Contemporary Mathematics
Volume **00**, 0000

Global Construction of General Exceptional Covers

with motivation for applications to encoding

MICHAEL D. FRIED

ABSTRACT. The paper [**FGS**] uses the classification of finite simple groups and covering theory in positive characteristic to solve Carlitz's conjecture (1966). We consider only *separable* polynomials; their derivative is nonzero. Then, $f \in \mathbb{F}_q[x]$ is *exceptional* if it acts as a permutation map on infinitely many finite extensions of the finite field $\mathbb{F}_q$, $q = p^a$ for some prime p. Carlitz's conjecture says f must be of odd degree (if p is odd). The main theorem of [**FGS**; Theorem 14.1] restricts the list of possible *geometric monodromy groups* of exceptional *indecomposable* polynomials (§1.1): either $p = 2$ or 3 or these must be *affine groups*.

The proof of Carlitz's conjecture motivates considering *general exceptional covers* of nonsingular projective algebraic curves. For historical reasons we sometimes call these Schur covers [**Fr2**]. Suppose $\phi : X \to \mathbb{P}^1$ is an exceptional cover over $\mathbb{F}_q$. Then, for some integer s, there is a unique $\boldsymbol{x} \in X(\mathbb{F}_{q^t})$ over each $z \in \mathbb{P}^1(\mathbb{F}_{q^t})$ for *each* integer t with $(t, s) = 1$. In particular, $|X(\mathbb{F}_{q^t})| = q^t + 1$ when $(t, s) = 1$. We include a complete proof that exceptionality is equivalent to a statement about the geometric/arithmetic monodromy pair of the cover. Theorem 2.5 shows all geometric/arithmetic monodromy pairs satisfying necessary conditions (§1.1–§1.2) derive from covers over $\mathbb{F}_p$ for all suitably large primes p. Other topics:

(i) How modular curve points over finite fields explicitly produce rational function exceptional covers of prime degree (Corollary 3.5).
(ii) How fiber products produce abundant general exceptional covers (Lemma 3.7).
(iii) How Müller-Cohen-Matthews produced exceptional polynomials with nonsolvable monodromy group (§1.7).
(iv) How general exceptional covers realize curves of *high* genus over $\mathbb{F}_q$ with q small and $|X(\mathbb{F}_{q^{t'}})|$ *large* for some t' (§3.4–§3.5).

1991 *Mathematics Subject Classification*. Primary 12E20, 12E25, 12F12: Secondary 11G20, 11G25, 11G35, 11R58, 11T71.

Supported by NSA grant #MSPR-129-90 and NSF #DMS-99305590.

This paper is in final form and no version of it will be submitted for publication elsewhere.

We had several valuable talks with Noam Elkies. These included his comment that you could prove Median Value Curve Statement 3.11 using S-integers.

§0. INTRODUCTION

Here $\mathbb{F}_q$ denotes the finite field of order $q = p^a$ for some prime p and $\bar{\mathbb{F}}_q$ is its algebraic closure. The *monodromy method* (§1.1) applies to considerations of many polynomial properties over finite fields. A statement about a polynomial $f(x) \in \mathbb{F}_q[x]$ translates to properties of fibers of the cover $x \mapsto f(x) = z$ from $\mathbb{P}^1_x \to \mathbb{P}^1_z$. That is, f gives a degree $n = \deg(f)$ map from one copy of the projective line to another. In turn, properties of cover fibers translate to statements on the *geometric* and *arithmetic* Galois (monodromy) groups of the Galois closure covers. This brings in group theory: often effective in limiting the possibilities for geometric/arithmetic pairs of groups $(G, \hat{G})$ that arise from a cover. How effective depends on our ability to encode data about covers.

Even in considering polynomials, this step is nontrivial; we must group theoretically translate the data the cover is of genus 0 and totally ramifies at ∞. Further, we must reduce to situations commensurable with the present state of group theory. Today, the classification of simple groups has become a general tool for applications. In practice this means we can accomplish much if our groups have natural *primitive* permutation representations. The classification of exceptional polynomials (and general exceptional covers) is thus a serious test for group theory: We easily reduce to the case where the larger group $\hat{G}$ is primitive, but not so easily to where G is primitive.

It is inevitable that when group theory returns data to our original investigations, we are left with challenging problems. Which of the potentially allowable geometric/arithmetic pairs $(G, \hat{G})$ arise from an exceptional polynomial (resp. general exceptional cover)? Unless the potential pairs $(G, \hat{G})$ are utterly trivial, this presents arithmetic challenges. Classification of exceptional polynomials leaves us to consider the vast collection of *affine* groups; for general exceptional covers we have even more open territory. The outcome of [**FGS**] poses a marvelous test for generalizing the tools available for this last stage of the monodromy method. In some form or another, this requires further generalizations of arithmetic forms of *Riemann's Existence Theorem* to positive characteristics. We give evidence for the following ingredients to support this conception.

(0.1) The *monodromy method* is an appropriate tool for the classification of exceptional polynomials.

(0.2) Techniques successful on versions of the *inverse Galois problem* will find exceptional polynomials (and general exceptional covers) from the [**FGS**] restricted class of groups.

(0.3) Exceptional polynomials relate to broader finite field themes through general exceptional covers.

§0.1. Classifying exceptional polynomials. For item (0.1), §1 outlines the place of Carlitz's conjecture in the complete classification of exceptional polynomials. Is this classification imminent? Justifying that possibility is one goal of this paper. Carlitz conjectured a limitation on degrees of exceptional

polynomials over odd order finite fields. Still, the abstract negative result from [**FGS**] points to hiding places for unsuspected examples. Suppose $f \in \mathbb{F}_q[x]$ is a composition $f_1(f_2(x))$ with $f_1, f_2 \in \mathbb{F}_q[x]$. Then, f permutes the elements of $\mathbb{F}_q$ if and only if both f_1 and f_2 do also. Thus, for the main ingredients of a classification, we may assume f is indecomposable (see Exceptionality Lemma 1.1): the arithmetic monodromy group is *primitive*.

Affine groups were the main groups to pass through the classification filter in [**FGS**]. These are always of prime power degree, and excluding easy cases, the prime is the same as the characteristic of $\mathbb{F}_q$. This gave the proof of Carlitz's conjecture. Yet, it left the possibility of many unknown affine groups arising from exceptional polynomials. Excluding affine groups, the only possible monodromy groups of indecomposable exceptional polynomials occur in characteristics $p = 2$ or 3. These have $n = q(q-1)/2$ with $q = p^a$, $a \geq 3$ and a odd, and G normalizes $\mathrm{PSL}_2(\mathbb{F}_q)$ in its transitive representation on n points. Here n is the degree of the possible exceptional polynomial. This is precise, but the main point is how would you check if there is a polynomial that produces such a group?

Müller traces the above group in the case $a = 3$ and $p = 2$ to a finite collection of exceptional polynomials in characteristic 2 (not part of Carlitz's conjecture). These are the first examples of exceptional polynomials with nonsolvable monodromy groups. We discuss Müller's method for his degree 28 example in §1.7. It inspired Cohen and Matthews to generalize this for all odd values of a. This is a practical illustration of item (0.2). We anticipate more general and abstract lessons coming from listing affine groups that are the geometric monodromy group of an exceptional polynomial. Also, the case $p = 3$ gives odd degree representations of classical Chevalley groups over $\mathbb{F}_{3^a}$. Theorem 2.5 (more below) gives the spirit of what we have in mind for mentioning the inverse Galois problem in (0.2). It shows each of these groups appears as the monodromy group of a general exceptional cover over *each* finite field of suitably large characteristic.

§**0.2. General exceptional covers and fiber products.** In §2 we support item (0.3) using the notion of *general exceptional cover*. This is the most exciting development. A (nonsingular absolutely irreducible projective) curve X that appears as a general exceptional cover has this amazing diophantine property:

(0.4) X has exactly $q^t + 1$ points over $\mathbb{F}_{q^t}$ for infinitely many t.

Indeed, the values t for (0.4) are those relatively prime to a critical integer s (Exceptionality Lemma §1.2). You can express this property of X through the *zeta function* of X. We call X satisfying (0.4) a *median value* curve. Median Value Curve Statement 3.11 says this implies there is an integer s_X such that (0.4) holds for all t with (t, s_X)=1. Thus, exceptional polynomials are part of explicitly counting points on curves over finite fields. The Riemann hypothesis for curves over finite fields gives us the famous *Weil bound* $2gq^{\frac{t}{2}}$. This bounds the difference between q^t+1 and the number of points on X (of genus g) over $\mathbb{F}_{q^t}$. For median value curves, the Weil bound is clearly overkill for t with $(t, s) = 1$.

Even, however, when $(t, s) \neq 1$, when g is large compared to q^t, the Weil bound is a poor approximate truth for rational points on X. For example, the Weil bound may exceed the total of rational points in the ambient projective space for the curve.

Coding theory problems connect to curves over finite fields with many rational points. Thus, they encourage us to investigate the discrepancy between the Weil bound and actual realizations of rational points. We explain (§3.4–3.5) why median value curves contribute to production of curves with an abundance of rational points. The values of t, however, which have X be median are different from the values of t which have it exceed the median. In particular, we use (twists of) fiber product constructions to produce collections of such curves from exceptional covers. Achieving the Weil bound happens when a curve has a Jacobian variety isogenous over the algebraic closure of the finite field to a product of supersingular elliptic curves (see §3.5). This doesn't, however, answer many cryptology questions because it is unclear which curves have this property and they don't arise in sufficient abundance to satisfy coding theorists. It doesn't at all tell us a complete story on median value curves, nor the subset of exceptional polynomials. Still, Example 3.14, derived from [**GV**], entwines coding with general exceptional covers.

With this motivation, we highlight our main theorem. As with exceptional polynomials, exceptional covers have their associated geometric and arithmetic monodromy groups G and $\hat{G}$. The General Exceptionality Theorem (§2.2) gives precise necessary conditions for the pair $(G, \hat{G})$ to arise from an exceptional cover. They are also sufficient. Given that $(G, \hat{G})$ satisfy these conditions, the production of exceptional covers requires techniques previously applied to the *Inverse Galois Problem* (Theorem 2.5). Many problems remain in clarifying the scope of these existence results and their connection to coding theory (§3).

Throughout these examples, primitive covers $X \to Y$ play a special role. Fiber products give a handy criterion for a cover to be primitive (Prop. 3.6). This came from an e-mail discussion with J. Gutierrez [**AGR**]. We also include a complete proof (from [**FGS**, §11] and [**Fr3**]) of equivalence of (0.4) with

(0.5) the fiber product test for exceptionality (§2.2).

This result has a long history: see Exceptionality Lemma §1.2, General Exceptionality Theorem 2.1 and §2.3 for comments on priority.

§**0.3. Comments on the scope of the Čebotarev analogs.** The *nonregular analog of the Čebotarev Density Theorem* is a powerful tool. It translates many statements on points on curves over finite fields into group theory. Still, there are special loci—used in a general sense—for which the translation is inadequate. Primarily there are two: when the defining finite field is small, or when relevant points lie over ramified points in a cover. For Schur covers, however, (0.5) implies exceptionality, and this implies (0.4). This is with no exception, in the finite field of definition, or equivocation (leaving out a few points). Thus,

with some extra work, the Čebotarev Theorem tells the full story. Adherents of the area appreciate this. We show the potential for expanding this argument to other applications where one readily applies Čebotarev analogs (§1.4). Indeed, much of §1 is exposition to acquaint readers with the monodromy method and how to interpret old arguments with these relatively young tools.

§**0.4. The Inverse Galois Problem and modular curves.** Theorem 2.5 is our main theoretical offering to produce exceptional covers by inverting the monodromy method. It shows that a geometric/arithmetic pair satisfying the Exceptionality Theorem arises from an exceptional cover over most prime finite fields. The present state, however, of the theory that produces these covers doesn't allow much control on the genus, nor on the excluded primes. This isn't an intrinsic difficulty with the theory. Partly, it is just its newness: we lack experience with the large amount of information available from the theory.

In this direction we elaborate an example from [**Fr4**]. §3 discusses covers with geometric monodromy group $D_{p'}$, the *dihedral* group of odd prime degree p', not equal to the characteristic. A subcase of this includes exceptional covers coming from rational functions (rather than polynomials) of prime degree. Most such covers correspond to finding special rational points on modular curves over finite fields (Cor. 3.5). It is still our best explicit source of the spaces that appear in the proof of Theorem 2.5. With them we have historical motivation for properties of spaces that would classify exceptional covers of a given type (as at the end of §1.7). Even easy groups—specifically dihedral groups—are nontrivial if we want to classify exceptional covers.

