota_1} & \mathrm{Gal}(\mathbf{F}_{q^D}/\mathbf{F}_q)\times\prod_{i=1}^r \mathrm{Sym}(\cup_{j=1}^{d_i} S_{i,j}) \\ {\scriptstyle \sigma\mapsto\sigma|_{M_k}}\big\downarrow & & \pi\big\downarrow \\ \mathrm{Gal}(M_k/\mathbf{F}_q(u)) & \xrightarrow{\iota_2} & \mathrm{Gal}(\mathbf{F}_{q^{d_k}}/\mathbf{F}_q)\times \mathrm{Sym}(\cup_{j=1}^{d_k} S_{k,j}) \end{array}. \tag{5}$$

Here the maps ι_1, ι_2 are given by

$$\iota_1 \colon \sigma \mapsto (\sigma|_{\mathbf{F}_{q^D}}, \sigma|_{\cup_{j=1}^{d_1} S_{1,j}}, \dots, \sigma|_{\cup_{j=1}^{d_r} S_{r,j}}),$$
$$\iota_2 \colon \sigma \mapsto (\sigma|_{\mathbf{F}_{q^{d_k}}}, \sigma|_{\cup_{j=1}^{d_k} S_{k,j}}),$$

and

$$\pi\colon (\tau,\sigma_1,\dots,\sigma_r)\mapsto(\tau|_{\mathbf{F}_{q^{d_k}}},\sigma_k).$$

Note that ι_1 and ι_2 are embeddings while π is a surjection.

The remainder of this section is devoted to an explicit description of the images of ι_1 and ι_2 under a mild restriction on h. This characterization is obtained under the following two hypotheses:

$$\mathrm{disc}_u^{n-1}\mathrm{disc}_T^n(h(T)-u-\theta_i^{(j)}) \neq 0 \quad \text{for all} \quad 1\leqslant i\leqslant r, \quad 1\leqslant j\leqslant d_i, \tag{6}$$

and

$$\mathrm{res}_u^{n-1,n-1}\left(\mathrm{disc}_T^n(h(T)-u-\theta_i^{(j)}), \mathrm{disc}_T^n(h(T)-u-\theta_{i'}^{(j')})\right) \neq 0$$
$$\text{whenever } i,i',j,j' \text{ are as above and } (i,j)\neq(i',j'). \tag{7}$$

(Note that (6) implies immediately that h is not a polynomial in T^p.) That together (6) and (7) impose only a mild restriction on h is borne out by the following lemma, which we prove in §4:

Lemma 9. *Let $h(T)$ range over the polynomials of the form $T^n + a_{n-1}T^{n-1}+\cdots+a_1T$, with all coefficients a_i belonging to $\mathbf{F}_q$. Assume that q is prime to $2n$. Then both of the following hold:*

i) *The number of such h for which (6) fails is bounded above by*

$$(2n-1)(2n-3)q^{n-2}. \tag{8}$$

ii) *For any fixed pairs of indices $(i,j)\neq(i',j')$, the same bound holds for the number of such h which fail to satisfy (7).*

Consequently, for all but at most

$$4n^2\left(1+\binom{d_1+\cdots+d_r}{2}\right)q^{n-2}$$

values of h as above, both (6) and (7) hold for all distinct pairs of indices (i,j) and (i',j').

We now present the promised descriptions of the images of ι_1 and ι_2, beginning with ι_2:

Lemma 10. *Let $n \geqslant 2$. Assume that the characteristic of $\mathbf{F}_q$ is prime to $2n$. Then if $h(T)$ has the form*

$$h(T) = T^n + a_{n-1}T^{n-1} + \cdots + a_1 T, \quad \text{with each } a_i \in \mathbf{F}_q,$$

and $h(T)$ satisfies both (6) and (7), then all of the following hold:

- i) *The $L_{i,j}$ are Galois over $\mathbf{F}_{q^{d_i}}(u)$ with Galois group $\mathrm{Sym}(S_{i,j})$ for each $1 \leqslant i \leqslant r, 1 \leqslant j \leqslant d_i$.*
- ii) *For every $1 \leqslant i \leqslant r, 1 \leqslant j \leqslant d_i$, the field $L_{i,j}$ is linearly disjoint from the compositum of all other fields $L_{i,j'}$ with $1 \leqslant j' \neq j \leqslant d_i$.*
- iii) *$\mathbf{F}_{q^{d_i}}$ is the full field of constants of $M_i/\mathbf{F}_{q^{d_i}}$.*
- iv) *The extension $M_i/\mathbf{F}_{q^{d_i}}(u)$ is Galois with*

$$\mathrm{Gal}(M_i/\mathbf{F}_{q^{d_i}}(u)) \cong \prod_{j=1}^{d_i} \mathrm{Gal}(L_{i,j}/\mathbf{F}_{q^{d_i}}(u)) \cong \prod_{j=1}^{d_i} \mathrm{Sym}(S_{i,j}),$$

  the first isomorphism being induced by restriction in each component.
- v) *Fix $1 \leqslant i \leqslant r$. Let* Frob *denote the qth power map, so that* Frob *generates* $\mathrm{Gal}(\mathbf{F}_{q^{d_i}}/\mathbf{F}_q)$. *The image of ι_2 consists of all pairs $(\mathrm{Frob}^k, \sigma)$ which obey the following compatibility condition:*

$$\sigma(S_{i,j}) \subset \sigma(S_{i,j+k}).$$

A similar lemma characterizes the image of ι_1:

Lemma 11. *Let $n \geqslant 2$. Assume that the characteristic of $\mathbf{F}_q$ is prime to $2n$. Then if $h(T)$ has the form*

$$h(T) = T^n + a_{n-1}T^{n-1} + \cdots + a_1 T, \quad \text{with each } a_i \in \mathbf{F}_q,$$

and $h(T)$ satisfies both (6) and (7), then all of the following hold:

- i) *The $\widetilde{L}_{i,j}$ are Galois over $\mathbf{F}_{q^D}(u)$ with Galois group $\mathrm{Sym}(S_{i,j})$ for each $1 \leqslant i \leqslant r, 1 \leqslant j \leqslant d_i$.*
- ii) *For every $1 \leqslant i \leqslant r, 1 \leqslant j \leqslant d_i$, the field $\widetilde{L}_{i,j}$ is linearly disjoint from the compositum of all other fields $\widetilde{L}_{i',j'}$ with $1 \leqslant i' \leqslant r, 1 \leqslant j' \leqslant d_{i'}$ and $(i,j) \neq (i',j')$.*
- iii) *$\mathbf{F}_{q^D}$ is the full field of constants of $\widetilde{M}$.*
- iv) *The image of ι_2 consists of all pairs $(\mathrm{Frob}^k, \sigma)$ which obey the compatibility condition*

$$\sigma(S_{i,j}) \subset \sigma(S_{i,j+k}) \qquad \text{for every } i = 1, 2, \ldots, r.$$

The proofs of Lemmas 9, 10, and 11 are deferred to the next section. The curious reader may jump directly to the proof of Theorem 2 in §5.

4. Proofs of Lemmas 9, 10, and 11

4.1 Proof of Lemma 9

The proof of Lemma 9 rests on the following elementary bound for the number of affine zeros of a polynomial:

Lemma 12. *Let $E/\mathbf{F}_q$ be an arbitrary field extension and let $P(T_1,\dots,T_m)$ be a nonzero polynomial in m variables over E with total degree bounded by d. Then there are at most dq^{m-1} solutions to $P(x_1,\dots,x_m)=0$ in $\mathbf{F}_q^m$.*

This lemma is well-known in the case when $E=\mathbf{F}_q$ (see, e.g., [LN97, Theorem 6.13]), and the general case reduces to this one upon writing the coefficients of P with respect to an $\mathbf{F}_q$-basis of E.

Our computations also require the following evaluation of the discriminants of certain trinomials (cf. [EM99, Exercise 4.5.4]):

Lemma 13. *Let R be any integral domain, and let a and b be any elements of R. Then*

$$\mathrm{disc}_T(T^n+aT+b)=(-1)^{\binom{n}{2}}(n^n b^{n-1}+(-1)^{n-1}(n-1)^{n-1}a^n).$$

Proof of Lemma 9(i). For every pair of i and j with $1\leqslant i\leqslant r$ and $1\leqslant j\leqslant d_i$, we have

$$\mathrm{disc}_u^{n-1}\mathrm{disc}_T^{n}(h(T)-u-\theta_i^{(j)})=\mathrm{disc}_u^{n-1}\mathrm{disc}_T^{n}(h(T)-u); \tag{9}$$

indeed, the T-discriminant on the left-hand side differs from the one on the right only in that u is replaced by $u-\theta_i^{(j)}$, and such a shift leaves the outer u-discriminant unaffected.

Define a polynomial $\widehat{P}$ with integer coefficients in the $n-1$ indeterminates $T_1,\dots,T_{n-1}$ by

$$\widehat{P}(T_1,\dots,T_{n-1}):=\mathrm{disc}_u^{n-1}\mathrm{disc}_T^{n}(T^n+T_{n-1}T^{n-1}+\cdots+T_1T-u). \tag{10}$$

(Note that T and u are successively eliminated by the right-hand discriminants, so that only the indeterminates $T_1,\dots,T_{n-1}$ remain.) We claim that if q is prime to $2n$, then $\widehat{P}$ does not reduce to the zero polynomial when considered over $\mathbf{F}_q$. This suffices to prove (8). To see why, observe (from the definition of the discriminant in terms of the determinant of the $(2n-1)\times(2n-1)$ Sylvester matrix) that the inner T-discriminant on the right of (10) is a polynomial in u of degree at most $n-1$, each coefficient of which is a polynomial in $T_1,\dots,T_{n-1}$ of total degree bounded by $2n-1$. These coefficients determine the entries of the $(2n-3)\times(2n-3)$ determinant used to compute $\widehat{P}$, whence $\widehat{P}$ has total degree at most $(2n-1)(2n-3)$ in $T_1,\dots,T_{n-1}$. The desired bound (8) on the number of h which fail to satisfy (6) now follows from Lemma 9.

It remains to prove our claim that $\widehat{P}$ is nonvanishing when considered over $\mathbf{F}_q$. This is easiest if we adopt the further assumption that the characteristic p of $\mathbf{F}_q$ is prime to $n-1$. Indeed, successive application of Lemma 13 shows

$$\begin{aligned}\widehat{P}(1,0,\dots,0)&=\mathrm{disc}_u^{n-1}\mathrm{disc}_T^{n}(T^n+T-u)\\&=\mathrm{disc}_u^{n-1}\left((-1)^{\binom{n}{2}}\left(n^n(-u)^{n-1}+(-1)^{n-1}(n-1)^{n-1}\right)\right)\\&=\mathrm{disc}_u^{n-1}(n^nu^{n-1}+(n-1)^{n-1})=\pm(n-1)^{(n-1)^2}n^{n(n-2)},\end{aligned}$$

which is nonzero under this additional hypothesis.

We therefore suppose that p divides $n-1$. In this case we consider

$$\widehat{P}(1,1,\dots,1)=\mathrm{disc}_u^{n-1}\mathrm{disc}_T^{n}(T^n+T^{n-1}+\cdots+T-u).$$

To understand the inner discriminant, note that

$$(T-1)(T^n+T^{n-1}+\cdots+T-u)=T^{n+1}-T-(T-1)u.$$

By Lemma 13, the T-discriminant of the right-hand polynomial is given explicitly by

$$(-1)^{\binom{n+1}{2}}\left((n+1)^{n+1}u^n-n^n(u+1)^{n+1}\right). \tag{11}$$

We can relate this to the discriminant we are after by using the relations

$$\begin{aligned}&\mathrm{disc}_T((T-1)(T^n+T^{n-1}+\cdots+T-u)) = \\ &\qquad \pm\left((T^n+T^{n-1}+\cdots+T-u)|_{T=1}\right)^2 \mathrm{disc}_T(T^n+T^{n-1}+\cdots+T-u) = \\ &\qquad\qquad \pm(n-u)^2\mathrm{disc}_T(T^n+T^{n-1}+\cdots+T-u).\end{aligned}$$

Piecing this all together we obtain

$$\widehat{P}(1,1,\dots,1) = \mathrm{disc}_u^{n-1}\left(\frac{(n+1)^{n+1}u^n - n^n(u+1)^{n+1}}{(u-n)^2}\right).$$

Let $Q(u)$ denote the polynomial in u appearing in the argument of disc_u here, so that Q has degree $n-1$ in u. If $\widehat{P}(1,1,\dots,1)$ vanishes, then Q has a multiple root, which is necessarily also a multiple root of (11). One computes easily that unless p divides $n+1$, the only common root of (11) and its derivative is $u=n$. If $u=n$ is a multiple root of Q, then it must be a root of multiplicity at least 4 of (11), which forces the second derivative of (11) to vanish at $u=n$. But this second derivative is given by

$$(-1)^{\binom{n+1}{2}}\left((n+1)^{n+1}n(n-1)n^{n-2} - n^{n+1}(n+1)(n+1)^{n-1}\right) = (-1)^{\binom{n+1}{2}+1}n^{n-1}(n+1)^n.$$

Since the characteristic p is prime to n, this can only vanish if p divides $n+1$. So we are forced to the conclusion that $\widehat{P}(1,\dots,1)$ is nonvanishing except possibly if p divides $n+1$. However, p divides $n-1$ in the case we are considering, so that p can divide $n+1$ only if $p=2$, which is excluded. □

Proof of Lemma 9(ii). We proceed as in the proof of Lemma 9(i). Write $h(T) = T^n + a_{n-1}T^{n-1} + \cdots + a_1T$ as usual. Fix pairs (i,j) and (i',j') with $(i,j)\neq(i',j')$ and set

$$P(a_1,\dots,a_{n-1}) := \mathrm{res}_u^{n-1,n-1}\left(\mathrm{disc}_T^n(h(T)-u-\theta_i^{(j)}), \mathrm{disc}_T^n(h(T)-u-\theta_{i'}^{(j')})\right).$$

Arguing as in Lemma 9(i), we see that there is some polynomial $\widehat{P}(T_1,\dots,T_{n-1})$ over $\overline{\mathbf{F}}_q$ of degree at most $(2n-1)(2n-3)$ for which

$$P(a_1,\dots,a_{n-1}) = \widehat{P}(a_1,\dots,a_{n-1}) \quad \text{for all } a_1,\dots,a_{n-1}\in\mathbf{F}_q.$$

Then (7) is satisfied (for the fixed pairs (i,j) and (i',j')) as long as $\widehat{P}$ is nonvanishing. This nonvanishing is easily checked: indeed,

$$\begin{aligned}\widehat{P}(0,\dots,0) &= \mathrm{res}_u^{n-1,n-1}(\mathrm{disc}_T(T^n-u-\theta_i^{(j)}), \mathrm{disc}_T(T^n-u-\theta_{i'}^{(j')}))\\ &= \mathrm{res}_u^{n-1,n-1}(\mathrm{disc}_T(T^n-u), \mathrm{disc}_T(T^n-u+\theta_i^{(j)}-\theta_{i'}^{(j')}))\\ &= (-1)^{n+1}n^{n(2n-2)}(\theta_i^{(j)}-\theta_{i'}^{(j')})^{(n-1)^2}\neq 0.\end{aligned}$$

Lemma 12 now implies that $\widehat{P}$ has at most $(2n-1)(2n-3)q^{n-2}$ zeros in $\mathbf{F}_q^{n-1}$, finishing the proof. □

4.2 Proofs of Lemmas 10 and 11

Our fundamental tool is the following criterion of Birch & Swinnerton-Dyer [BSD59] for certain polynomials to have the full symmetric group as their Galois group. We state their result in an alternative form attributed by the same authors to Davenport:

A Criterion of Birch & Swinnerton-Dyer. *Let h be a polynomial of degree $n\geqslant 2$ with coefficients from a finite field F whose characteristic is prime to n. Suppose that with u an indeterminate over F, we have*

$$\mathrm{disc}_u^{n-1}\mathrm{disc}_T^n(h(T)-u)\neq 0. \tag{12}$$

Then the Galois group of $h(T)-u$ over the rational function field $\overline{F}(u)$ is the full symmetric group on the n roots of $h(T)-u$. Consequently, if E is any algebraic extension of F, then the Galois group of $h(T)-u$ over $E(u)$ is also the full symmetric group.