§**0.5 Abhyankar's conjecture and exceptional covers.** An analog of Theorem 2.5 would be even more valuable. It would say something like this. Let p be a fixed prime and $(G, \hat{G})$ a geometric/arithmetic pair that passes the criterion of the General Exceptionality Theorem.

p-Analog of Theorem 2.5. *For q, a large power of p, there exists an exceptional cover over $\mathbb{F}_q$ having $(G, \hat{G})$ as its geometric/arithmetic pair.*

Actually, the proof of Theorem 2.5 provides a proof ([**FrV3**] will discuss this). Yet, it is unsatisfactory. Theorem 2.5 has the potential to give precise information on the ramification allowed in exceptional covers with a given geometric/arithmetic pair, when the characteristic of the field is suitably large. Yet, for a fixed characteristic we lack a true replacement for *Riemann's existence theorem*. We have only an awkward understanding of covers that arise over the projective line even over $\bar{\mathbb{F}}_q$. What we do know comes from the recent proof of Abhyankar's conjecture ([**H**] and [**Ra**]). This tells exactly which groups arise as geometric monodromy groups of covers of $\mathbb{P}^1_z$ ramified at a given $r > 0$ points. These are precisely groups G for which G/G_P requires less than r generators. Here P denotes a p-Sylow of G; and G_P is the subgroup of G generated by all conjugates of P. An improvement on the p- Analog of Theorem 2.5 would show this for a given geometric/arithmetic pair $(G, \hat{G})$ as in the statement above.

CONJECTURED p,r-ANALOG OF THEOREM 2.5. *Assume $r-1$ elements generate G/G_P. Then, for q a suitably large power of p, there exists an exceptional cover over $\mathbb{F}_q$ having $(G,\hat{G})$ as its associated geometric/arithmetic pair.*

Note: From [**FGS**] our main concern (excluding $p = 2$ or 3) is with affine groups if we restrict to polynomial covers. Unlike, however, Abhyankar's conjecture over $\bar{\mathbb{F}}_p$, our question has an arithmetic component. Further, we should be considering this: When is there an indecomposable exceptional polynomial having this group as geometric monodromy group? There are known limitations on the monodromy groups of polynomials over finite fields. For example, Guralnick and Saxl have shown most Chevalley groups don't occur as the geometric monodromy group of a polynomial cover [**GS**]. This direction leaves many unsolved problems. We hope to address some in a later paper.

0.6 A final question. §1.e of [**FGS**] paints an historical picture of activity around Carlitz's conjecture. It also alludes to M. Aschbacher and J.-P. Serre commenting on the classification of finite simple groups. I was Don Lewis's student in graduate school 1964–1967 at University of Michigan. During visits of Davenport and Schinzel I heard much about the Schur conjecture. Essentially: The polynomials (over $\mathbb{Q}$) that are one-one mod p for infinitely many p are compositions of twists of cyclic and chebychev polynomials [**Fr2**]. Thus, it was natural to apply tools around the *monodromy method* (§1 and [**Fr1**]) to Schur's conjecture. For personal reasons, 1992 was an appropriate time for me to return to the area. The luck of success prompts me to pose one further question.

From the beginning, while Guralnick, Saxl and I worked on [**FGS**], I was certain Carlitz's conjecture would be false. This scepticism, was valuable. For example, while checking group-theoretic-computations we came upon several rough arguments through which counterexamples could easily slip. One almost proved the undoing. We established the general situation for indecomposable exceptional polynomials: Their degrees are a power of the characteristic. Thus, they are of odd degree. (This excludes exceptional polynomials of degree relatively prime to p that are twists of cyclic and chebychev polynomials.) Yet, in characteristic $p = 2$ and 3, we couldn't exclude polynomials of degree $p^a(p^a-1)/2$ with a odd. Check for $p = 3$ to see how close this is to even. Müller's example (§1.4) shows these weren't accidents.

So, how could Carlitz have guessed his conjecture was true, without exception, in such generality? (As an analog, consider the finitely many counterexamples in the Artin conjecture by Ax and Kochen, and the fudging required in Artin's primitive root conjecture.) Yet, there were no exceptions in the Carlitz conjecture. Did any of his papers express an appropriate insight in this direction?

§1. BACKGROUND ON CARLITZ'S CONJECTURE

We use the notation $\bar{K}$ for the algebraic closure of a field K. The proof of the Schur conjecture handles Carlitz's conjecture when $(\deg(f),p) = 1$ [**Fr2**].

For this case, the polynomial is a composition of (twists of) cyclic and chebychev polynomials reduced from characteristic 0. When a nontrivial power of p divides $\deg(f)$, proving Carlitz's conjecture requires new techniques. Recall: A polynomial is *indecomposable* (over $\mathbb{F}_q$) if it isn't a composition of polynomials over $\mathbb{F}_q$ of smaller degree. The Exceptionality Lemma (§1.2) shows we may, with no loss, take exceptional polynomials to be monic and *indecomposable* over $\mathbb{F}_q$. Our statements below make this assumption.

When $\deg(f) = p$, f is from an explicit collection [**FGS**, Theorem 1]. Consider an integer k that divides $p-1$. Over any $\mathbb{F}_q$ a rational variety pleasantly parametrizes exceptional f having geometric monodromy group (§1.1) equal to the semi-direct product of $\mathbb{Z}/k$ acting naturally on $\mathbb{Z}/p$ as multiplications by invertible integers. When $\deg(f) = p$, these are the only possibilities. If, however, $\deg(f) = mp$, $(m,p) = 1$ and $m > 1$, then f cannot be exceptional. This is a special case of the main theorem of [**FGS**].

§**1.1. Producing monodromy groups.** Regard f as a map from affine x to affine z space: $f : \mathbb{A}^1_x \to \mathbb{A}^1_z$ by $x \mapsto f(x) = z$. Consider the fiber product:

$$Y_f = Y = \mathbb{A}^1_x \times_{\mathbb{A}^1_z} \mathbb{A}^1_x \stackrel{\text{def}}{=} \{(x_1, x_2) \mid f(x_1) = f(x_2)\}.$$

Remove the diagonal Δ from Y. Suppose $Y \setminus \Delta$ has at least one absolutely irreducible component Y_1 defined over $\mathbb{F}_q$. For q large compared to $\deg(f)$, the Lang-Weil estimate says Y_1 has $\mathbb{F}_q$ points. These would be points $(x_1, x_2) \in \mathbb{F}_q^2$ such that $f(x_1) = f(x_2)$, but $x_1 \neq x_2$. So, f would not be one-one on $\mathbb{F}_q$.

Thus, if f is exceptional,

(1.1) no irreducible component of $Y \setminus \Delta$ is absolutely irreducible over $\mathbb{F}_q$.

That is, each component decomposes further over the algebraic closure $\bar{\mathbb{F}}_q$. Use K for $\mathbb{F}_q$. Consider the Galois closure $\widehat{K(x)}$ of the extension $K(x)/K(z)$ in its natural permutation representation of degree $n = \deg(f)$. Denote the Galois group $G(\widehat{K(x)}/K(z))$ by $\hat{G} = \hat{G}_f$: the *arithmetic monodromy group* of f.

The field $\hat{K} \stackrel{\text{def}}{=} \widehat{K(x)} \cap \bar{K}$ is the key in arithmetic interpretation of exceptional polynomials. The group $\hat{G}$ has $G(\widehat{\bar{K}(x)}/\bar{K}(z)) = G = G_f$ as a normal subgroup: the *geometric* monodromy group of f. Both groups act on the n roots $x_1, \dots, x_n$ of the equation $f(x) = z$. This turns them into transitive subgroups of S_n. Denote the respective stabilizers of 1 of this representation by $\hat{G}(1)$ and $G(1)$, respectively. These act on $\{2, \dots, n\}$.

§**1.2. Exceptionality and ramification over ∞.** The goal is a complete group theoretic statement about the pair $(G_f, \hat{G}_f)$ that interprets exceptionality. For this, replace x by one root x_1 of $f(x) - z$. Then, orbits of $G(1)$ on $x_2, \dots, x_n$ correspond to components of $Y \setminus \Delta$ over $\bar{\mathbb{F}}_q$. Similarly, orbits of $\hat{G}(1)$ correspond to components of $Y' = Y \setminus \Delta$ over $\mathbb{F}_q$.

Exceptionality Lemma 1.1 [**Fr1**, §3]. *An $f \in \mathbb{F}_q[x]$ is exceptional if and only if $\hat{G}(1)$ fixes no orbit of $G(1)$ on $\{2, \dots, n\}$. In particular, G is not doubly*

transitive. Denote $[\hat{G} : G]$ *by* s. *If* f *is exceptional, then* f *is exceptional over* $\mathbb{F}_{q^v}$, *for each* v *with* $(v, s) = 1$. *Suppose* f *is a composition of* $f_1, f_2 \in \mathbb{F}_q[x]$. *Then,* f *is exceptional if and only if both* f_1 *and* f_2 *are exceptional.*

Total ramification over ∞. We clarify interpreting f being a polynomial. This is the statement that the cover $f : \mathbb{A}^1_x \to \mathbb{A}^1_z$ *ramifies totally* over ∞. Total ramification produces a crucial subgroup of G_f—the *inertia group* G_∞ over ∞. By definition, G_∞ is the group of the splitting field of $f(x) - z$ over the field $\bar{\mathbb{F}}_q((1/z))$ of Laurent series in $1/z$. It is transitive with a normal p-Sylow H:

(1.2) G_∞/H is cyclic and has order a multiple of m where $n = mp^a$ with $(p, m) = 1$.

Assume with no loss f is monic. When $a = 0$, G_∞ is cyclic of order n. Display this group by expressing a zero x_1 as a Laurent series in $z^{\frac{-1}{n}}$:

$$x_1 = z^{\frac{1}{n}} + a_0 + a_1 z^{\frac{-1}{n}} + a_2 z^{\frac{-2}{n}} + \dots$$

Determine each successive a_i by plugging back into the equation. Produce the other zeros of $f(x) - z$ from x_1 by applying the substitution $\sigma : z^{\frac{-1}{n}} \mapsto \zeta_n z^{\frac{-1}{n}}$ with $\zeta_n = e^{2\pi i/n}$. Then, σ generates G_∞.

It's not so easy to calculate G_∞ when $a > 0$. If $a = 1$, the p-Sylow H is a product of copies of $\mathbb{Z}/p$. In fact, the G_∞-Lemma of [**FGS**, §4.c] shows how to compute the rank of H over $\mathbb{Z}/p$ in this case. Any group, however, satisfying (1.2) can be the inertia group over ∞ of some polynomial in characteristic p.

§**1.3. Using Burnside's Theorem.** Consider the case when degree of f is p. Then, we know much about $G = G_f$. The Exceptionality Lemma implies it can't be doubly transitive. Burnside's Theorem says a degree p, not doubley transitive group, must be a subgroup of $\mathbb{Z}/p \times^s (\mathbb{Z}/p)^*$. From the Riemann-Hurwitz formula:

$$2(p + g - 1) = \sum_{i=1}^{r} \mathrm{ord}_{x \in \mathbb{P}^1_x}(D_x). \tag{1.3}$$

Here D_x is the *different* of the cover computed at points $x \in \mathbb{P}^1_x$. Also, g is the genus of the curve covering: the genus of $\mathbb{P}^1_x$ is 0. The following is now a simple computation from (1.3). The element τ denotes a generator of the cyclic inertia group for the one finite ramified place z_0.

Ramification Lemma 1.2 [**FGS**, §8]. *Assuming the above,* $f : \mathbb{P}^1_x \to \mathbb{P}^1_z$ *has but one finite branch point* z_0. *Above* z_0, $\frac{p-1}{k}$ *points of* $\mathbb{P}^1_x$ *ramify, each of index* $k = \mathrm{ord}(\tau)$. *One point above* z_0 *does not ramify. The rest of the ramification lies over* ∞.

Put $t = \frac{p-1}{k}$. With linear change of variables we conclude

(1.4) *normalized* exceptional polynomials are of form $f(x) = x(x^t + b)^k$.

The polynomial of (1.4) is exceptional exactly when $x^t + a$ has no zeros over $\mathbb{F}_q$.

Also, if the $\deg(f)$ is a prime $p' \neq p$, the same computation with Burnsides' Theorem and (1.3) gives these conclusions [Fr2]. Either, the cover has one finite totally ramified place (a cyclic cover) or, there are two finite branch points with involutions as inertia groups. In the latter case G is the dihedral group $D_{p'}$. Also, if $p \not| n$ and n is not a prime, then Schur's Theorem implies the monodromy group is doubly transitive. Again, the Exceptionality Lemma excludes this case.

§**1.4. Exceptional versus permutation polynomials.** The story for exceptional polynomials is clear and complete when $\deg(f) = p$ [**FGS**, Theorem 8.1]. Dickson's 1896 conjecture [**D**] predicted the form of a degree p (normalized) exceptional polynomial to be as in (1.4). G. Turnwald, however, discussed with me how that conjecture relates to a complete description of all permutation polynomials of degree p. Here we have a subtler relation. Discussing this illustrates an area mentioned in §0.3 where Čebotarev methods need improvement.

Consider a degree p permutation polynomial f over $\mathbb{F}_q$ that is not exceptional. The previous argument, using Burnside's Theorem, shows one of two events occurs. Either: $Y' = Y \setminus \Delta$ (§1.1) is absolutely irreducible over $\mathbb{F}_q$; or a change of variables gives the form (1.4). Consider a case: Can a *general* degree p polynomial f over $\mathbb{F}_q$ be permutation? The answer is yes if you take $q = p$. Such a monic polynomial would have these properties.

(1.5a) $f(x) = x^p + a_1x^{p-1} + \cdots + a_p$, with $a_1 = 0$.

(1.5b) $\frac{df}{dx}(x)$ has $p-2$ distinct zeros, whose images under f are also distinct.