Proof of Lemmas 10(i) and 11(i). Suppose that h satisfies both conditions (6) and (7). Then part (i) of Lemma 10 is immediate from the Birch & Swinnerton-Dyer criterion. Since $\widetilde{L}_{i,j}$ is the splitting field of $h(T)-u-\theta_i^{(j)}$ over $\mathbf{F}_{q^D}$, the same argument also establishes Lemma 11(i). $\square$

To continue we require two more technical tools. The first is a lemma of Hayes appearing in an alternative proof of the Birch & Swinnerton-Dyer criterion:

Lemma 14 (Hayes). *Let h be a polynomial of degree $n \geqslant 2$ over the finite field $\mathbf{F}_q$ which satisfies the hypotheses of the Birch & Swinnerton-Dyer criterion with $F=\mathbf{F}_q$. Let L be the splitting field of $h(T)-u$ over $\overline{\mathbf{F}}_q(u)$. Let P_∞ be the prime of $\overline{\mathbf{F}}_q(u)$ corresponding to the $(1/u)$-adic valuation on $\overline{\mathbf{F}}_q[1/u]$, and let P be any prime of L lying above above P_∞. Then $e(P|P_\infty)=n$, where $e(P|P_\infty)$ denotes the ramification index of P over P_∞.*

Hayes proves this explicitly only in the case $h=T^n+T-u$ (see [Hay73, Proof of Lemma 1]), but as he remarks the arguments extend easily to the general case. It is necessary for us to also understand the ramification of P_∞ in certain extensions of the fields appearing in Hayes's lemma; for this we appeal to the following result ([Sti93, Proposition III.8.9]):

Abhyankar's Lemma. *Let F'/F be a finite separable extension of function fields. Suppose that $F'=F_1F_2$ is the compositum of two intermediate fields $F\subset F_1,F_2\subset F'$. Let P be a prime of F and P' a prime of F' lying above P. With $P_i := P'\cap F_i$ for $i=1$ and 2, assume that at least one of the extensions P_1/P or P_2/P is tame (i.e., that $e(P_i/P)$ is relatively prime to the characteristic of F). Then*

$$e(P'/P)=\operatorname{lcm}[e(P_1/P),e(P_2/P)].$$

In particular, if both P_1/P and P_2/P are tamely ramified, then so is P'/P.

Proof of Lemmas 10(ii) and 11(ii). Define the constant field extensions

$$\widehat{K}_{i,j} := K_{i,j}\overline{\mathbf{F}}_q,\quad \widehat{L}_{i,j} := L_{i,j}\overline{\mathbf{F}}_q,\quad \text{and}\quad \widehat{M_i} := M_i\overline{\mathbf{F}}_q.$$

Thus $\widehat{L}_{i,j}$ is the splitting field of $h(T)-u-\theta_i^{(j)}$ over $\overline{\mathbf{F}}_q$. To prove Lemma 10(ii), it suffices to show that for each fixed i,

$$\widehat{L}_{i,j} \text{ is linearly disjoint from the compositum of } \widehat{L}_{i,j'} \text{ for } 1\leqslant j'\neq j\leqslant d_i. \tag{13}$$

Indeed, once (13) is known, we may deduce that

$$\operatorname{Gal}(\widehat{M_i}/\overline{\mathbf{F}}_q(u))\cong \operatorname{Gal}(\widehat{L}_{i,1}/\overline{\mathbf{F}}_q(u))\times\cdots\times\operatorname{Gal}(\widehat{L}_{i,d_i}/\overline{\mathbf{F}}_q(u)).$$

By the Birch & Swinnerton-Dyer criterion the right-hand Galois groups each have size $n!$, so that the left-hand Galois group has size $n!^{d_i}$. But the left-hand Galois group injects (via restriction) into $\operatorname{Gal}(M_i/\mathbf{F}_{q^{d_i}}(u))$, and degree counting shows that this injection must be an isomorphism; thus

$$[M_i:\mathbf{F}_{q^{d_i}}(u)]=[L_{i,1}L_{i,2}\cdots L_{i,d_i}:\mathbf{F}_{q^{d_i}}(u)]=[L_{i,1}:\mathbf{F}_{q^{d_i}}(u)][L_{i,2}:\mathbf{F}_{q^{d_i}}(u)]\cdots[L_{i,d_i}:\mathbf{F}_{q^{d_i}}(u)],$$

which implies Lemma 10(ii).

To prove (13), consider the intersection N of $\widehat{L}_{i,j}$ with the compositum of the fields $\widehat{L}_{i,j'}$ for $1\leqslant j\neq j'\leqslant d_i$. The only primes of $\overline{\mathbf{F}}_q(u)$ that can ramify in N ramify in both $\widehat{K}_{i,j}$ and some $\widehat{K}_{i,j'}$ with $1\leqslant j\neq j'\leqslant d_i$. But by (7), the polynomials

$$\operatorname{disc}_T^n(h(T)-u-\theta_i^{(j)}) \quad\text{and}\quad \operatorname{disc}_T^n(h(T)-u-\theta_i^{(j')}) \quad \text{have no common roots,}$$

and so the only prime that can possibly ramify in both extensions is P_∞. By Hayes's Lemma 14 and repeated application of Abhyankar's Lemma, P_∞ is tamely ramified in $\widehat{L}_{i,j}$ and hence also in N. (Here we again use our hypothesis that q is prime to n.) Thus N is a finite, tamely ramified geometric extension of $\overline{\mathbf{F}}_q(u)$ unramified except possibly at primes above the degree 1 prime P_∞. It follows that $N = \overline{\mathbf{F}}_q(u)$ (this is an immediate consequence of the Riemann-Hurwitz genus formula; see, e.g., [Hay73, p.460] or [Ros02, Exercise 6, p.99]). This proves (13) and together with the above argument completes the proof of Lemma 10(ii).

The proof of Lemma 11(ii) is nearly identical but is based instead on the claim that

$$\widehat{L}_{i,j} \text{ is linearly disjoint from the compositum of } \widehat{L}_{i,j} \text{ for } (i,j) \neq (i',j'); \tag{14}$$

we omit the details. □

Proof of Lemmas 10(iii) and 11(iii). In the course of proving Lemma 10(ii), we showed that restriction induces an isomorphism

$$\mathrm{Gal}(\widehat{M}_i/\overline{\mathbf{F}}_q(u)) \cong \mathrm{Gal}(M_i/\mathbf{F}_{q^{d_i}}(u)).$$

If $\alpha \in M_i \cap \overline{\mathbf{F}}_q$, then α is fixed by every element of the left-hand Galois group appearing above, and so must be fixed by all elements of the right-hand Galois group. But this forces α to lie in the field of rational functions $\mathbf{F}_{q^{d_i}}(u)$. Since α is algebraic over $\mathbf{F}_q$, it must belong to $\mathbf{F}_{q^{d_i}}$. So $\mathbf{F}_{q^{d_i}}$ is the full field of constants of M_i. Lemma 11(iii) can be proved similarly, using that restriction induces an isomorphism $\mathrm{Gal}(\widetilde{M}\overline{\mathbf{F}}_q/\overline{\mathbf{F}}_q(u)) \cong \mathrm{Gal}(\widetilde{M}/\mathbf{F}_{q^D}(u))$. □

Proof of Lemma 10(iv). This is immediate from parts (i) and (ii) of Lemma 10. □

Proof of Lemma 10(v) and Lemma 11(iv). Suppose that $\sigma \in \mathrm{Gal}(M_i/\mathbf{F}_{q^{d_i}}(u))$ satisfies $\sigma|_{\mathbf{F}_{q^{d_i}}} = \mathrm{Frob}^k$. Then σ takes $\theta_i^{(j)}$ to $\theta_i^{(j+k)}$ and so takes every root of $h(T) - u - \theta_i^{(j)}$ to a root of $h(T) - u - \theta_i^{(j+k)}$. It follows that the image of ι_2 is contained within the set of elements obeying the compatibility condition specified in Lemma 10(v). A straightforward counting argument shows that there are $d_i n!^{d_i}$ such elements of $\mathrm{Gal}(\mathbf{F}_{q^{d_i}}/\mathbf{F}_q) \times \mathrm{Sym}(\cup_{j=1}^{d_i} S_{i,j})$. On the other hand, we know that $M_i/\mathbf{F}_q(u)$ is Galois of degree $[M_i : \mathbf{F}_q(u)] = [M_i : \mathbf{F}_{q^{d_i}}(u)][\mathbf{F}_{q^{d_i}}(u) : \mathbf{F}_q(u)] = d_i n!^{d_i}$. Since ι_2 is injective, it follows that the image of ι_2 must coincide with the set specified in (v).

A similar argument establishes Lemma 11(iv): in that case $\widetilde{M}$ is Galois over $\mathbf{F}_q(u)$ of degree $Dn!^{d_1+\cdots+d_r}$, and this degree coincides with the number of elements obeying the compatibility condition of Lemma 11(iv). □

5. Proof of Theorem 2

Throughout this section $f_1(T), \ldots, f_r(T)$ denote pairwise nonassociated irreducible polynomials of respective degrees $d_1, \ldots, d_r$ over $\mathbf{F}_q$ and $h(T) = T^n + a_{n-1}T^{n-1} + \cdots + a_1 T$ denotes a monic polynomial over $\mathbf{F}_q$ of degree $n \geqslant 2$ without constant term satisfying conditions (6) and (7).