With no loss consider the case when $a_p = 0$. Take α to be a generator of $\mathbb{F}_p^*$. Let $b_1, \ldots, b_{p-1}$ be *any* ordering of $\mathbb{F}_p^*$. Consider finding f with this property:

$$f(\alpha^i) = b_i, i = 1, \ldots, b_{p-1}.$$

Rewrite this as $V_\alpha(\boldsymbol{a}') = \boldsymbol{b}$. Here V_α is the Vandermonde matrix for the $p-1$ distinct powers of α, $\boldsymbol{a}' = (a_1, a_{p-2}, \ldots, a_2 + 1)$ and $\boldsymbol{b} = (b_1, \ldots, b_{p-1})$. For example:

(1.6) $f(\alpha^j) = a_1 + (a_{p-1}+1)\alpha^j + a_{p-2}\alpha^{2j} + \cdots + a_2\alpha^{(p-2)j} = b_j$, $j = 1, \ldots, p-1$ has a unique solution in $a_1, \ldots, a_{p-1}$.

It is, however, harder to know when to expect a permutation, not exceptional, polynomial of degree p, over a proper extension of the prime field. We analyze this when (1.5) holds.

Let $\bar{Y}'$ be a projective normalization of Y'. Then, $\phi(x, y) = \frac{f(x)-f(y)}{x-y} = 0$ describes an affine portion Y' of $\bar{Y}'$. By the properties of normalization, $\bar{Y}'$ has a natural degree $p-1$ map to the x-line continuing the projection $(x, y) \mapsto x$. The following lemma is the easiest case of an argument from [**Fr6**, p. 231–234].

LEMMA 1.3. *Assume only (1.5a). Then, Y' is totally ramified over $x = \infty$.*

OUTLINE OF PROOF. Find y in $\phi(x, y) = 0$ as a Puiseux series in x. Write

$$y = x + b_{p-2}x^{\frac{p-2}{p-1}} + b_{p-3}x^{\frac{p-3}{p-1}} + \ldots.$$

Substitute y in $\phi(x,y)$. Use that all terms of the expansion must be identically 0 to solve for the coefficients $b_{p-2}, b_{p-3}, \dots$. The highest non-identically zero term is $b_{p-2}^p x^{\frac{p(p-2)}{p-1}} - a_1 b_{p-2} x^{p-2+\frac{p-2}{p-1}}$. Draw this conclusion: $b_{p-2}^p - a_1 b_{p-2} = 0$. The $p-1$ nonzero solutions for b_{p-2} give the beginning terms of the $p-1$ distinct Puiseux expansions for solutions y of $\phi(x,y)=0$. For any one of these, inductively (and uniquely) solve for the remaining coefficients $b_{p-3}, \dots$. □

Let x' be one of the $p-2$ unramified points lying over one of the $p-2$ finite branch points z' of the cover $f : \mathbb{P}^1_x \to \mathbb{P}^1_z$. Then, there is one ramified point $(x', y') \in Y'$ of order 2 over x'. Here, y' is the unique ramified value of x lying over z'. Thus, not counting the point over ∞, Y' has $(p-2)(p-2)$ points of ramification over $\mathbb{P}^1_x$, all of order 2. Apply (1.3): the genus g' of (the projective closure of) Y' satisfies

$$2(p-1+g'-1) = (p-2)(p-2) + (p-2). \tag{1.7}$$

The last summand of $p-2$ is the contribution over ∞. This is the worst case scenario for the genus. It gives us the following result even without the assumptions of (1.5). Related remarks appear in [**LN**, Lemma 7.28] and [**C2**].

Permutation Territory Theorem 1.4. *Suppose f is a degree p permutation, but not exceptional, polynomial over a finite field $\mathbb{F}_q$. Let $\bar{Y}' \to \mathbb{P}^1_x$ the cover deriving from Y' as above. The genus of $\bar{Y}'$ does not exceed $\frac{(p-2)(p-3)}{2}$. In particular, if $q > p^3$, a permutation polynomial of degree p over $\mathbb{F}_q$ must be exceptional.*

Outline of Proof. Solve for g' in (1.7) to compute the extreme possible value for the genus of Y'. The Weil estimate gives the number of points over $\mathbb{F}_q$ on Y' as N with

$$|q+1-N| \le (p-2)(p-3)q^{\frac{1}{2}} \text{ [**FJ**, Chap. 4].} \tag{1.8}$$

Denote the diagonal of $\mathbb{P}^1_x \times_{\mathbb{P}^1_z} \mathbb{P}^1_y$ by Δ. The curve Y' has an affine representative in (x,y)-space of degree $p-1$. Let N_Δ be the number of points on Y' that are also on Δ. For a general polynomial we bound this by $p-1$. Thus, if N exceeds $p-1$, f is not a permutation polynomial. In particular, if $q+2-p$ exceeds $(p-2)(p-3)q^{\frac{1}{2}}$, such an f cannot be a permutation polynomial. Check: For $q \ge p^4$ such an inequality doesn't hold. □

We did the analysis above to show how to explicitly compute the genus of Y'. For detailed analysis in cases where f isn't general, this replacement of Bezout's Theorem is essential in a problem of such delicacy. Still, Theorem 1.4 is inadequate; when the genus of a curve is large compared to q, the Weil bound says little. That is precisely the situation for the curve Y' above. Many papers now consider how to improve the Weil bound for this circumstance. There are programs to produce curves of large genus over $\mathbb{F}_q$ with many rational points (for example, [**E**], [**GV**], [**GV1**], [**MM**], [**Se**]). Note, however, our problem is the

curve Y' might have exceptionally few points. §3.4-§3.5 treats other aspects of this phenomenon. The papers [**K**], [**Ma**] and [**MM**] use p-adic methods. They generalize Chevalley's theorem that the number of rational points of a form of degree d in $d+1$ variables over $\mathbb{F}_q$ is divisible by p. In particular, they inspect the power of p that divides the number of rational points; moreover, they are aimed at higher dimensional varieties.

§**1.5. The case $2p$ of Cohen [C] and Wan [W].** This argument is from the introduction of [**FGS**]. It illustrates the power of group theory by showing there are no exceptional polynomials of degree $2p$. In particular, it proves Carlitz's conjecture for such degrees.

Suppose f is exceptional and $\deg(f) = 2p$. If f *decomposes* over $\mathbb{F}_q$, then $f = f_1(f_2)$ with $f_1, f_2 \in \mathbb{F}_q[x]$. Either $\deg(f_1)$ or $\deg(f_2)$ is 2, and both polynomials are exceptional. It is trivial to show that a polynomial of degree 2 cannot be exceptional. Conclude: f is indecomposable over $\mathbb{F}_q$. If f is indecomposable over $\bar{\mathbb{F}}_q$, then its *geometric monodromy group* G is *primitive*.

Wielandt [**We**] says a primitive group of degree $2p$ is rank two (doubly transitive) or three. That is, the stabilizer of an integer has one or two orbits acting on $\{2, \dots, n\}$. Interpret this to say that $\phi(x, y) = \frac{f(x)-f(y)}{x-y}$ has one or two irreducible factors over $\bar{\mathbb{F}}_q$. Yet, each irreducible factor of ϕ over $\mathbb{F}_q$ factors into smaller degree polynomials—each of the same degree—over $\bar{\mathbb{F}}_q$. Thus, ϕ must have two factors of the same degree. Since ϕ is of odd degree, this is impossible.

Finally, consider f that is indecomposable over $\mathbb{F}_q$, but it is decomposable over $\bar{\mathbb{F}}_q$. We show group theoretically this is impossible. Take $(G, \hat{G})$ to be the geometric/arithmetic monodromy groups of f. Then $\hat{G}$ is primitive of degree $2p$ and G is a nontrivial normal subgroup. Denote the stabilizer of 1 of a subgroup H of $\hat{G}$ by $H(1)$.

LEMMA 1.5. *Under the hypotheses above, G is primitive.*

PROOF. Let A be a minimal normal subgroup of $\hat{G}$. If we show A is primitive, then any group containing A is primitive. In particular, G is.

Since $\hat{G}$ is primitive, A is transitive. Suppose $A(1)$ is not maximal. Consider M properly between $A(1)$ and A. Thus either $[A : M] = 2$ or $[M : A(1)] = 2$. In the first case the intersection of the $\hat{G}$ conjugates of M is normal in $\hat{G}$. Thus, this intersection must be trivial. Since A is a product of isomorphic simple groups, it is an elementary abelian 2-group. Yet, A is transitive. So $2p$ divides $|A|$, a contradiction.

In the second case, $A(1)$ is normal in M. It is also normal in $\hat{G}(1)$. If $A(1) = \{1\}$, conclude a contradiction as above to A being a 2-group. Thus, $A(1) \neq \{1\}$. Since $\hat{G}(1)$ is maximal, $\hat{G}(1)$ is the full normalizer of $A(1)$. In particular, $M \leq \hat{G}(1)$. Conclude $M = A(1)$, a contradiction. □

§**1.6. Role of classification and Main Theorem of [FGS].** Here are two places in the proof of the main theorem of [**FGS**] that give a flavor of the

nontrivial appearance of the classification. There are others. The first is purely from the classification.

LEMMA 1.6 [**FGS**, Lemma 12.4]. *Let L be a nonabelian simple group. There exist two distinct primes that divide $|L|$, but not $|\mathrm{Out}(L)|$, the outer automorphism group of L.*

The truth of this opens to two keys. Key1: Sporadic simple groups and alternating groups have tiny outer automorphism groups. Key 2: For the Chevalley groups there are formulas for the orders of the groups and their automorphism groups expressed as products of terms of the form $q^t - 1$.

Now consider the second use of the classification. Since G_∞ is transitive, $\hat{G} = \hat{G}(1) \cdot G_\infty$. This is the meaning of a *factorization* of a group $\hat{G}$. Also, $\hat{G}(1)$ is maximal; that is the meaning of primitivity. Liebeck, Praeger, and Saxl [**LPS**] have found a list of all maximal factorizations of *almost simple groups*. The list is complicated, but our conditions allow effective use of it.

Assume f is an exceptional, indecomposable polynomial over a finite field $\mathbb{F}_q$. As above, we start by limiting all possibilities for geometric and arithmetic monodromy groups of such polynomials. An extensive discussion in [**FGS**, §9–§11] advocates for a form of Riemann's existence theorem in positive characteristic to describe which of these produce exceptional polynomials. A later paper will return to this by following the lead of [**Fr6**, p. 231–234]. We describe Theorem 14.1 of [**FGS**]. Exclude the case $p \not| \deg(f)$ and $p = \deg(f)$ from §1.3.

p different from 2 or 3. Indecomposable exceptional polynomials have geometric monodromy group an *affine group*. These are of form $V \times^s G(1)$. Here V is a vector space of dimension p^a. Also, $G(1)$ is a subgroup of $GL(V)$ acting irreducibly on V: there is no group properly between $G(1)$ and $V \times^s G(1)$. That is, the group is primitive in its action on V. In this case, [**FGS**] says the degree of f is p^a. When p is odd, p^a is odd. This thereby solves Carlitz's conjecture, except for the case $p = 3$ (below).

Here is the next step to classifying all exceptional polynomials when $(p, 6) = 1$. Find which groups $V \times^s G(1)$ occur as geometric monodromy groups of exceptional polynomials. Our next subsection describes the first known nonsolvable groups that are monodromy groups of exceptional polynomials. Theorem 11.1 of [**FGS**] completes the case when $G(1)$ is a cyclic group C (acting irreducibly on V). These include all examples known except those of §1.7.

$p = 2$ or 3. Of course, there are the analogs of the case of $p > 3$: G an affine group of degree p^a. Other than these, exceptional polynomials have $n = p^a(p^a - 1)/2$ with $a \geq 3$, a odd, and G normalizes $PSL_2(\mathbb{F}_{p^a})$ in its transitive representation on n points. Fortunately, $3^a - 1 \equiv 2 \bmod 4$ when a is odd. So, these characteristic 3 possibilities don't give counterexamples to Carlitz's conjecture.

§1.7. Müller and Cohen-Matthews examples when $p = 2$. Müller's

Theorem 2 [**Mu**] considers the nonaffine group case when $p = 2$ and $a = 3$ ($n = 28$). It is easy that

$$f_1 = x(1 + x^9 + x^{27}),\ f_2 = x(1 + x^3 + x^9)^3, \text{ and } f_3 = x(1 + x + x^3)^9 \tag{1.9}$$

are indecomposable over $\bar{\mathbb{F}}_p$. In addition, they are permutation polynomials over all extensions of $\mathbb{F}_2$ of degree relatively prime to 3. Their geometric and arithmetic monodromy groups are $\mathrm{PGL}_2(8)$ and $\mathrm{P\Gamma L}_2(8)$, respectively.

How Müller got his examples. The group theory from [**FGS**] shows an example of an exceptional polynomial f over $\mathbb{F}_2$ of degree 28 would be exceptional over $\mathbb{F}_{2^m}$ with $(m, 3) = 1$. Without loss take $f(0) = 0$. He considers the complete set of permutation polynomials on $\mathbb{F}_{2^4}$ with coefficients in $\mathbb{F}_2$ that take 0 to 0. These commute with the Frobenius σ (square map). He writes the permutation σ on $\mathbb{F}_{2^4}$ and easily lists all permutations that commute with it. Use that x^{16} is the identity on $\mathbb{F}_{2^4}$ to count 2^{12} polynomials of degree 28 in $\mathbb{F}_2[x]$ induce a given permutation on $\mathbb{F}_{2^4}$.

Finally, Müller asks the computer program **GAP** to list all interpolation polynomials for each such polynomial. He checks all $768 \cdot 12$ of them for being a permutation polynomial on $\mathbb{F}_{2^5}$. From the few survivors, he checks the factorization of $\phi(x, y)$ for application of the Exceptionality Lemma §1.2. Thus, he produces the complete list over $\mathbb{F}_2$.

$p = 2$ and general odd a. Motivated by Müller's method and his talk, Cohen and Matthews [**CM**] have constructed examples for $p = 2$ and each odd a. Building on Müller's use of **GAP** , they caught a pattern in his computations. In particular, they produce a *primal* polynomial. First: Let $T_a(x) = x + x^2 + x^{2^2} + \cdots + x^{2^{a-1}}$. That is, $T_a(x)$ is the *trace* function from $\mathbb{F}_{2^a}$. The polynomial

$$f_a(x) = T_a(x^{2^a+1})/x^{2^a} \tag{1.10}$$

is exceptional. To show this they factor $\phi_a(x) = \frac{f_a(x)-f_a(y)}{x-y}$ and conclude from the Exceptionality Lemma shows it is a permutation polynomial on $\mathbb{F}_{2^e}$ exactly when $(e, a) = 1$ [**CM**, Theorem 1.1]. They do not directly compute its geometry monodromy group. Rather, they use [**FGS**, Theorems 13.4 and 14.1] to conclude the only possibility: the geometric monodromy group is $G = \mathrm{PSL}_2(2^a)$ and the arithmetic monodromy group is $\hat{G} = \mathrm{P\Gamma L}_2(2^a)$. Thus, this part of their conclusions depends on part of the classification of finite simple groups.

Finally, [**CM**, §5] considers $d|2^a + 1$ and the observation

$$f_a^d(x) = f_{a,d}(x^d) \tag{1.11}$$

for some polynomial $f_{a,d}(x)$. Example: $d = 3, c = 3$, and f_1 and f_2 as in (1.9):

$$f_1^3(x) = x^3(1 + x^9 + x^{27})^3 = f_2(x^3).$$

Clearly, if $(d, 2^e - 1) = 1$, $f_{a,d}(x)$ is also a permutation polynomial on $\mathbb{F}_{2^e}$. Thus, $f_{a,d}(x)$ is also exceptional. From this we also see the relation between the ramification groups and the monodromy groups of the two polynomials. They

have the same monodromy groups. The ramification groups, however, are a little different. Whereas, $f_a(x)$ gives a cover ramified only over ∞, the cover for $f_{a,d}(x)$ has additional tame ramification over 0 and ∞. That is, the group G_∞ is slightly different for the two covers.

All exceptional polynomials with given monodromy G. Müller and Cohen-Matthews examples are polynomials over $\mathbb{F}_2$. It is naive to assume the collection $f_{a,d}(x)$, $d|2^a+1$, gives the complete list of degree $2^{a-1}(2^a-1)$ exceptional polynomials in characteristic 2. Extensions of $\mathbb{F}_2$ will have more with the same geometric/arithmetic mondromy group pair.

Exceptional Degree $2^{a-1}(2^a-1)$ Polynomial Problem. *With a odd, give explicit algebraic varieties V_a parametrizing exceptional degree $2^{a-1}(2^a-1)$ polynomials.*

Here are properties V_a must satisfy. There is a finite Galois cover $C_a \to V_a$ with group $H = G(C_a/V_a)$ and a collection $\mathbf{C}$ of conjugacy classes in H. All should be defined over $\mathbb{F}_2$. Over V_a there is an algebraic family of polynomials $\mathcal{P}_a \to V_a$, defined over $\mathbb{F}_2$. For each integer e, and each $\boldsymbol{v}_0 \in V_a(\mathbb{F}_{2^e})$ denote the Frobenius class of $\boldsymbol{v}_0$ in the cover $C_a \to V_a$ by $F_{\boldsymbol{v}_0}$. Then,

(1.12) the polynomial in the fiber of $\mathcal{P}_a$ over $\boldsymbol{v}_0$ is an exceptional polynomial over $\mathbb{F}_{2^e}$ if and only if $F_{\boldsymbol{v}_0}$ is in $\mathbf{C}$.

Also, each degree $2^{a-1}(2^a-1)$ exceptional polynomial over $\mathbb{F}_{2^e}$ corresponds to such a point $\boldsymbol{v}_0 \in V_a(\mathbb{F}_{2^e})$.

§2. GENERAL EXCEPTIONAL COVERS

In §2.1 we remind of the precise group theoretic conditions that hold for a geometric/arithmetic monodromy group pair $(G, \hat{G})$ of an exceptional polynomial. From these we give the definition and main properties of *general* exceptional covers. Our first result shows why these are *median value* curves (§0.2). Our Main Theorem 2.5 shows how every pair $(\hat{G}, G)$ satisfying the necessary conditions for a geometric/arithmetic monodromy pair actually produces exceptional covers with such pairs. Here, however, we are in new territory; we can only say this happens for all but finitely many primes p.

§2.1. The groups conditions. Fix a prime p. The geometric and arithmetic monodromy groups of an exceptional polynomial satisfy the following four conditions (§1.1–§1.2).

(i) $\hat{G}$ is a primitive group on $\{1, 2, \dots, n\}$.
(ii) G is normal in $\hat{G}$ with the quotient $\hat{G}/G$ cyclic.
(iii) G has a transitive subgroup G_∞ whose p-Sylow H_∞ is normal in G_∞ and G_∞/H_∞ cyclic.
(iv) $\hat{G}(1)$ stabilizes no orbit of $G(1)$ on $\{2, 3, \dots, n\}$.
(v) A condition to guarantee the possibility of realization of G as the geometric monodromy groups of a genus 0 field extension of $K(z)$.

Consider pairs $(G, \hat{G})$ satisfying (i), (ii) and (iv). In §1.1 on forming arithmetic monodromy groups, replace $K(x)/K(z)$ by a general field extension $L/K(z)$, $K = \mathbb{F}_q$, and L has no constants outside K. That is, $L/K(z)$ is a *regular* extension over K. Then, $\hat{G}$ is the group of the Galois closure of $L/K(z)$, and G is the same for $\bar{K}L/\bar{K}(z)$.

Conclude: L is the function field of a cover $\psi : X \to \mathbb{P}^1_z$, with equations having coefficients in $K = \mathbb{F}_q$. For example, compatible with §1.1, consider when this situation comes from a polynomial cover given by f. Then, $X = \{(x, z) \mid f(x) - z = 0\}$ and $(x, z) \mapsto z$ gives ψ.

§**2.2. Characterizations of exceptional covers.** The main result of this section is already in [**FGS**, §10]. The first statement of it was in [**Fr3**]. The latter reference didn't give a proof, because it considered the result analogous to what had already been done in [**Fr3**]. [**FGS**, §10], together with the main observation of [**Fr3**], comprise a complete proof. Still, it's not together in one place. So, we offer a complete proof here. In the next section we add historical comments. Now we give a general geometric formulation of an exceptional cover.

Definition: *General Exceptional Covers.* Let $\phi : X \to Y$ be a cover of nonsingular projective curves, defined and absolutely irreducible over $\mathbb{F}_q = K$. In particular, $K(X)/K(Y)$ is a regular extension as in §2.1. Let $X_{1,2}$ be the fiber product $X \times_Y X$ of this map as in §1.1. Then (ϕ, X) is an *exceptional cover* when the following holds. The fiber product with the diagonal removed leaves a curve $X_{1,2} \setminus \Delta$ with no absolutely irreducible components over $\mathbb{F}_q$.

Retain the notation for geometric/arithmetic monodromy groups $G \subset \hat{G} \subset S_n$ as above, $n = \deg(\phi)$. As previously, $\hat{K}$ is the constants of the Galois closure of $K(X)/K(Y)$. The crucial set for arithmetic computation is

$$G^* = \{\tau \in \hat{G} \mid \tau \text{ is the Frobenius generator of } G(\hat{K}/K).\}$$

General Exceptionality Theorem 2.1. *An $\mathbb{F}_q$ cover $\phi : X \to Y$ is exceptional if and only if $\hat{G}(1)$ fixes no orbit of $G(1)$ on $\{2, \dots, n\}$. Equivalently:*

(2.1) *each element of G^* fixes exactly one integer in the representation.*

Denote $[\hat{G} : G]$ by s. Take t with $(t, s) = 1$. Exceptionality is equivalent to each $\mathbb{F}_{q^t}$ non-branch point of Y has exactly one $\mathbb{F}_{q^t}$ point of X above it. In particular, if $\phi : X \to Z$ factors through $Y \to Z$, then $\phi : X \to Z$ is exceptional if and only if both $X \to Y$ and $Y \to Z$ are exceptional. When X is of genus zero, some rational function gives ϕ. Then, for t with $(t, s) = 1$, each $\mathbb{F}_{q^t}$ point of $\mathbb{P}^1_z$ has exactly one $\mathbb{F}_{q^t}$ point of X above it. Indeed, this holds more generally even if X is not of genus 0, if Y is of genus 0.

Proof. The proof of the first sentence follows exactly the proof of the special case in the Exceptionality Lemma 1.1. Statement (2.1) is purely group theoretic. Suppose α is one element in G^*. The coset αG is all of G^*. [**FGS**, Lemma 13.1] has a careful list of equivalent conditions to (2.1). Here, however, we use the

simple counting proof of [**Fr3**, Theorem 1]. Use the notation of §1.1 to see that $\tau \in G^*$ can fix at most one element. Suppose, τ fixes x_1. Then, it fixes none of the integers $2, \dots, n$ because it must act nontrivially on the components over $\bar{\mathbb{F}}_q$ of $Y \setminus \Delta$. Denote the elements of G^* that stabilize 1 by $G^*(1)$. Thus, the union H of the conjugates of $G^*(1)$ is a set of cardinality $n \cdot |G^*(1)|$. Since this is the cardinality of $\alpha G = G^*$, this also equals H. We have shown (2.1).

The sentence after (2.1) interprets the action of the Frobenius using the non-regular analog of the Čebotarev Density Theorem [**FrJ**, Prop. 5.16]. (Actually, one must follow the proof here to see the role of the branch points. The original proof in [**Fr7**] or in [**Fr5**] is better for this.) Now consider the statement when $\phi : X \to Z$ factors through $Y \to Z$.

Suppose both $Y \to Z$ and $X \to Y$ are exceptional. We show $X \to Z$ is exceptional by showing each non-branch point $z \in Z$ over $\mathbb{F}_{q^t}$ (with $(t, s) = 1$) has above it just one $\mathbb{F}_{q^t}$ point. Suppose not. Let x_1, x_2 be $\mathbb{F}_{q^t}$ points above z. If their images y_1, y_2 in Y are equal, this violates exceptionality for $X \to Y$. Thus, assume $y_1 \neq y_2$. Then, these distinct $\mathbb{F}_{q^t}$ points both lie over z. This violates exceptionality for $Y \to Z$.

Now assume $X \to Z$ is exceptional. Here are the implications with the last paragraph notations. Above each non-branch $\mathbb{F}_{q^t}$ point of Z, there is a $\mathbb{F}_{q^t}$ point of Y: the image in Y of the $\mathbb{F}_{q^t}$ point of X above z. Thus, the Riemann Hypothesis Lemma 2.2 says $Y \to Z$ is exceptional. Above each $\mathbb{F}_{q^t}$ point of Y there is at most one $\mathbb{F}_{q^t}$ point of X, or we would violate exceptionality of $X \to Z$. Again, the Riemann Hypothesis Lemma says $X \to Y$ is exceptional.

Finally, consider the case Y is of genus 0, but X may not be. The concluding statements of the theorem are that X has exactly one $\mathbb{F}_{q^t}$ point above *each* $\mathbb{F}_{q^t}$ point of Y. When X is of genus 0 this is already in [**Fr4**]: this works exactly as for polynomials. The Riemann Hypothesis Lemma shows this under the weaker assumption Y is of genus 0. □

Riemann Hypothesis Lemma 2.2. *Consider a cover $X \to Y$ of absolutely irreducible nonsingular projective curves. Suppose one of the following holds for infinitely many t. Either:*

(2.2a) *over each non-branch point of $Y(\mathbb{F}_{q^t})$ is at most one point of $X(\mathbb{F}_{q^t})$; or*

(2.2b) *over each non-branch point of $Y(\mathbb{F}_{q^t})$ there is at least one point of $X(\mathbb{F}_{q^t})$.*

Then, $X \to Y$ is an exceptional cover. In addition, suppose $X \to Y$ is exceptional, Y is of genus 0 and $s = [\hat{G} : G]$. Then , for $(t, s) = 1$,

(2.2c) *over each (including branch) point of $Y(\mathbb{F}_{q^t})$ there is exactly one point of $X(\mathbb{F}_{q^t})$.*

Proof. From the Riemann Hypothesis, both X and Y have $q^t + O(q^{t/2})$ points over $\mathbb{F}_{q^t}$: two times the genus of the curve bounds the O. The Riemann-Hurwitz formula (§1.3) bounds the number of branch points of $X \to Y$. We can choose the bound linear in the genus of X. The proof has four parts; the last two correspond to the case when Y has genus 0.