Our plan is to use the Chebotarev density theorem to estimate, for each individual $h(T)$, the number of $a \in \mathbf{F}_q$ for which all of the specializations $f_i(h(T) - a)$ are irreducible. We begin by recalling the following well-known lemma (see, e.g., [Coh89, pp. 408-409]):

LEMMA 15. *Let f be an irreducible polynomial of degree d over $\mathbf{F}_q$ and let θ be a root of f from the extension $\mathbf{F}_{q^d}$. Let $p(T)$ be a nonconstant polynomial over $\mathbf{F}_q$. Then $f(p(T))$ is irreducible over $\mathbf{F}_q$ if and only if $p(T) - \theta$ is irreducible over $\mathbf{F}_{q^d}$.*

The next result explains how the Chebotarev density theorem enters the picture:

Lemma 16. *There is a conjugacy class $\mathcal{C}$ of $\mathrm{Gal}(\widetilde{M}/\mathbf{F}_q(u))$ with the following property: If a is an element of $\mathbf{F}_q$ which is not a zero of any of the polynomials*

$$\mathrm{disc}_T(h(T)-u-\theta_i^{(j)}) \quad \textit{for} \quad 1 \leqslant i \leqslant r, \quad 1 \leqslant j \leqslant d_i, \tag{15}$$

then $f_i(h(T)-a)$ is irreducible over $\mathbf{F}_q$ if and only if $\mathcal{C}$ coincides with the Frobenius conjugacy class $(\widetilde{M}/\mathbf{F}_q(u), P_a)$.

Proof. Since a is not a root of any of the polynomials (15), P_a is unramified in $\widetilde{M}$, where P_a denotes the prime of $\mathbf{F}_q(u)$ corresponding to the $(u-a)$-adic valuation on $\mathbf{F}_q(u)$. Now fix $1 \leqslant i \leqslant r$. Using Lemma 15 and Kummer's Theorem ([Sti93, Theorem 3.3.7]), we find

$$\begin{aligned} f_i(h(T)-a) \text{ is irreducible over } \mathbf{F}_q &\iff h(T)-a-\theta_i^{(1)} \text{ is irreducible over } \mathbf{F}_{q^{d_i}} \\ &\iff P_a \text{ stays prime in } K_{i,1}. \end{aligned}$$

This last possibility can be recast in terms of the action of Frobenius. Let σ denote any element of the Frobenius conjugacy class $(M_i/\mathbf{F}_q(u), P_a)$; then necessarily

$$\sigma \text{ restricts to the } q\text{th power map on } \mathbf{F}_{q^{d_i}}. \tag{16}$$

Moreover, P_a stays prime in $K_{i,1}$ if and only if

$$\mathrm{Gal}(M_i/\mathbf{F}_q(u)) = \dot{\bigcup}_{l=0}^{d_i n-1} \mathrm{Gal}(M_i/K_{i,1})\sigma^l. \tag{17}$$

We now investigate when (17) holds.

Write $K_{i,1} = \mathbf{F}_{q^{d_i}}(u)(\alpha)$, where $\alpha \in S_{i,1}$. Now (16) implies that under ι_2 the element σ is identified with (Frob, σ'), where σ' is a permutation of $\cup_{j=1}^{d_i} S_{i,j}$. We claim that (17) holds if and only if σ' is an nd_i-cycle. Indeed, suppose that σ (equivalently, σ') acts as an nd_i-cycle on $\cup_{j=1}^{d_i} S_{i,j}$; then for any $\gamma \in \mathrm{Gal}(M_i/\mathbf{F}_q(u))$, there is a unique $0 \leqslant l < d_i n$ for which $\tau\sigma^{-l}$ fixes α, and this implies (17). Conversely, if (17) holds then $\sigma \notin \mathrm{Gal}(M_i/K_{i,1})$, so that σ (and hence σ') must move α. Thus in the decomposition of σ' into disjoint cycles, α must occur in a nontrivial cycle. If this cycle has length $l < nd_i$, then both σ^l and σ^0 belong to $\mathrm{Gal}(M/K_{i,1})$, and this contradicts that (17) is a disjoint union.

Let γ denote an element of the conjugacy class of $(\widetilde{M}/\mathbf{F}_q(u), P_a)$. Since γ restricts down to an element of the conjugacy class of $(M_i/\mathbf{F}_q(u), P_a)$, in order for P_a to stay prime in M_i for every $i = 1, 2, \ldots, r$ it is necessary and sufficient that $\gamma|_{M_i}$ satisfies both (16) and (17) for every $1 \leqslant i \leqslant r$. By our work above and the commutativity of diagram (5), this condition on γ holds if and only if γ (identified with its representation under ι_1) has the form $(\mathrm{Frob}, \sigma_1, \ldots, \sigma_r)$, where each σ_i is an nd_i-cycle on $\cup_{j=1}^{d_i} S_{i,j}$. It remains to prove that the γ in $\mathrm{Gal}(\widetilde{M}/\mathbf{F}_q(u))$ of this form make up a single conjugacy class of size $n^{-r} n!^{d_1+\cdots+d_r}$.

Suppose that $\gamma \in \mathrm{Gal}(\widetilde{M}/\mathbf{F}_q(u))$ has the above form. The compatibility condition of Lemma 11(iv) implies that

$$\sigma_i(S_{i,j}) \subset S_{i,j+1} \quad \text{for all } 1 \leqslant i \leqslant r \text{ and all } j.$$

Now fix $1 \leqslant i \leqslant r$. Since σ_i is an nd_i-cycle on $\cup_{j=1}^{d_i} S_{i,j}$, it follows that σ_i has exactly n representations in the form

$$\begin{aligned} &(a_1\ a_2\ \ldots\ a_{nd_i}), \quad \text{where for each } 1 \leqslant k \leqslant d_i, \\ &\qquad\qquad (a_k\ a_{k+d_i}\ \ldots\ a_{(n-1)k+d_i}) \text{ is an } n\text{-cycle of } \mathrm{Sym}(S_{i,k}). \end{aligned}$$

Consequently, there are exactly $n^{-1} n!^{d_i}$ possibilities for σ_i, and so exactly

$$n!^{-r} n!^{d_1+\cdots+d_r}$$

possibilities for γ. Moreover, this explicit description shows that the γ of this form make up a single conjugacy class of $\mathrm{Gal}(\widetilde{M}/\mathbf{F}_q(u))$. To see this observe that

$$\mathrm{Gal}(\widetilde{M}/\mathbf{F}_q(u)) \supset \mathrm{Gal}(\widetilde{M}/\mathbf{F}_{q^D}(u)) = \prod_{\substack{1\leqslant i\leqslant r\\ 1\leqslant j\leqslant d_i}} \mathrm{Sym}(S_{i,j})$$

and that $\mathrm{Sym}(S_{i,j})$ acts transitively by conjugation on its own n-cycles. □

To apply the Chebotarev density theorem we require an estimate for the genus of $\widetilde{M}/\mathbf{F}_{q^D}$. This will be obtained as a corollary of the next result, which appears as [Sti93, Theorem III.10.3]:

Castelnuovo's Inequality. *Let F/k be a function field with full constant field k. Suppose we are given two subfields F_1/k and F_2/k of F/k satisfying*

i) *$F = F_1F_2$ is the compositum of F_1 and F_2,*

ii) *$[F : F_i] = n_i$ and F_i/k has genus g_i for $i = 1, 2$.*

Then the genus g of F/k obeys the bound

$$g \leqslant n_1g_1 + n_2g_2 + (n_1 - 1)(n_2 - 1).$$

Corollary 17. *Let $f_1(T), \ldots, f_r(T)$ be pairwise nonassociated monic irreducible polynomials of respective degrees $d_1, \ldots, d_r$ over $\mathbf{F}_q$ and suppose that $h(T)$ is a polynomial of degree $n \geqslant 2$ without constant term satisfying conditions* (6) *and* (7)*. Then the genus of $\widetilde{M}/\mathbf{F}_{q^D}$ is bounded above by*

$$(2(d_1 + \cdots + d_r) - 1)n!^{d_1+\cdots+d_r-1}n^n.$$

Proof. We make repeated use of Castelnuovo's Inequality. Our first application is an estimate for the genus of the function fields $\widetilde{L}_{i,j}/\mathbf{F}_{q^D}$. For a fixed pair of i and j, let $\widetilde{K}^{(1)}, \ldots, \widetilde{K}^{(n)}$ be the complete list of conjugate fields of $\widetilde{K}_{i,j}$, so that $\widetilde{L}_{i,j}$ is the compositum of $\widetilde{K}^{(1)}, \ldots, \widetilde{K}^{(n)}$. For any $m \leqslant n$, Castelnuovo's Inequality implies that (using g_N to denote the genus of $N/\mathbf{F}_{q^D}$)

$$\begin{aligned} g_{\widetilde{K}^{(1)}\cdots\widetilde{K}^{(m)}} \leqslant [\widetilde{K}^{(1)}\cdots\widetilde{K}^{(m)} : \widetilde{K}^{(1)}\cdots\widetilde{K}^{(m-1)}]g_{\widetilde{K}^{(1)}\cdots\widetilde{K}^{(m-1)}} + [\widetilde{K}^{(1)}\cdots\widetilde{K}^{(m)} : \widetilde{K}^{(m)}]g_{\widetilde{K}^{(m)}} + \\ \left([\widetilde{K}^{(1)}\cdots\widetilde{K}^{(m)} : \widetilde{K}^{(1)}\cdots\widetilde{K}^{(m-1)}] - 1\right)\left([\widetilde{K}^{(1)}\cdots\widetilde{K}^{(m)} : \widetilde{K}^{(m)}] - 1\right). \end{aligned}$$

Since each $\widetilde{K}^{(i)}$ is a rational function field (obtainable by adjoining a single root of $h(T) - u - \theta_i^{(j)}$ to $\mathbf{F}_{q^D}$), we have $g_{\widetilde{K}^{(m)}} = 0$ and so the second summand on the right hand side vanishes. Estimating the size of the field extensions appearing here trivially, we find

$$g_{\widetilde{K}^{(1)}\cdots\widetilde{K}^{(m)}} \leqslant ng_{\widetilde{K}^{(1)}\cdots\widetilde{K}^{(m-1)}} + (n-1)(n^{m-1} - 1) \leqslant ng_{\widetilde{K}^{(1)}\cdots\widetilde{K}^{(m-1)}} + n^{m-1}.$$

This relation implies inductively that

$$g_{\widetilde{K}^{(1)}\cdots\widetilde{K}^{(m)}} \leqslant (m-1)n^{m-1}$$

and so taking $m = n$ yields

$$g_{\widetilde{L}_{i,j}} \leqslant (n-1)n^{n-1} \leqslant n^n.$$

To continue we enumerate the $\widetilde{L}_{i,j}$ as $\widetilde{L}^{(1)}, \ldots, \widetilde{L}^{(d_1+\cdots+d_r)}$, so that $\widetilde{M}$ is the compositum of the $\widetilde{L}^{(i)}$ for $1 \leqslant i \leqslant d_1 + \cdots + d_r$. By Castelnuovo's Inequality, we have for any $k \leqslant d_1 + \cdots + d_r$ that

$$\begin{aligned} g_{\widetilde{L}^{(1)}\cdots\widetilde{L}^{(k)}} \leqslant [\widetilde{L}^{(1)}\cdots\widetilde{L}^{(k)} : \widetilde{L}^{(k)}]g_{\widetilde{L}^{(k)}} + [\widetilde{L}^{(1)}\cdots\widetilde{L}^{(k)} : \widetilde{L}^{(1)}\cdots\widetilde{L}^{(k-1)}]g_{\widetilde{L}^{(1)}\cdots\widetilde{L}^{(k-1)}} + \\ ([\widetilde{L}^{(1)}\cdots\widetilde{L}^{(k)} : \widetilde{L}^{(k)}] - 1)([\widetilde{L}^{(1)}\cdots\widetilde{L}^{(k)} : \widetilde{L}^{(1)}\cdots\widetilde{L}^{(k-1)}] - 1); \end{aligned}$$

thus

$$\begin{aligned} g_{\widetilde{L}^{(1)}\ldots\widetilde{L}^{(k)}} &\leqslant n!^{k-1}n^n + n!g_{\widetilde{L}^{(1)}\ldots\widetilde{L}^{(k-1)}} + (n!^{k-1}-1)(n!-1) \\ &\leqslant n!^{k-1}n^n + n!g_{\widetilde{L}^{(1)}\ldots\widetilde{L}^{(k-1)}} + n!^{k-1}n^n. \end{aligned}$$

Another induction now shows

$$g_{\widetilde{L}^{(1)}\ldots\widetilde{L}^{(k)}} \leqslant (2k-1)n!^{k-1}n^n;$$

taking $k = d_1 + d_2 + \cdots + d_r$ gives the result. □

Finally we state the particular version of the Chebotarev density theorem required in our application. This result is implicit in Fried & Jarden's discussion of that theorem (see [FJ05, Proposition 6.4.8] and its proof, which incorporates corrections from [GJ98, Appendix]). A similar result could also be derived from the work of Murty & Scherk [MS94].

Explicit Chebotarev Density Theorem for First Degree Primes. *Suppose $M/\mathbf{F}_q(u)$ is a finite Galois extension having full field of constants $\mathbf{F}_{q^D}$. Let $\mathcal{C}$ be a conjugacy class of* $\mathrm{Gal}(M/\mathbf{F}_q(u))$ *every element of which restricts down to the qth power map on $\mathbf{F}_{q^D}$. Let*

$$\mathcal{P} := \left\{ \textit{first degree primes } P \textit{ of } \mathbf{F}_q(u) \textit{ unramified in } M : \left(\frac{M/\mathbf{F}_q(u)}{P}\right) = \mathcal{C} \right\}.$$

Then

$$\left| \#\mathcal{P} - \frac{\#C}{[M:\mathbf{F}_{q^D}(u)]} q \right| \leqslant 2\frac{\#C}{[M:\mathbf{F}_{q^D}(u)]}(gq^{1/2} + g + [M:\mathbf{F}_{q^D}(u)]),$$

where g denotes the genus of $M/\mathbf{F}_{q^D}$.

Proof of Theorem 2. Suppose that the polynomial $h(T) = T^n + a_{n-1}T^{n-1} + \cdots + a_1 T$ over $\mathbf{F}_q$ satisfies both (6) and (7). The number of $a \in \mathbf{F}_q$ for which at least one of the polynomials (15) vanishes is bounded above by

$$(n-1)(d_1 + \cdots + d_r) \leqslant (n-1)B.$$

For all other $a \in \mathbf{F}_q$ the simultaneous irreducibility of the $f_i(h(T)-a)$ is equivalent to $(\widetilde{M}/\mathbf{F}_q(u), P_a)$ coinciding with the conjugacy class $\mathcal{C}$ appearing in Lemma 16. Since $\mathcal{C}$ has size $n^{-r}n!^{d_1+\cdots+d_r}$ and $[\widetilde{M}:\mathbf{F}_{q^D}(u)] = n!^{d_1+\cdots+d_r}$, the explicit Chebotarev density theorem implies there are at least

$$\frac{q}{n^r} - \frac{2}{n^r}\left(gq^{1/2} + g + n!^{d_1+\cdots+d_r}\right) - (n-1)B$$

values of $a \in \mathbf{F}_q$ for which all the polynomials $f_i(h(T)-a)$ are irreducible, and at most

$$(n-1)B + \frac{q}{n^r} + \frac{2}{n^r}\left(gq^{1/2} + g + n!^{d_1+\cdots+d_r}\right)$$

such values of a. (Here g denotes the genus of $\widetilde{M}/\mathbf{F}_{q^D}(u)$.)

We now replace $d_1 + \cdots + d_r$ by B and sum over the possibilities for h. Assume that

$$q^{n-1} > 4n^2\left(1 + \binom{B}{2}\right),$$

which holds if q is sufficiently large in terms of n and B. (This inequality guarantees that there is some h of degree n for which (6) and (7) both hold. Note that this inequality can be assumed for the proof of Theorem 2, since for q bounded in terms of n and B the estimate of that theorem is trivial.) Then we find that the total number of monic degree n polynomials $\widetilde{h}(T)$ for which all the $f_i(\widetilde{h}(T))$ are irreducible is bounded below by

$$\left(q^{n-1} - 4n^2\left(1 + \binom{B}{2}\right)\right)\left(\frac{q}{n^r} - \frac{2}{n^r}\left(gq^{1/2} + g + n!^B\right) - (n-1)B\right) \tag{18}$$

and bounded above by

$$4n^2q^{n-1}\left(1+\binom{B}{2}\right)+\left(q^{n-1}-4n^2q^{n-2}\left(1+\binom{B}{2}\right)\right)\left(\frac{q}{n^r}+\frac{2}{n^r}\left(gq^{1/2}+g+n!^B\right)+(n-1)B\right).$$

Since g is $O_{n,B}(1)$ by Corollary 17, both the upper and lower bounds have the form $q^n/n^r + O_{n,B}(q^{n-1/2})$, finishing the proof. □

6. Proof of Theorem 3

We begin with some comments on the relation between Theorem A and Theorem 3. For q large in terms of r and B, Theorem A asserts the existence of infinitely many irreducibility preserving substitutions $T \mapsto T^{l^k} - \beta$ for some prime l dividing $q-1$ and some $\beta \in \mathbf{F}_q$. So we obtain irreducibility-preserving substitutions whose degrees are exactly the powers of l. In the proof of Theorem A, there is some control over the choice of l, and this could be used to establish Theorem 3 in a number of special cases.