Part 1: If (2.2b) holds, yet $X \to Y$ isn't exceptional. Let $\hat{G}$ be the arithmetic monodromy group of the cover. Then, for some $\tau \in \hat{G}(1)$:

(2.3a) τ fixes at least one other integer from $\{2, \dots, n\}$; and

(2.3b) restriction of τ to $\hat{\mathbb{F}}_q$ is the Frobenius.

The nonregular Čebotarev Density Theorem [**FrJ**, Prop. 5.16] says: $cq^t + O(q^{t/2})$ points $\boldsymbol{y} \in Y(\mathbb{F}_{q^t})$ realize (the conjugacy class of) τ as the Artin symbol of a point $\boldsymbol{x} \in X$ over $\boldsymbol{y}$. Here c, independent of t, is the number of elements in the conjugacy class of τ divided by the number of elements in $\hat{G}$ satisfying (2.3b). Thus, c and the O constant are independent of t. From (2.3a), above each such point there are at least two $\mathbb{F}_{q^t}$ points of X. So, (2.2b) gives a count of at least $(1+c)q^t + O(q^{t/2})$ for the $\mathbb{F}_{q^t}$ points of X. This contradicts the Riemann Hypothesis.

Part 2: If (2.2a) holds, yet $X \to Y$ isn't exceptional. This is similar to Part 1. Here, however, we would have $\tau \in \hat{G}$ fixing no integer from $\{1, \dots, n\}$ having the Frobenius as its restriction to $\hat{\mathbb{F}}_q$. Above each such $\boldsymbol{y} \in Y$ with τ as Artin symbol there are no points of $X(\mathbb{F}_{q^t})$. Thus, we have an upper bound of $(1-c)q^t + O(q^{t/2})$ for $X(\mathbb{F}_{q^t})$. This contradicts the Riemann Hypothesis.

Part 3: If Y is genus 0 and $X \to Y$ is exceptional, then X is a median value curve. There are $q^t + 1$ points over $\mathbb{F}_{q^t}$ on Y. We show X also has exactly q^t+1 points over $\mathbb{F}_{q^t}$. To see this, use the more precise estimate from the Riemann hypothesis. Let g be the genus of X. Then, X has $q^t+1-\sum_{i=1}^{2g} \alpha_i^t$ points over $\mathbb{F}_{q^t}$. Here the α_i s are algebraic integers of absolute value $q^{1/2}$.

Let N_t be the number of $\mathbb{F}_{q^t}$ points on X. From above, for $(t,s) = 1$, the number of points on X over branch points of $Y = \mathbb{P}^1$ bounds $N_t - q^t - 1$. This bound is independent of t. We want to show $S_t \stackrel{\text{def}}{=} \sum_{i=1}^{2g} \alpha_i^t = 0$. First: There is a subsequence T of t s for which S_t is a fixed constant. Let t_1 be the minimal value in T. Then

$$S_{t_1} - S_t = 0 = \sum_{i=1}^{2g} \alpha_i^{t_1}(1 - \alpha_i^{t-t_1}). \tag{2.4}$$

Put the expression with α_1 on the left side and divide both sides by $1 - \alpha_1^{t-t_1}$. For large t, the ratios $(1 - \alpha_i^{t-t_1})/(1 - \alpha_1^{t-t_1})$ approach $(\alpha_i/\alpha_1)^{t-t_1}$. Conclude, for $t \in T$, that $S_t = 0$.

The last argument shows there are only finitely many t with $(s,t) = 1$ for which S_t is nonzero. For a given positive t_0 relatively prime to s, consider the arithmetic progression $T_{t_0} = \{t_0, t_0 + s, t_0 + 2s, \dots\}$. We are done if we show $S_t = 0$ for all $t \in T_{t_0}$. Rewrite S_{t_0+ks} as $q^{ks}S'_k$ with $S'_k = \sum_{i=0}^{2g} A_i e^{2\pi i k\theta_i}$. Here $A_i = \alpha_i^{t_0}$ and θ_i is real, $i = 1, \dots, 2g$. We know $S'_k = 0$ for k large and S_t is an integer for all t.

Suppose for an arbitrarily large value of k the vector $(e^{2\pi i k\theta_1}, \dots, e^{2\pi i k\theta_{2g}})$ is suitably close to a vector of 1 s. Then, $0 = S_{t_0+sk}/q^{ks} = S'_k$ is close to S_{t_0}. For this, we use a *box principle* argument.

The function $k \mapsto (e^{2\pi i k\theta_1}, \dots, e^{2\pi i k\theta_{2g}})$ is from the positive integers into a (compact) torus. Thus, there are two integers k_1, k_2, arbitrarily far apart, whose images are as close as desired. Take $k = k_2 - k_1$ to complete the proof.

Part 4: If $X \to Y$ is as in Part 3, then (2.2c) holds. Here we apply the argument of [**Fr3**, Theorem 1]. Let $\boldsymbol{y}_0 \in Y(\mathbb{F}_{q^t})$ and let $\boldsymbol{p}_0$ be a place on the Galois closure of $X \to Y$ above $\boldsymbol{y}_0$. Denote the decomposition group of $\boldsymbol{p}_0$ by $D(\boldsymbol{p}_0)$. Choose $\tau(\boldsymbol{p}_0) \in D(\boldsymbol{p}_0)$ to map to the Frobenius element by the residue class map: restriction of $\tau(\boldsymbol{p}_0)$ to $\mathbb{F}_{q^t}(\boldsymbol{p}_0)$ generates $G(\mathbb{F}_{q^t}(\boldsymbol{p}_0)/\mathbb{F}_{q^t})$. From (2.1), $\tau(\boldsymbol{p}_0)$ fixes a unique integer. This corresponds to a point $\boldsymbol{x}_0 \in X$ above $\boldsymbol{y}_0$ that $\tau(\boldsymbol{p}_0)$ fixes. Since $\tau(\boldsymbol{p}_0)$ restricts to the Frobenius—q^t-th power map—on the residue class field, the coordinates of $\boldsymbol{x}_0$ are in $\mathbb{F}_{q^t}$. Thus, $\boldsymbol{x}_0 \in X(\mathbb{F}_{q^t})$.

In particular, above each $\boldsymbol{y}_0 \in Y(\mathbb{F}_{q^t})$ is at least one point $\boldsymbol{x}_0 \in X(\mathbb{F}_{q^t})$. From Part 3, $|Y(\mathbb{F}_{q^t})| = |X(\mathbb{F}_{q^t})|$. Thus, there must be *exactly* one point of $X(\mathbb{F}_{q^t})$ above each $\boldsymbol{y}_0 \in Y(\mathbb{F}_{q^t})$. □

§**2.3. Brief history of the general exceptionality theorem.** We could exploit the argument above for higher dimensional maps. For example, [**Fr3**, Theorem 1] considers *finite* maps $F : \mathbb{A}^k \to \mathbb{A}^k$. Finite here is a technical term from algebraic geometry. For this case it is equivalent to surjective with finite fibers [**Mum**, p. 243]. Use the fiber product definition of exceptional to consider when such a k-variable polynomial map F is *exceptional*. The conclusion is that F is one-one on $\mathbb{A}^k(\mathbb{F}_{q^t})$ for $(t, s) = 1$ as in the General Exceptionality Theorem (or Exceptionality Lemma 1.1). This is uses Čebotarev analogs, which hold as well for higher dimensional covers.

Still, there is no reason to stop. The above would certainly work for finite maps $F : \mathbb{P}^k \to \mathbb{P}^k$. Indeed, given the Riemann hypothesis for projective varieties over finite fields, the Riemann Hypothesis Lemma should work there for finite maps $F : X \to \mathbb{P}^k$ with X non-singular.

C. MacCluer, as in the title of [**Fr3**] proved The Exceptionality Lemma for a tamely ramified polynomial map. I wrote the papers [**Fr3**] and [**Fr6**] in 1968, but had troubles with the referee. Thus, their late appearance. S. Cohen considered the case of a possibly wildly ramified (one variable) polynomial map in [**C3**]. I quote that paper for the fluid use of the Frobenius as in Part 4. [**CM**] reminds of Cohen's priority, but doesn't mention MacCluer.

§**2.4. Totally ramified general exceptional covers.** Consider a general exceptional cover $\psi : X \to \mathbb{P}^1$ over $\mathbb{F}_{q^t} = K$. As in the General Exceptionality Theorem, for $(s, t) = 1$ with $[\hat{K} : K] = s$, over each $\mathbb{F}_{q^t}$ point of $\mathbb{P}^1$, there is exactly one $\mathbb{F}_{q^t}$ point of the cover X.

Consider covers for which ψ has a totally ramified place: over a $z_0 \in \mathbb{F}_q \cup \{\infty\}$. This means there is one and only one point (over $\bar{\mathbb{F}}_q$) on X over z_0.

Definition 2.3: *Arithmetically primitive covers.* We say ψ is arithmetically primitive if ψ does not factor through maps of degree exceeding 1, $\psi' : X \to Y$ and $\psi'' : Y \to \mathbb{P}^1$, defined over $\mathbb{F}_q$ with $\psi'' \circ \psi' = \psi$.

Assume ψ is arithmetically *primitive*. Let p' be a prime, possibly different from p. Take H to be a subgroup of $\mathbb{F}_{p'}^*$. Denote the semidirect product $\mathbb{F}_{p'} \times^s H$ by $A(p', H)$. It is convenient to represent this group as 2×2 matrices $\left(\begin{smallmatrix} h & b \\ 0 & 1 \end{smallmatrix}\right)$ with $h \in H$, $b \in \mathbb{F}_{p'}$. As in §1.3, apply Burnside's Theorem to conclude any exceptional prime degree cover must have arithmetic and geometric monodromy groups of the form $A(p', H)$ for some H.

If the degree of the cover is n, with $(n, p) = 1$ and n not prime, then the totally ramified place produces an n-cycle in the group G. From [**FGS**, Lemma 4.1′], $\hat{G}$ primitive and G containing an n-cycle imply G is primitive. As in §1.3, apply Schur's Theorem to conclude G is doubly transitive. This contradicts exceptionality in the General Exceptionality Theorem. Conclude the following.

THEOREM 2.4 [**FGS**, Theorem 14.1]. *Assume $\psi : X \to \mathbb{P}^1$ is an arithmetically primitive exceptional cover, totally ramified over some $\mathbb{F}_q$ place. Then, either $p = 2$ or 3, or the cover is of prime degree p'—with $p' \neq 2$, or $\hat{G}$ and G are affine groups of degree p^a (see §1.6). Also, when $p = 2$ or 3, the exceptions to the affine group cases are when G normalizes $\mathrm{PSL}_2(\mathbb{F}_q)$ as in §1.6. Thus, the conclusion of Carlitz's conjecture holds here: general exceptional covers over finite fields (with q odd) are of odd degree if there is a totally ramified $\mathbb{F}_q$ place in the cover.*

2.5. Production of general exceptional covers. We continue the notation for a general exceptional cover $\psi : X \to \mathbb{P}^1$ over $\mathbb{F}_{q^t} = K$ from §2.4. Theorem 2.5 proves there are many general exceptional covers. We do a full proof in one general subcase, when G is a product of simple groups. The complete proof depends on ideas from [**FrV3**] which we only outline. In the next subsection we do an explicit case in detail: exceptional covers with $A(\{\pm 1\}, p')$ (§2.4) as geometric monodromy group. Looks easy, but it's not!

Properties (i), (ii) and (iv) of the geometric/arithmetic monodromy group pair $(G, \hat{G})$ of any exceptional cover appear in §2.1. They aren't, however, relevant. Theorem 2.5 applies to achieving *any* geometric/arithmetic pair. The goal is to *achieve* $(G, \hat{G})$ as the geometric/arithmetic monodromy group pair over $\mathbb{F}_p$ for almost all primes p. Hypotheses (2.6a)–(2.6c) are part of the conditions for producing a primitive, exceptional cover. This includes $\hat{G} =< G, g >$: some $g \in \hat{G}$ generates $\hat{G}$ over G. Note: If we do achieve $(G, \hat{G})$, it is automatic no element of $\hat{G} \setminus G$ centralizes G. Otherwise, the Galois closure process would give an arithmetic monodromy group smaller than $\hat{G}$. Thus, we must include this in the natural hypotheses on $(G, \hat{G})$.

EXISTENCE THEOREM 2.5. *Consider a pair of groups $(G, \hat{G})$ with an element $g \in \hat{G} \setminus G$ such that $\hat{G} =< G, g >$. Assume also the following properties.*

(2.5a) *$G \leq \hat{G} \leq S_n$ are transitive subgroups of S_n.*

(2.5b) *$< G, g >= \hat{G}$ is primitive ((i) holds).*

(2.5c) *Conditions (ii) and (iv) of §2.1 hold for the pair $(G, \hat{G})$.*

(2.5d) *No element of $\hat{G} \setminus G$ centralizes G.*

Then, for all suitably large primes p, $(G,\hat{G})$ is the geometric/arithmetic monodromy group pair of an exceptional cover $\psi: X \to \mathbb{P}^1$ over $\mathbb{F}_p$ where restriction of g to the constants of the Galois closure field $\widehat{\mathbb{F}_p(X)}$ is the frobenius. Further, we may produce a ψ without any bound on the number of its branch points (or on the genus of X).

PROOF. We use the Main Theorem of [**FrV1**, Prop. 3] to give a complete proof of the theorem when a pair $(G',\hat{G}')$ exists satisfying the conditions (2.6). The proof has four parts. The first is a general Galois theoretic setup to which we apply an amalgam of the classical Čebotarev density theorem and its nonregular finite field analog. The second shows the hypothesis of (2.6) holds when G is a product of simple groups, and the third handles the case when (2.6) holds. Finally, the fourth part discusses the replacement for (2.6) that allows us to give the general proof.

(2.6a) G' is normal in $\hat{G}' =< G', g' >$.

(2.6b) There exists a surjective homomorphism $\psi: \hat{G}' \to \hat{G}$ mapping g' to g that induces a surjective map $G' \to G$ and an isomorphism $\hat{G}'/G' \cong \hat{G}/G$.

(2.6c) G' has trivial center, $\hat{G}'$ has no centralizer in G' and its *Schur multiplier* is generated by commutators.

The Schur multiplier condition (2.6c) holds in particular if G' has trivial Schur multiplier. That is what we use in Part 2 of the proof. So we don't explain it further, except to say it allows us to quote [**FrV1**, Prop. 3].

Part 1: Applying Bertini-Noether and Čebotarev. Suppose we have a pair $(G',\hat{G}')$ satisfying (2.6a) and (2.6b). Assume also, these occur in a geometric/arithmetic situation of the following type. There are indeterminates $\boldsymbol{x} = \{x_1, \dots, x_t\}$, algebraically independent of any other fields that arise here. In addition, there are fields $K', \hat{K}'$, and L' with these properties.

(2.7a) K' and $\hat{K}'$ are finitely generated and disjoint from $\bar{\mathbb{Q}}$ over $\mathbb{Q}$ and $\hat{K}'$ is the algebraic closure of K' in L'.

(2.7b) $\hat{G}' = G(L'/K'(\boldsymbol{x}))$ and $G' = (L'/\hat{K}'(\boldsymbol{x}))$.

Take L the fixed field in L' of the kernel of the map $\hat{G}' \to \hat{G}$. Let $K = K'$; let $\hat{K}$ be the algebraic closure of K in L. Then, $G = G(L/\hat{K}(\boldsymbol{x}))$ and $\hat{G} = G(L/K(\boldsymbol{x}))$. To get a cover of the z-line replace $\boldsymbol{x}$ with a general linear combination of the coordinates of $\boldsymbol{x}$ with coefficients in $\mathbb{Q}$. Take N as the fixed field in L of $\hat{G}(1)$. Then, N is the function field of a projective nonsingular curve X_K. Also, X_K comes with a natural map $X_K \to \mathbb{P}^1_z$ over K inducing the injection $K(z) \subset N$. This is the *Bertini-Noether argument* [**FrJ**, Prop. 9.31].

With the hypotheses above, K is the function field of an absolutely irreducible variety V over $\mathbb{Q}$. In addition, $\hat{K}$ is the function field of another absolutely irreducible variety $\hat{V}$. This has a covering map $\psi: \hat{V} \to V$ that induces the field inclusion $K \subset \hat{K}$.

Now consider reduction of V and V' modulo a prime p. Apply the Bertini-Noether argument again to an affine open variety of V and its pullback to V'

to make the following assumption. For all but finitely many primes p, reduction modulo p gives an étale cover $\psi_p : \hat{V}_p \to V_p$ of absolutely irreducible varieties with the same group, indentified with $\hat{G}/G = G(\hat{K}/K)$ as the cover ψ. Further, for each $\boldsymbol{v} \in V_p(\mathbb{F}_p)$, there is a specialization of $X_K \to \mathbb{P}^1_z$ to $X_{\boldsymbol{v}} \to \mathbb{P}^1_z$ defined over $\mathbb{F}_p$. Let $D_{\boldsymbol{v}} =< F_{\boldsymbol{v}} >$ be the decomposition group of the point $\boldsymbol{v}$ in this cover. Our notation shows that a specific element $F_{\boldsymbol{v}}$ plays the role of the Frobenius generator of this cover. We naturally identify this with an element of $G(\hat{K}/K)$. Then, the geometric/arithmetic monodromy group pair of $X_{\boldsymbol{v}} \to \mathbb{P}^1_z$ is $(G, < G, g_{\boldsymbol{v}} >)$ where $g_{\boldsymbol{v}}$ maps to $F_{\boldsymbol{v}} \in G(\hat{K}/K)$.

Now we show the conclusion of Theorem 2.5. To produce the desired exceptional cover with given geometric/arithmetic pair, choose $\boldsymbol{v} \in V_p$ so $F_{\boldsymbol{v}}$ is the image of g in the statement of the theorem. Apply the General Exceptionality Theorem to conditions (2.5): this is the desired cover. The non-regular Čebotarev density theorem gives the existence of $\boldsymbol{v}$. This many-variable-version is well known, and the arguments here go back to [**Fr7**] (see Remark 2.6).

Part 2: G is a product of simple groups. Form $(G', \hat{G}')$ with property (2.6b) and $(G', \hat{G}')$ is a split extension: $\hat{G}' \cong G' \times^s M$ for some M acting faithfully on G'. For example, take $G' = G$ and M a cyclic subgroup of $\hat{G}$ that maps onto $\hat{G}/G$. The map $A = G \times^s M \to \hat{G}$ by $(g, m) \mapsto gm$ gives the desired conclusion. This reduces us to $(G, \hat{G})$ with $\hat{G} = G \times^s M$ for some cyclic group M.

The essential case when G is a direct product of simple groups is when $G = S^m$, S simple. We show existence of $K', \hat{K}'$ and L' satisfying (2.7) for groups $(G', \bar{G}')$ covering $(G, \hat{G})$.

The case where S is an abelian simple group is well known. Since M is cyclic, of order m, it is easy to construct K'_M and $\hat{K}'_M$ with $G(\hat{K}'_M/K'_M)$ isomorphic to M and $\mathbb{Q}$ algebraically closed in $\hat{K}'_M$. Now, for example, apply [**FrJ**, Lemma 24.46]. This produces L'/E with these properties.

(2.8a) E is pure transcendental over K'_M and L' is regular over $\hat{K}'_M$.
(2.8b) $G(L'/E) \cong G \times^s M$ through restricting elements of $G(L'/E)$ to $\hat{K}'_M$.

Now consider the case S is non-abelian and simple.

We follow [**FrV2**, Lemma 3] which contains the appropriate references. A product of simple groups is perfect, so it has a *universal central extension*, $\tilde{G}$. This universality implies the action of M on G automatically extends to an action on $\tilde{G}$. The key is that $\tilde{G}$ has trivial Schur multiplier. The rest of the argument is to form a cover G' of $\tilde{G}$. We need this: The action of M extends to assure the centralizer of $G' \times^s M$ in G' is trivial. We must do this while assuring G' has trivial Schur multiplier. This construction uses $G' = T^N \times^s \tilde{G}$ where T is *any* simple group with trivial Schur multiplier. Here N is the order of $\hat{G} = \tilde{G} \times^s M$ with $T^N \times^s \hat{G}$ the wreath product of T and $\hat{G}$. This verifies (2.6) holds.

Part 3: Apply [FrV1, Prop. 3]. [**FrV1**, Prop. 3] produces an unramified cover of absolutely irreducible varieties $\Psi : \mathcal{H}' \to \mathcal{H}$ varieties over $\mathbb{Q}$ with the following properties.

(2.9a) $\Psi : \mathcal{H}' \to \mathcal{H}$ is a Galois cover, with automorphisms defined over $\mathbb{Q}$ and group the full outer automorphism group of G' at the end of Part 2.

(2.9b) Any point $\boldsymbol{p} \in \mathcal{H}$ and $\hat{\boldsymbol{p}} \in \mathcal{H}'$ over $\boldsymbol{p}$, produces a Galois field extension $L'_{\boldsymbol{p}}/\mathbb{Q}(\boldsymbol{p})(z)$ with the algebraic closure of $\mathbb{Q}(\boldsymbol{p})$ in $L'_{\boldsymbol{p}}$ equal to $\mathbb{Q}(\hat{\boldsymbol{p}})$.

(2.9c) To the data of (2.9b) we attach an exact sequence of groups

$$1 \to G' = G(L'_{\boldsymbol{p}}/\mathbb{Q}(\hat{\boldsymbol{p}})(z)) \to G(L'_{\boldsymbol{p}}/\mathbb{Q}(\boldsymbol{p})(z)) \to G(\mathbb{Q}(\hat{\boldsymbol{p}})/\mathbb{Q}(\boldsymbol{p})) \to 1.$$

(2.9d) The middle term in sequence (2.9c) is $G' \times^s M$ precisely when the decomposition group $D_{\boldsymbol{p}}$ for $\boldsymbol{p}$ in the cover Ψ is M.

Let $\boldsymbol{p}'$ be a generic point of the variety $\mathcal{H}'$ and $\boldsymbol{p}$ the point on $\mathcal{H}$ below $\boldsymbol{p}'$. Our hypotheses give M as a subgroup of the outer automorphism group of G', identified with $G(\mathbb{Q}(\boldsymbol{p}')/\mathbb{Q}(\boldsymbol{p}))$. With no loss, replace $\mathcal{H}$ with the integral closure of $\mathcal{H}$ in the fixed field of M in $\mathbb{Q}(\boldsymbol{p}')$. We still call this $\mathcal{H}$. Now we have the setup of (2.7) by taking $K' = \mathbb{Q}(\boldsymbol{p})$, $\hat{K}' = \mathbb{Q}(\boldsymbol{p}')$, and $L' = \mathbb{Q}(\boldsymbol{p})L'_{\boldsymbol{p}}$.

Part 4: How [FrV3] intends to weaken the hypotheses that give conditions (2.9). Theorem 3.3 explains the condition that gives (2.9). It is transitivity of Hurwitz monodromy action on Nielsen classes. The Schur multiplier condition is there precisely to assure this transitivity. We don't actually need transitivity. Rather, each orbit of the Hurwitz monodromy action corresponds to a variety like $\mathcal{H}$. Transitivity guarantees this variety is defined over $\mathbb{Q}$. [**FrV3**] has, however, found a weaker condition that geometrically forces the variety corresponding to particular orbits to be defined over $\mathbb{Q}$. We conclude the proof with a brief explanation of this.

In Def. 3.1 of Nielsen class assume $r = 2r'$. Consider the collection of $\boldsymbol{s}$ in the Nielsen class of form $(s_1, s_1^{-1}, \ldots, s_{r'}, s_{r'}^{-1})$. Call this set $\mathcal{P}_{\mathbf{C}}$. We assume $\mathbf{C}$ is a rational union of conjugacy classes as in Def. 3.2. Here is the key condition:

(2.10) $\mathcal{P}$ is contained in one orbit of H_r acting on the Nielsen class of $\mathbf{C}$.

If (2.10) holds, the variety of the orbit containing $\mathcal{P}$ is defined over $\mathbb{Q}$. Also, (2.10) holds if $\mathbf{C}$ contains all conjugacy classes at least four times. □

REMARK 2.6. *Dependence of excluded primes on the construction of Theorem 2.5.* We don't attempt here to bound excluded primes except that such will be a corollary in a paper by H. Völklein and myself. The statement in Theorem 2.5 that we can produce a cover with an arbitrary number of branch points does affect the excluded primes. Present theory forces a bound on these to grow with the number of branch points. Finally, the use of the Čebotarev density theorem at the end of Part 1 requires explicit computation to bound excluded primes. [**FHJ**] is the best source we know here. □

§3. PRACTICAL PRODUCTION OF EXCEPTIONAL COVERS

Theorem 2.5 says, given any feasible geometric/arithmetic monodromy group pair $(G, \hat{G})$, we can achieve this from a general exceptional cover over $\mathbb{F}_p$ for

almost all primes p. This encourages us to the end of creating more practical achievement of $(G, \hat{G})$. §3.1–§3.2 considers the easiest special case and its relation to modular curves. §3.4 uses fiber products to create many general exceptional covers from any one. The problems here center around which medium value curves arise from exceptional covers. Free use of fiber products raises the question of detecting when a cover is primitive. §3.3 states a geometric criterion for this generalizing one that appears in [**AGR**]. We conclude the paper in §3.4–§3.5 with ideas from coding, especially relating median value curves to achievement of high Weil bounds.

§**3.1. Branch cycles descriptions.** Theorem 2.5 uses abstract principles. We use an example to give more explicit realization of large collections of general exceptional covers. For this, the geometric/arithmetic pair is

(3.1) $(D'_p, A(p', H))$ with H a subgroup of $\mathbb{F}_{p'}$ properly containing $\{\pm 1\}$.

Here p' is an odd prime. In the proof of Theorem 2.5, Part 3, we find the magic phrase that gets the proof to work: [**FrV1**, Prop. 3] produces an unramified cover of absolutely irreducible varieties $\Psi : \mathcal{H}' \to \mathcal{H}$ varieties over $\mathbb{Q}$ (with the properties of (2.9)). We use this case to explain exactly how we can often verify conditions (2.9) directly.