In order to prove Theorem 3 in full, we require two additional ingredients:

i) the existence of a preliminary irreducibility-preserving substitution $T \mapsto h(T)$ of degree d, for an appropriate d belonging to the progression $a \bmod m$,
ii) the existence of some l prime to m and some $\beta \in \mathbf{F}_q$ for which all the substitutions $T \mapsto T^{l^k} - \beta$ preserve the irreducibility of the polynomials $f_i(h(T))$, where $h(T)$ is as in (i).

If we can establish (i) and (ii), then Theorem 3 follows immediately, since $h(T^{l^k} - \beta)$ has degree from the progression $a \bmod m$ whenever k is divisible by $\varphi(m)$. The most difficult part of the proof is obtaining (i), which requires Theorem 2. By contrast, the techniques necessary for the proof of (ii) are present already in [Pol06]. However, the details here are slightly different; this is because in proving Theorem 3 we take l as a divisor of q^d-1 (with d as in (i) above), while in the cited paper l is always chosen as a divisor of $q-1$.

We now give the specifics. Recall the following elementary result of Bang [Ban86] (see [Roi97, Theorem 3] for a short modern account):

Bang's Theorem on Primitive Prime Divisors. *Let a and d be integers greater than 1. Then there is a prime p for which a has order d modulo p in all except the following cases:*

i) $d = 2$, $a = 2^s - 1$, *where* $s \geqslant 2$,
ii) $d = 6$, $a = 2$.

Corollary 18. *Let m be a positive integer. Then every integer $d > \max\{2, \varphi(m)\}$ has the following property: if q is any odd integer $\geqslant 3$, then $q^d - 1$ has an odd prime divisor not dividing m.*

Proof. Suppose $d > \max\{2, \varphi(m)\}$. By Bang's theorem there is a prime l for which q has order d in $(\mathbf{Z}/l\mathbf{Z})^\times$. Since $d > 1$, we must have $l \neq 2$. Moreover, l is necessarily prime to m: for if l divides m, then the order of q in $(\mathbf{Z}/l\mathbf{Z})^\times$ is a divisor of $\varphi(l)$, hence also a divisor of $\varphi(m)$ and so less than d, a contradiction. Hence l is an odd prime divisor of q^d-1 which is prime to m. □

The next lemma, due to Serret in the case of prime fields [Ser66, Théorème I, p. 656] and Dickson in the general case ([Dic97, p. 382]; see also [Dic58, §34]), plays an essential role in the proofs of both Theorems 3 and 4. (For a modern treatment see [LN97, Theorem 3.3.5].) Recall that if $f(T)$ is an irreducible polynomial over $\mathbf{F}_q$ not associated to T, then by the *order of f* we mean the order of any of its roots in the multiplicative group of its splitting field (equivalently, the order of T in the unit group $(\mathbf{F}_q[T]/f)^\times$). Thus if f has degree d, then the order of f is a divisor of q^d-1.

Lemma 19 (Serret, Dickson). *Let f be an irreducible polynomial over $\mathbf{F}_q$ of degree d and order e. Let l be an odd prime. Suppose that f has a root $\alpha \in \mathbf{F}_{q^d}$ which is not an lth power, or equivalently that*

$$l \mid e \quad \text{but} \quad l \nmid (q^d - 1)/e. \tag{19}$$

Then the substitution $T \mapsto T^{l^k}$ leaves f irreducible for every $k = 1, 2, 3, \ldots$.

We also require the following estimate for character sums which appears as [Pol06, Lemma 7]:

Lemma 20. *Let $f_1(T), \ldots, f_s(T)$ be pairwise nonassociated irreducible polynomials over $\mathbf{F}_q$ with the degree of $f_1 \cdots f_s$ bounded by B. Fix roots $\alpha_1, \ldots, \alpha_s$ of $f_1, \ldots, f_s$, respectively, lying in an algebraic closure of $\mathbf{F}_q$. Suppose that for each $i = 1, 2, \ldots, s$ we have a character χ_i of $\mathbf{F}_q(\alpha_i)$ and that at least one of these χ_i is nontrivial. Then*

$$\left| \sum_{\beta \in \mathbf{F}_q} \chi_1(\alpha_1 + \beta) \cdots \chi_s(\alpha_s + \beta) \right| \leqslant (B - 1)\sqrt{q}. \tag{20}$$

We can now establish the following variant of Theorem A:

Lemma 21. *Let $f_1(T), \ldots, f_r(T)$ be pairwise nonassociated irreducible polynomials over $\mathbf{F}_q$ with each f_i of degree > 1 and the degree of $f_1 \cdots f_r$ bounded by B. Suppose that there is a common odd prime l dividing $q^{\deg f_i} - 1$ for each $i = 1, 2, \ldots, r$. If*

$$q > (2^{r-1}B - 2^r + 1)^2,$$

then there is a $\beta \in \mathbf{F}_q$ for which all the polynomials $f_1(T^{l^k} - \beta), \ldots, f_r(T^{l^k} - \beta)$ are irreducible for each $k = 1, 2, 3, \ldots$.

Proof. Fix roots $\alpha_1, \ldots, \alpha_r$ of $f_1(T), \ldots, f_r(T)$, respectively. By Lemma 19, it suffices to produce an element $\beta \in \mathbf{F}_q$ with the property that $\alpha_i + \beta$ is an lth power nonresidue in $\mathbf{F}_q(\alpha_i)$ for every $i = 1, 2, \ldots, r$. Since l divides $q^{\deg f_i} - 1$ for each i, there are characters χ_i of order l on each of the fields $\mathbf{F}_q(\alpha_i)$. If for every choice of β, there is an $i \in \{1, 2, \ldots, r\}$ for which $\alpha_i + \beta$ is an lth power in $\mathbf{F}_q(\alpha_i)$, then the sum

$$\sum_{\beta \in \mathbf{F}_q} (1 - \chi_1(\alpha_1 + \beta))(1 - \chi_2(\alpha_2 + \beta)) \cdots (1 - \chi_r(\alpha_r + \beta))$$

vanishes. (Note that it is impossible for any of the arguments $\alpha_i + \beta$ inside a character to vanish, since each α_i belongs to a nontrivial extension of $\mathbf{F}_q$.) But by Lemma 20, the absolute value of this sum is bounded below by

$$q - \sum_{\substack{\mathcal{I} \subset \{1,2,\ldots,r\} \\ \mathcal{I} \neq \emptyset}} \left(-1 + \sum_{i \in \mathcal{I}} \deg f_i(T) \right) \sqrt{q} =$$

$$q + (2^r - 1)\sqrt{q} - \sum_{i=1}^{r} \deg f_i \left(\sum_{\substack{\mathcal{I} \subset \{1,2,\ldots,r\} \\ i \in I}} 1 \right) \sqrt{q} \geqslant q + (2^r - 1)\sqrt{q} - 2^{r-1}B\sqrt{q},$$

and this is positive for q as in the hypothesis of the lemma. □

Proof of Theorem 3. Suppose $f_1, \ldots, f_r$ are irreducible polynomials over $\mathbf{F}_q$, where $\mathbf{F}_q$ is a finite field with characteristic p coprime to $2\gcd(a, m)$. Let d be the smallest integer exceeding $\max\{2, \varphi(m)\}$ relatively prime to p and satisfying $d \equiv a \pmod{m}$. Since p is prime to $\gcd(a, m)$, it follows that p

divides at most one of any two consecutive terms from the progression $a \bmod m$, so that $d \leqslant 3m$. In particular d is bounded solely in terms of m. So by Theorem 2, as long as q is sufficiently large (depending just on B and m), there is a polynomial h of degree d for which all of $f_1(h(T)), \dots, f_r(h(T))$ are irreducible over $\mathbf{F}_q$. Using Corollary 18, choose a prime l dividing $q^d - 1$ which is relatively prime to m. Then l also divides $q^{\deg f_i(h(T))} - 1$ for each $i = 1, 2, \dots, r$. According to Lemma 21 (applied to the polynomials $f_1(h(T)), \cdots, f_r(h(T))$), if

$$q > (2^{r-1} dB - 2^r + 1)^2,$$

then there is some $\beta \in \mathbf{F}_q$ with the property that the polynomials $f_i(h(T^{l^k} - \beta))$ are all irreducible over $\mathbf{F}_q$ for $k = 1, 2, 3, \dots$. Since

$$\deg h(T^{l^k} - \beta) = dl^k \equiv al^k \equiv a \pmod{m}$$

whenever k is a multiple of $\varphi(m)$, the proof of Theorem 3 is complete. $\square$

7. Application to a Question of Hall

We prove Theorem 4 in two parts:

7.1 Part I: Infinitely Many Twin Prime Pairs of Odd Degree

In the case when $q - 1$ has an odd prime divisor the twin prime pairs constructed by Hall [Hal06] already have odd degree, so we may suppose that $q - 1$ is a power of 2. Now recall that if q is an odd prime power for which $q - 1$ is a power of 2, then either $q = 9$ or q is a Fermat prime ([Sie88, p. 374, Exercise 1]).