For the remainder of this subsection consider covers over $\mathbb{C}$. As usual, whenever necessary,assume all characteristic 0 fields have a representative embedding in $\mathbb{C}$. Riemann's existence theorem considers how to combinatorially describe a cover $\phi : X \to \mathbb{P}^1_z$ ramified over the collection of points $\{z_1, \dots, z_r\} = \boldsymbol{z}$. The criterion comes from topology. Let z_0 be any point in $\mathbb{P}^1 \setminus \boldsymbol{z}$. The fundamental group $\pi_1 = \pi_1(\mathbb{P}^1 \setminus \boldsymbol{z})$ is free on r-generators $\bar{s}_i$, $i = 1, \dots, r$, with the one relation $\bar{s}_1 \cdots \bar{s}_r = 1$. Thus, produce a *branch cycle description* $(s_1, \dots, s_r)$ of a cover by corresponding to the cover the unramified pullback of X over $\mathbb{P}^1 \setminus \boldsymbol{z}$. This cover corresponds to a subgroup $\bar{G}(1)$ of index n. This gives a permutation representation $T : \pi_1 \to S_n$ by mapping $\bar{s}_i$ to s_i, $i = 1, \dots, r$. The image group G is exactly the geometric monodromy group of the cover.

Conversely, given $s_1, \dots, s_r \in S_n$ generating a group G, there is a cover $\phi : X \to \mathbb{P}^1_z$ ramified over the collection of points $\{z_1, \dots, z_r\} = \boldsymbol{z}$ having $s_1, \dots, s_r$ as its branch cycle description. This is a topological description, and it depends on the data for producing generators for π_1. Nevertheless, from [**Fr1**, Lemma 1], up to conjugation by S_n, the collection $\{\mathrm{C}_1, \dots, \mathrm{C}_r\}$ of conjugacy classes of $s_1, \dots, s_r$ in the group $< \boldsymbol{s} >$ is an algebraic invariant of this cover. This observation gives the definition of the *Nielsen class* of a cover.

Let G be a subgroup of S_n and let $\mathbf{C} = (\mathrm{C}_1, \dots, \mathrm{C}_r)$ be an r-tuple of nontrivial (not necessarily distinct) conjugacy classes of G.

Definition 3.1. To the data $(G, \mathbf{C})$ associate its *Nielsen class*:

$$\mathrm{Ni}(\mathbf{C}) = \{s \in G^r \mid < \boldsymbol{s} > = G,\ s_1 \cdots s_r = 1 \text{ and there exists } \omega \in S_r, s_{(i)\omega} \in \mathrm{C}_i, i = 1, \dots, r\}.$$

Suppose a cover $\phi : X \to \mathbb{P}^1$ has any branch cycle description $\boldsymbol{s}$, up to conjugation by elements of S_n, in $\mathrm{Ni}(\mathbf{C})$. We say the cover is in $\mathrm{Ni}(\mathbf{C})$. Alternatively, $\mathrm{Ni}(\mathbf{C})$ is the Nielsen class of the cover. The order we list the conjugacy classes doesn't matter.

Under certain assumptions, there is a space representing a solution to a natural *moduli problem*. This is the problem of parametrizing equivalence classes of covers in a given Nielsen class. *Hurwitz monodromy action* interprets properties of this moduli space. We explain the monodromy action. Still, we deal with a practical situation, so our example will illustrate rather than discuss the moduli properties. Consider the free group on generators Q_i, $i = 1, \dots, r-1$, with these relations:

$$Q_iQ_{i+1}Q_i = Q_{i+1}Q_iQ_{i+1}, i = 1, \dots, r-2; \tag{3.2a}$$

$$Q_iQ_j = Q_jQ_i, \ |i-j| > 1; \text{ and} \tag{3.2b}$$

$$Q_1Q_2 \cdots Q_{r-1}Q_{r-1} \cdots Q_1 = 1. \tag{3.2c}$$

This group, a quotient of the *Artin braid group*, is the *Hurwitz monodromy group* H_r of degree r. The Q_is act on $\mathrm{Ni}(\mathbf{C})$ by this formula: for $\boldsymbol{s} \in \mathrm{Ni}(\mathbf{C})$

$$(\boldsymbol{s})Q_i = (s_1, \dots, s_{i-1}, s_is_{i+1}s_i^{-1}, s_i, s_{i+2}, \dots, s_r), i = 1, \dots, r-1. \tag{3.2d}$$

Thus, they induce a permutation representation of H_r on $\mathrm{Ni}(\mathbf{C})$: the Hurwitz monodromy action on the Nielsen class $\mathrm{Ni}(\mathbf{C})$.

Definition 3.2. *Rational union of conjugacy classes.* Consider the union $S = \cup_{i=1}^r \mathrm{C}_i$ of elements in all conjugacy classes of $\mathbf{C}$. Let N be the least common multiple of all elements in S. We say $\mathbf{C}$ is a rational union of conjugacy classes if putting elements to powers relatively prime to N maps S into S.

Next we summarize basic moduli space properties when $\mathbf{C}$ is a rational union of conjugacy classes ([**Fr1**, §4 and 5], [**DFr**, §4] or [**FrV1**, Prop. 3]).

Theorem 3.3. *The cover $\mathcal{H}' \to \mathcal{H}$ has the properties stated in Part 3 of the proof of Theorem 2.5 if H_r acts transitively on* $\mathrm{Ni}(\mathbf{C})$.

§**3.2. Exceptional primitive covers of genus 0.** The group $D_{p'}$ has two types of conjugacy classes, one conjugacy class is of involutions, and $\frac{p-1}{2}$ conjugacy classes are powers of elements of order p'. We consider the case when all conjugacy classes in $\mathbf{C}$ are involutions. We call the corresponding covers *involution* realizations of $D_{p'}$. Thus, r must be even. From the Riemann-Hurwitz formula (1.3), $2(p+g-1) = r(\frac{p-1}{2})$. If a cover in this Nielsen class is of genus 0, then $r = 4$. For any (even) r transitivity holds in Theorem 3.3.

Theorem 3.4. *For any $r \geq 4$ when $G = D_{p'}$ and $\mathbf{C}$ consists of the conjugacy class of involutions, H_r is transitive on Ni($\mathbf{C}$). Thus, $\mathcal{H}'$ is an absolutely irreducible variety defined over $\mathbb{Q}$. For $(p, 2p') = 1$, the cover $\mathcal{H}' \to \mathcal{H}$ reduces modulo p to a cover with group identified with $(\mathbb{Z}/p)^*/ < \pm 1 >$. Further, each degree p' involution realization with geometric monodromy group $G = D_{p'}$ over*

$\mathbb{F}_q$ corresponds to a point $\boldsymbol{p} \in \mathcal{H}(\mathbb{F}_q)$ mod p: $\phi_{\boldsymbol{p}} : X_{\boldsymbol{p}} \to \mathbb{P}^1$. Then, $\phi_{\boldsymbol{p}}$ is an exceptional cover if and only if for a point $\boldsymbol{p}' \in \mathcal{H}'$ above $\boldsymbol{p}$, $[\mathbb{F}_q(\boldsymbol{p}') : \mathbb{F}_q] > 1$.

PROOF. An element $\boldsymbol{s} = (s_1, \dots, s_r)$ from this Nielsen class has $s_i = \left(\begin{smallmatrix} -1 & b_i \\ 0 & 1 \end{smallmatrix}\right)$ for some $b \in \mathbb{F}_{p'}$. The condition the product of the s_i s is 1 is that the alternating sum of the b_i's is 0. Consider the effect of Q_i on $\boldsymbol{s}$: it changes s_{i+1} to s_i and replaces s_i with $\left(\begin{smallmatrix} -1 & 2b_i - b_{i+1} \\ 0 & 1 \end{smallmatrix}\right)$. To assure the s_i s generate $D_{p'}$ requires only that the b_i s aren't all the same. Thus, transitivity of the action follows if the collection of linear transformations

$$\boldsymbol{b} \to (b_1, \dots, b_{i-1}, 2b_i - b_{i+1}, b_i, b_{i+1}, \dots, b_r)$$

is transitive on the hyperplane in affine $\boldsymbol{b}$-space defined by $b_1 - b_2 + \cdots - b_r = 0$ minus the scalar multiples of $(1, \dots, 1)$. Denote this space by $Y_r = Y_r(\mathbb{F}_p)$.

The effect of Q_i is to add $b_i - b_{i+1}$ to both the ith and i+1th positions. If $b_i - b_{i+1} \neq 0$, iterations of Q_i thereby allow adding arbitrary $b \in \mathbb{F}_p$ to both positions. Apply elements from H_r to braid to a situation where b_{r-2} and b_{r-1} are different. The computation above lets us add $b_r - b_{r-1}$ to both b_{r-2} and b_{r-1}. Thus, we may assume in the orbit of H_r a vector $\boldsymbol{b}$ with $b_{r-1} = b_r$. Suppose two from $b_1, \dots, b_{r-2}$ are distinct. Then, apply induction to braid on the first $r-2$ terms to get $(b_1, \dots, b_{r-2})$ to be an arbitrary member of $Y_{r-2}(\mathbb{F}_p)$. To complete the induction we must treat two cases: $r = 4$ and

$$b_1 = b_2 = \cdots = b_{r-2} \neq b_{r-1} = b_r. \tag{3.3}$$

If $r > 4$, we may braid to where we shift all subscripts by 2. Thus, case (3.3) reverts to the case we set up for induction. This leaves us only one case to check transitivity of the orbit of H_r. If $r = 4$ and $b_1 = b_2 \neq b_3 = b_4$ we must show we can braid to where b_1 and b_2 are arbitrary distinct elements in $\mathbb{F}_p$. This special case is in [**Fr4**].

Good reduction for $\mathcal{H}' \to \mathcal{H}$ isn't trivial, even in this special case. It follows from transitivity of H_r and a theorem of Grothendieck [**Gr**]. Fulton [**Fu**] explained this and [**FrV3**] has more details. □

It remains to effectively realize exceptional covers that arise from Theorem 3.4. Consider just the case $r = 4$ to give the flavor of the problem: [**DFr**, §5.2–§5.3] considers this example in the service of dihedral group realizations as Galois groups. Suppose p' is odd and different from p. Consider a rational function f giving an *exceptional involution cover* $f : \mathbb{P}^1_x \to \mathbb{P}^1_z$ over $\mathbb{F}_q$. In the regular representation of $D_{p'}$ the involutions are products of p' 2-cycles. Thus, each contributes p' to the right side of the Riemann-Hurwitz formula (1.3). Conclude: The genus of the Galois closure of the cover of f is g with $2(2p' + g - 1) = 4p'$: $g = 1$. The geometric Galois closure is a genus 1 curve. We get to this genus 1 curve by considering

$$Y' = \mathbb{P}^1_x \times_{\mathbb{P}^1_z} \mathbb{P}^1_x \setminus \Delta \tag{*}$$

as in §1.2.This is the usual fiber product from the Exceptionality Theorem 2.1. Then, f is exceptional if and only if no component of Y' is defined over $\mathbb{F}_q$. We now translate finding f to finding points on certain explicit classical curves.

A full explanation requires notation for the modular curves $X_0(p')$ and $X_1(p')$. These are projective completions of the quotients of the upper half plane by these subgroups of $\mathrm{PSL}_2(\mathbb{Z}) = \mathrm{SL}_2(\mathbb{Z})/\langle \pm 1\rangle$:

$$\Gamma_0(p') = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid ad - bc = 1, c \equiv 0 \bmod p' \right\} \text{ and}$$
$$\Gamma_1(p') = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(p') \mid a \equiv 1 \bmod p' \right\}.$$

There is a natural Galois cover $X_1(p') \to X_0(p')$ defined over $\mathbb{Q}$ with group $\mathbb{Z}/k$ with $k = (p-1)/2$.

COROLLARY 3.5. *Assume $q = p^a$ with $p \neq p'$. Exceptional involution covers $f : \mathbb{P}^1_x \to \mathbb{P}^1_z$ over $\mathbb{F}_q$ correspond to non-cusp points of $X_0(p')(\mathbb{F}_q)$ that lie under no point of $X_1(p')(\mathbb{F}_q)$. Two exceptional involution covers f_1 and f_2 correspond to the same point of $X_0(p')(\mathbb{F}_q)$ if and only if there exist linear fractional transformations λ and λ' (over $\mathbb{F}_q$) for which $\lambda(f_1(\lambda'(x))) = f_2(x)$.*

PROOF. Use the notation prior to the statement of the Corollary. List the components of Y' in (*) as $\mathcal{Y} = \{Y'_1, \dots, Y'_{\frac{p'-1}{2}}\}$. Any one of these is the genus 1 geometric Galois closure of the cover from f. Thus, all are isomorphic. If Y'_1 is defined over $\mathbb{F}_q = K$ (equivalent to all Y'_is are also), then f isn't exceptional. Otherwise it is and as in §1 we let $\hat{\mathbb{F}}_q = \hat{K}$ denote this minimal field of definition. Our concern is how to interpret this latter case. For notational simplicity we assume one orbit of $G(\bar{\mathbb{F}}_q/\mathbb{F}_q)$ on the collection $\mathcal{Y}$.