Theorem 3 guarantees the existence of a twin prime pair $f, f + 1$ of degree $\equiv 1 \pmod 2$ over all sufficiently large finite fields $\mathbf{F}_q$ with q odd. The next lemma is an explicit version of a slightly weaker result:

Lemma 22. *Suppose $q > 10^6$ is a prime power coprime to 6. Then there are infinitely many twin prime pairs $f, f + 1$ over $\mathbf{F}_q$ for which $\deg f = \deg(f + 1)$ is odd.*

It is worth remarking that no Fermat primes $> 10^6$ are known, and it is plausible that none exist.

Proof. By Theorem 2, if q is large enough and prime to 6, then we may choose a monic prime pair $f, f + 1$ of degree 3 over $\mathbf{F}_q$. In fact, referring to the lower bound (18) (with $r = 2$, $B = 2$ and $n = 3$), we see that such pairs exist as long as q satisfies the inequalities

$$q^2 > 8 \cdot 3^2 \quad \text{and} \quad \frac{q}{9} - \frac{2}{9}(gq^{1/2} + g + 6^2) - 2 \cdot 2 > 0, \tag{21}$$

where g is the genus of an appropriate function field. The left hand inequality is satisfied already for $q \geqslant 9$. By Corollary 17, we have

$$g \leqslant (2 \cdot 2 - 1)6^{2-1}3^3 = 486;$$

and so the right hand inequality of (21) holds as soon as

$$\frac{1}{9}q - 108\sqrt{q} - 120 > 0,$$

which is valid for $q \geqslant 946943$, so certainly for $q > 10^6$. To complete the proof, choose an odd prime divisor l of $q^3 - 1$ (e.g., any prime divisor of $q^2 + q + 1$) and apply Lemma 21 to the pair $f, f + 1$ (taking $B = 6$ and $r = 2$). We obtain that for $q > 81$, there is some $\beta \in \mathbf{F}_q$ for which both $f(T^{l^k} - \beta)$

Table 1: For each odd prime power $q = 2^N + 1$ not exceeding 10^6, we exhibit a monic prime polynomial f of odd degree d over $\mathbf{F}_q$ for which $f + 1$ is also prime, together with the factorization of $q^d - 1$, the factorizations of the orders of f and $f + 1$, and an odd prime l for which Lemma 19 can be applied to both f and $f + 1$. We write P_9 for the 9-digit prime 116085511.

q	f	$q^d - 1$	**order of** f	**order of** $f + 1$	l
3	$T^3 - T + 2$	$2 \cdot 13$	13	26	13
9	$T^3 - T + 2$	$2^3 \cdot 7 \cdot 13$	13	26	13
5	$T^3 + 3T + 2$	$2^2 \cdot 31$	$2^2 \cdot 31$	$2^2 \cdot 31$	31
17	$T^3 + T + 8$	$2^4 \cdot 307$	$2^2 \cdot 307$	$2^2 \cdot 307$	307
257	$T^3 + T + 15$	$2^8 \cdot 61 \cdot 1087$	$2^5 \cdot 61 \cdot 1087$	$2^2 \cdot 61 \cdot 1087$	61
65537	$T^3 + T + 18$	$2^{16} \cdot 37 \cdot P_9$	$2^{15} \cdot 37 \cdot P_9$	$2^{15} \cdot 37 \cdot P_9$	37

and $f(T^{l^k} - \beta) + 1$ are simultaneously irreducible for $k = 1, 2, 3, \ldots$. This is an infinite family of twin prime pairs of odd degree. □

To finish off this half of Theorem 4, it remains to consider the cases when $q = 9$ or when q is a Fermat prime $< 10^6$. These small finite fields are treated by hand. For each such q, Table 1 exhibits the first member f of a monic twin prime pair $f, f + 1$ of odd degree together with all the information necessary to verify that Lemma 19 can be applied to both f and $f + 1$ with the specified odd prime l.

7.2 Part II: Infinitely Many Twin Prime Pairs of Even Degree

We first argue that for $q \geqslant 4$, there is always a monic, quadratic twin prime pair $f, f + 1$ over $\mathbf{F}_q$. In the proof of this result it is convenient to consider odd and even q separately.

Lemma 23. *Let $\mathbf{F}_q$ be a finite field of odd characteristic with $q \geqslant 5$. Then there is a pair $f, f + 1$ of monic irreducible quadratic polynomials over $\mathbf{F}_q$.*

Lemma 23 could be established by the methods of Theorem 2, in analogy with the proof of Lemma 22 in Part I. However, the direct approach below leads to better bounds.

Proof. It suffices to show that there is some pair of consecutive quadratic nonresidues in $\mathbf{F}_q$. Letting χ denote the quadratic character on $\mathbf{F}_q$, the number of such pairs is $\frac{1}{4}$ of the sum $\sum(1 - \chi(\alpha))(1 - \chi(\alpha + 1))$, the sum being taken over $\alpha \neq 0, -1$ from $\mathbf{F}_q$. Now a straightforward calculation using the evaluation $\sum_{\alpha \in \mathbf{F}_q} \chi(\alpha)\chi(\alpha + 1) = -1$ (cf. [BEW98, Theorem 2.1.2]) results in a count of

$$\frac{1}{4}\left(q - 3 + \chi(1) + \chi(-1)\right) = \frac{1}{4}\left(q - 2 + \chi(-1)\right)$$

such pairs, which is positive for $q > 3$. □

Lemma 24. *Let $\mathbf{F}_q$ be a finite field of characteristic 2 with $q \geqslant 4$. Then there is a pair $f, f + 1$ of monic quadratic polynomials both of which are irreducible over $\mathbf{F}_q$.*

Proof. For any fixed $\gamma \in \mathbf{F}_q$, the map $\phi\colon \mathbf{F}_q \mapsto \mathbf{F}_q$ defined by $\phi(\beta) := \beta^2 + \gamma\beta$ is an endomorphism of the underlying additive group of $\mathbf{F}_q$. We choose γ so that $\gamma \neq 0$ and the image of ϕ contains 1 (and so contains all of $\mathbf{F}_2$). This is possible as soon as $\mathbf{F}_q$ is a nontrivial extension of $\mathbf{F}_2$; merely choose any $\beta \in \mathbf{F}_q \setminus \mathbf{F}_2$ and define γ so that $\beta^2 + \gamma\beta = 1$.

We claim that with this choice of γ, there is a pair $f, f + 1$ of irreducibles where f has the form $T^2 + \gamma T + \delta$. A polynomial of this form is irreducible if and only if δ is not in the image of ϕ. But by our choice of γ, the element δ is missing from the image of ϕ if and only if the same is true for

Table 2: For each prime power $2 < q \leqslant 25$ we exhibit a monic prime polynomial f of even degree d over $\mathbf{F}_q$ for which $f+1$ is also prime, together with the factorization of q^d-1, the factorizations of the orders of f and $f+1$, and a prime l for which Lemma 19 can be applied to both f and $f+1$.

q	f	q^d-1	**order of** f	**order of** $f+1$	l
3	$T^6+T^5+2T^3+2T^2+1$	$2^3\cdot 7\cdot 13$	$2^2\cdot 7\cdot 13$	$2^3\cdot 7\cdot 13$	7
4	$T^2+T+\alpha$	$3\cdot 5$	$3\cdot 5$	$3\cdot 5$	3
5	T^2+T+1	$2^3\cdot 3$	3	$2^3\cdot 3$	3
7	T^2+T+3	$2^4\cdot 3$	$2^4\cdot 3$	$2^3\cdot 3$	3
8	$T^2+(\beta+1)T+\beta^2+\beta$	$3^2\cdot 7$	$3^2\cdot 7$	$3^2\cdot 7$	7
9	$T^2+(\gamma+1)T+\gamma+1$	$2^4\cdot 5$	$2^4\cdot 5$	$2^4\cdot 5$	5
11	T^2+3	$2^3\cdot 3\cdot 5$	$2^2\cdot 5$	$2^2\cdot 5$	5
13	T^2+6	$2^3\cdot 3\cdot 7$	$2^3\cdot 3$	$2^3\cdot 3$	3
16	$T^2+(\delta^2+\delta)T+\delta$	$3\cdot 5\cdot 17$	$3\cdot 5\cdot 17$	$3\cdot 5\cdot 17$	3
17	T^2+T+2	$2^5\cdot 3^2$	$2^4\cdot 3^2$	$2^5\cdot 3^2$	3
19	T^2+4	$2^3\cdot 3^2\cdot 5$	$2^2\cdot 3^2$	$2^2\cdot 3^2$	3
23	T^2+2	$2^4\cdot 3\cdot 11$	$2^2\cdot 11$	$2^2\cdot 11$	11
25	$T^2+4\epsilon T+4\epsilon+2$	$2^4\cdot 3\cdot 13$	$3\cdot 13$	$2^2\cdot 3\cdot 13$	3

Here $\alpha^2+\alpha+1=0$, $\beta^3+\beta+1=0$, $\gamma^2+1=0$, $\delta^4+\delta+1=0$, and $\epsilon^2+2=0$.

$\delta+1$. So the lemma follows provided that ϕ is not onto. Since ϕ is a map from $\mathbf{F}_q$ to itself, if ϕ were onto it would also be injective. But $\phi(\gamma)=\phi(0)=0$, and the lemma is proved. □

Lemma 25. *Let $\mathbf{F}_q$ be a finite field with $q>25$. Then there are infinitely many twin prime pairs $f, f+1$ of even degree over $\mathbf{F}_q$.*

Proof. Lemmas 23 and 24 show that for $q \geqslant 4$ there is a monic twin prime pair $f, f+1$ of degree 2 over $\mathbf{F}_q$. Since $q>3$, it is impossible for both $q-1$ and $q+1$ to be powers of 2, and so there must be an odd prime divisor l of q^2-1. Lemma 21 (with $r=2$ and $B=4$) implies that for $q>25$, there is some $\beta\in\mathbf{F}_q$ for which both $f(T^{l^k}-\beta)$ and $f(T^{l^k}-\beta)+1$ are simultaneously irreducible for $k=1,2,3,\dots$. Since these twin prime pairs have even degree, the lemma follows. □

To complete the proof of Theorem 4 it suffices to consider those finite fields with at most 25 elements, and these are treated in Table 2.

Acknowledgements

Mitsuo Kobayashi and Tom Shemanske read over preliminary versions of this paper and offered suggestions which proved indispensable in coaxing it into its present form. Particular thanks are due to my advisor, Carl Pomerance, both for his helpful advice and encouragement on the paper at every stage of its development and for his initial suggestion that I attempt to prove Theorem 2 in its present generality.

References

Ban86 A. S. Bang, *Taltheoretiske Undersøgelser*, Tidsskrift Math. **5** (1886), no. IV, 70–80, 130–137.

BEW98 B. C. Berndt, R. J. Evans, and K. S. Williams, *Gauss and Jacobi sums*, Canadian Mathematical Society Series of Monographs and Advanced Texts, John Wiley & Sons Inc., New York, 1998, A Wiley-Interscience Publication. MR MR1625181 (99d:11092)

BH62 P. T. Bateman and R. A. Horn, *A heuristic asymptotic formula concerning the distribution of prime numbers*, Math. Comp. **16** (1962), 363–367. MR 26 #6139

BSD59 B. J. Birch and H. P. F. Swinnerton-Dyer, *Note on a problem of Chowla*, Acta Arith. **5** (1959), 417–423 (1959). MR MR0113844 (22 #4675)

CCG06 B. Conrad, K. Conrad, and R. Gross, *Prime specialization in genus* 0, Transactions of the AMS (to appear), 2006.

Cho66 S. Chowla, *A note on the construction of finite Galois fields* GF(p^n), J. Math. Anal. Appl. **15** (1966), 53–54. MR MR0202703 (34 #2563)

Coh70 S. D. Cohen, *The distribution of polynomials over finite fields*, Acta Arith. **17** (1970), 255–271. MR MR0277501 (43 #3234)

Coh89 ———, *The reducibility theorem for linearised polynomials over finite fields*, Bull. Austral. Math. Soc. **40** (1989), no. 3, 407–412. MR MR1037635 (91b:11140)

Con05 K. Conrad, *Irreducible values of polynomials: a non-analogy*, Number fields and function fields—two parallel worlds, Progr. Math., vol. 239, Birkhäuser Boston, Boston, MA, 2005, pp. 71–85. MR MR2176587

Dic97 L. E. Dickson, *Higher irreducible congruences*, Bull. Amer. Math. Soc. **3** (1897), 381–389.

Dic58 ———, *Linear groups: with an exposition of the Galois field theory*, with an introduction by W. Magnus, Dover Publications Inc., New York, 1958. MR 21 #3488

EHM02 G. W. Effinger, K. H. Hicks, and G. L. Mullen, *Twin irreducible polynomials over finite fields*, Finite fields with applications to coding theory, cryptography and related areas (Oaxaca, 2001), Springer, Berlin, 2002, pp. 94–111. MR MR1995330 (2004h:11104)

EM99 J. Esmonde and M. R. Murty, *Problems in algebraic number theory*, Graduate Texts in Mathematics, vol. 190, Springer-Verlag, New York, 1999. MR 2000f:11137

FJ05 M. D. Fried and M. Jarden, *Field arithmetic*, second ed., Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics], vol. 11, Springer-Verlag, Berlin, 2005. MR MR2102046 (2005k:12003)

GJ98 W.-D. Geyer and M. Jarden, *Bounded realization of l-groups over global fields. The method of Scholz and Reichardt*, Nagoya Math. J. **150** (1998), 13–62. MR MR1633151 (99d:12001)

Hal06 C. Hall, L*-functions of twisted Legendre curves*, J. Number Theory **119** (2006), no. 1, 128–147.

Hay73 D. R. Hayes, *The Galois group of $x^n + x - t$*, Duke Math. J. **40** (1973), 459–461. MR MR0314804 (47 #3354)

HL23 G. H. Hardy and J. E. Littlewood, *Some problems of Partitio Numerorum III: on the expression of a number as a sum of primes*, Acta Math. **44** (1923), 1–70.

Kor19 H. Kornblum, *Über die Primfunktionen in einer arithmetischen Progression*, Math. Z. **5** (1919), 100–111, posthumously edited by E. Landau.

LN97 R. Lidl and H. Niederreiter, *Finite fields*, second ed., Encyclopedia of Mathematics and its Applications, vol. 20, Cambridge University Press, Cambridge, 1997, With a foreword by P. M. Cohn. MR 97i:11115

MS94 V. K. Murty and J. Scherk, *Effective versions of the Chebotarev density theorem for function fields*, C. R. Acad. Sci. Paris Sér. I Math. **319** (1994), no. 6, 523–528. MR MR1298275 (95j:11104)

Pol06 P. Pollack, *Irreducibility-preserving substitutions for polynomials over finite fields*, Submitted, 2006.

Ree71 R. Ree, *Proof of a conjecture of S. Chowla*, J. Number Theory **3** (1971), 210–212. MR MR0277502 (43 #3235)

Ree72 ———, *Erratum to: "Proof of a conjecture of S. Chowla"*, J. Number Theory **4** (1972), 223. MR MR0294293 (45 #3362)

Roi97 M. Roitman, *On Zsigmondy primes*, Proc. Amer. Math. Soc. **125** (1997), no. 7, 1913–1919. MR MR1402885 (97i:11005)

Ros02 M. Rosen, *Number theory in function fields*, Graduate Texts in Mathematics, vol. 210, Springer-Verlag, New York, 2002. MR MR1876657 (2003d:11171)

Ser66 J.-A. Serret, *Mémoire sur la théorie des congruences suivant un module premier et suivant une fonction modulaire irréductible*, Mémoires de l'Académie des sciences de l'Institut Impérial de France **35** (1866), 617–688.

Sie88 W. Sierpiński, *Elementary theory of numbers*, second ed., North-Holland Mathematical Library, vol. 31, North-Holland Publishing Co., Amsterdam, 1988, Edited and with a preface by Andrzej Schinzel. MR 89f:11003

Sti93 H. Stichtenoth, *Algebraic function fields and codes*, Universitext, Springer-Verlag, Berlin, 1993. MR MR1251961 (94k:14016)

Paul Pollack paul.pollack@dartmouth.edu
Department of Mathematics, Dartmouth College, Hanover, NH 03755