Over a finite field we have F. K. Schmidt's result: a genus 1 curve over $\mathbb{F}_q$ must have a rational point [**FrJ**, Cor. 3.11]. To see there must be a genus 1 curve defined over $\mathbb{F}_q$ hanging around in this construction, consider the collection $\boldsymbol{z} = \{z_1, \dots, z_4\}$ of branch points of $f : \mathbb{P}^1_x \to \mathbb{P}^1_z$. Since f is defined over $\mathbb{F}_q$, so is this collection $\boldsymbol{z}$. (Individual elements in the set may not be; $G(\bar{\mathbb{F}}_q/\mathbb{F}_q)$ permutes them as a set.) Above each branch point z_i there are $\frac{p'-1}{2}$ ramified points, and one unramified point x_i. Again, consider the action of $G(\bar{\mathbb{F}}_q/\mathbb{F}_q)$. It permutes the points in the fibers over the z_is, and it preserves the cover's ramification indices of the points in these fibers. Thus, it permutes the collection $\boldsymbol{x} = \{x_1, \dots, x_4\}$. Now, this set $\boldsymbol{x}$ consists exactly of the four branch points of any one of the Y'_is as a cover of $\mathbb{P}^1_x$. Thus, all of these are equivalent to a cover $\mu'' : Y'' \to \mathbb{P}^1_x$ defined over K. The composition, however, of this cover with f isn't a Galois cover over K. The automorphisms of $\phi'' : Y'' \to \mathbb{P}^1_z$ aren't defined over K.

Nevertheless, we recover f from the geometric data of the cover ϕ''. Its automorphisms (defined over $\hat{K}$) include an element α of order p'. From Schmidt's result, Y'' is an elliptic curve with a canonical involution τ relative to the origin for the group structure. From the structure of elliptic curves, α corresponds to

translation by a point $\boldsymbol{y}$ of order p'—in the case of concern, defined over $\hat{K}$, but not over K. As a set, however, the elements in the group $< \boldsymbol{y} >$ on Y'' are defined over K because this is true of α. We refer to [**R**, §III.4] for details on the geometric identification to statements on elliptic curves. Also, [**R**, p. 215] has explicit coordinates to find f from the multiplication formulas. Our desired f appears as the bottom row of the following commutative diagram:

$$\begin{array}{ccc} Y'' & \xrightarrow{\hat{\phi}} & Y''/\langle \boldsymbol{y} \rangle \\ \downarrow{\scriptstyle \mu''} & & \downarrow{\scriptstyle \mu''_{\boldsymbol{y}}} \\ Y''/\langle \tau \rangle = \mathbb{P}^1_x & \xrightarrow{\phi_f} & Y''/\langle \boldsymbol{y}, \tau \rangle = \mathbb{P}^1_z \end{array} \tag{$\dagger$}$$

This diagram is essentially the same as diagram (2.21) of [**Fr1**] in a related topic. Here $\mu_{\boldsymbol{y}}$ is the canonical involution on the elliptic curve $Y''/\langle \boldsymbol{y} \rangle$ naturally isogenous to Y''. By the way, the collection $\mathcal{Y}$ consists of elliptic curves gotten from Y'' by declaring a new group structure on Y''. You use a point from $\langle \boldsymbol{y} \rangle$ as the origin, instead of an origin provided by Schmidt's Theorem.

See [M2] for corroboration with the next statements. From an exceptional polynomial we get the upper row, a cover over K, of diagram †. This corresponds uniquely to a point on the reduction of $X_0(p')$ modulo p. That is, it produces—with slight abuse of notation—an element $\boldsymbol{t} \in X_0(p')(K)$. Further, f is exceptional precisely when $\boldsymbol{y}$—producing the isogeny of the upper row of †—isn't defined over K. This means a (any) point of $X_1(p')$ above $\boldsymbol{t}$ in the cover $X_1(p') \to X_0(p')$ mod p is not defined over K.

The equivalence between exceptional covers corresponding to f_1 and f_2 traces the statement of how such functions produce the corresponding elliptic curves in the upper row of †. These two curves appear as covers of $\mathbb{P}^1$ branched over four points. The linear fractional transformations effect changes in the two sets of branch points that don't affect the outcome of the top row of the diagram. This concludes the proof of the corollary. □

An analog of Corollary 3.5 for even values of r larger than 4 should follow the lead of [**DFr**]. The spaces that replace modular curves are covers of the moduli spaces of hyperelliptic curves of genus $\frac{r-2}{2}$.

§**3.3. Fiber products.** Assume we have a cover $\phi : X \to \mathbb{P}^1$ defined over $\mathbb{F}_q$. Consider the fiber product of $\phi : X \to \mathbb{P}^1$ with itself:

$$X \times_{\mathbb{P}^1} X = \{(x_1, x_2) \mid \psi(x_1) = \psi(x_2)\}. \tag{3.4}$$

Exceptionality is equivalent to $X \times_{\mathbb{P}^1} X \setminus \Delta$ has no absolutely irreducible components over $\mathbb{F}_q$. Since it is more convenient to study primitive covers, we ask a question of any (not just exceptional) cover $\phi : X \to \mathbb{P}^1$.

(3.5) When does there exist a cover $\psi : W \to \mathbb{P}^1$ such that $\phi : X \to \mathbb{P}^1$ factors as $\rho : X \to W$ composed with ψ with both maps of degree exceeding 1?

[**FrMa**] gave an answer when ϕ is a polynomial cover. [**AGR**] has a proof based loosely on [**FrMa**] when ϕ is of genus 0. The next proposition—a proof will appear elsewhere—shows this is essentially a group theoretic idea.

PROPOSITION 3.6. *Condition* (3.5) *holds if and only if* $X \times_{\mathbb{P}^1} X$ *contains a subset of form* $X \times_W X$.

REMARK 3.7. *Practicality of Prop. 3.6.* When $X = \mathbb{P}^1$, [**AGR**] notes that Prop. 3.5 gives a practical criterion for primitivity. Starting from $f : \mathbb{P}^1 \to \mathbb{P}^1$, you factor $(f(x) - f(y))/(x - y)$ (after removing denominators). Then, check if any of the factors are of the form $(g(x) - g(y))/(x - y)$ with g a rational function of degree at least 2. Now that there are programs that factor polynomials in several variables over $\mathbb{Q}$ in polynomial time, this method is feasible. By contrast, computing the Galois group of the splitting field of $f(x) - z$ over $\mathbb{Q}(z)$ is not. The latter is natural, for it certainly tests for primitivity of the group, and this is equivalent to primitivity of the cover.

§**3.4. Median Value curves.** Suppose Y is a curve over $\mathbb{F}_q$. Recall: Y is a *median value* curve if $|Y(\mathbb{F}_{q^t})| = q^t + 1$ for ∞-ly many values of t (condition (0.4)). We call s a (median value) *modulus* for Y if this holds for all t with $(t, s) = 1$. Statement 3.11 says every median value curve has a modulus. This subsection uses fiber products to relate median value curves to exceptional covers. This leaves unsolved problems questioning which median value curves arise as exceptional covers.

LEMMA 3.8. *Suppose* $\phi : X \to \mathbb{P}^1$ *is exceptional and* Y *is of median value. Form* $Z = X \times_{\mathbb{P}^1} Y$. *Use any map* $\psi : Y \to \mathbb{P}^1$. *Then,* Z *is an exceptional cover of* Y. *Note:* Z *is not necessarily an exceptional cover of* $\mathbb{P}^1$.

PROOF. Let s_X (resp. s_Y) be the modulus of X (resp. Y) as a median value curve. We show Z is an exceptional cover of Y using those values of t with $(t, s_X s_Y) = 1$. Consider such a t. Let $\boldsymbol{y} \in Y(\mathbb{F}_{q^t})$. Since $(t, s_X) = 1$, there is exactly one point of $X(\mathbb{F}_{q^t})$ above $\psi(\boldsymbol{y})$. Thus, $|X(\mathbb{F}_{q^t})| = q^t + 1$. The General Exceptionality Theorem now implies Z is an exceptional cover of Y. □

Theorem 2.5 produces general exceptional covers in great abundance. It starts with the data for a geometric/arithmetic pair, and produces exceptional covers over almost all prime finite fields realizing this. Its present formulation, however, leaves uncertainty on which primes p are the exceptions. Thus, Lemma 3.8 has a different value. Once we have one exceptional cover over $\mathbb{F}_q$, we produce many related others. Our next example—an immediate corollary of Lemma 3.8—emphasizes this point.

EXAMPLE 3.9. Let $f : X = \mathbb{P}^1 \to \mathbb{P}^1$ be an exceptional polynomial, $g : Y = \mathbb{P}^1 \to \mathbb{P}^1$ any polynomial. Form $Z = \{(x, y) | f(x) = g(y)\}$. Denote projection on the y variable by $\phi : Z \to \mathbb{P}^1_y$. Ex. 3.14 revisits this. □

We now consider further a mystery. Lemma 3.8 produces a natural equivalence relation on median value curves over $\mathbb{F}_q$: Y versus $Z = X \times_{\mathbb{P}^1} Y$. A representative Y of a class of median value curves over $\mathbb{F}_q$ is minimal if it has no exceptional cover $Y \to Z$ with Z a median value curve.

MEDIAN VALUE CURVE QUESTION 3.10. *Suppose Y is a median value curve over $\mathbb{F}_q$ with modulus s_Y. Under what circumstances can you present Y as an exceptional cover, corresponding to the modulus s_Y? Specifically: What are the minimal median value curves?*

Suppose Y and Y' are curves over $\mathbb{F}_q$. We say Y' is a *twist* of Y over $\mathbb{F}_{q^s}$ if there is an isomorphism $\psi : Y \to Y'$ (whose graph is) defined over $\mathbb{F}_{q^s}$. Noam Elkies suggested the use of S-integers for the next proof.

MEDIAN VALUE CURVE STATEMENT 3.11. *Suppose X is a median value curve over $\mathbb{F}_q$. Then, there exist an integer a and an integer s_X for which $|X(\mathbb{F}_{q^t})| = q^t + 1$ for all t in the arithmetic progression $\{a + ms_X\}_{m\in\mathbb{Z}}$.*

PROOF. Recall these facts from the Riemann Hypothesis Lemma 2.2. If X is of genus g: $|X(\mathbb{F}_{q^t})| = q^t + 1 - S_t$ with

$$S_t = \sum_{i=1}^{2g} \alpha_i^t, \tag{3.6a}$$

$$\alpha_i \text{ s algebraic integers },|\alpha_i| = q^{1/2}, \text{ and } \alpha_i\alpha_{i+g} = q. \tag{3.6b}$$

Then, X is median value exactly when S_t is 0 for infinitely many t.

Now apply the theory of S-integers in the form of [**V**, Theorem 2.3.1]. Let Γ be a finitely generated subgroup of L^*, the multiplicative group of nonzero elements of a number field L. Then, all but finitely many solutions of

$$u_1 + \cdots + u_n = 1, \qquad u_i \in \Gamma \tag{**}$$

lie in one of the diagonal hyperplanes H_I defined by the equation $\sum_{i\in I} x_i = 0$ where I is a subset of $\{1, \dots, n\}$ with at least two, but no more than $n - 1$, elements. We take Γ to be the multiplicative subgroup generated by $\beta_{i-1} = \alpha_i/\alpha_1$, $i = 2, \dots, 2g$, $n = 2g - 1$. Apply an induction on n. If some proper subset of the α_i sum to 0, then we have two subsets of power sums equal 0. Find an arithmetic progression for the first, and we automatically get one for the second. Thus, for the conclusion we get, assume no proper subset of the α_i^t s sums to 0 for infinitely many t. Then, one of two things happens according to [**V**, loc. sit.]. Either:

(3.6c) for infinitely many values of t, $(\beta_1^t, \dots, \beta_{2g-1}^t)$ is a constant vector; or
(3.6d) some proper subset of the β_i^t s sums to 0 for infinitely many t.

By hypothesis (3.6d) doesn't happen, so it must be (3.6c). This says, the β_i s are roots of 1, and thereby the α_i s are some constant, independent of i, times roots of 1. Conclude the theorem easily. □

The proof of Statement 3.11 shows an elementary statement is equivalent to X being a Median value curve. It is a simple statement about the eigenvalues of the Frobenius. You can partition these into subsets $\{S_1, \dots, S_u\}$ where the following hold.

(3.7a) For each j, $S_j = \{\zeta_m \alpha, m = 1, \dots, r_j\}$, with ζ_m some root of 1.

(3.7b) For some integer a (independent of j), $\sum_{m=1}^{r_j} \zeta_m^a = 0$. If s is the least common multiple of the orders of all these roots of 1, then for any integers v, n with $(v, s) = 1$, integers t of the form $va+ns$ satisfy $|X(\mathbb{F}_{q^t})| = q^t+1$.

Refer to such a set of t as a *median value progression* $P(a, s)$ for X.

Median Value Curve Problem 3.12. *Suppose X is a median value curve over $\mathbb{F}_q$ with for a median progression of form $P(a, s)$. Is the Jacobian of X isogenous (over $\bar{\mathbb{F}}_q$) to the Jacobian of a curve X' (over $\mathbb{F}_q$) that one can present as an exceptional cover?*

We say X_1 is a *twist* of X_2 (projective nonsingular curvesX_1 and X_2 are isomorphic over a finite extension $\mathbb{F}_{q^a}$ for some a. Thus, the zeta functions of X_1 and X_2 are the same over $\mathbb{F}_{q^a}$. Deduce that the zeros of the zeta function of X_1, each multiplied by some root of 1, give the zeros of the zeta function of X_2. This takes advantage of the formula [**FrJ**; p. 31]: $Z_{\mathbb{F}_q^a}(X, u^a) = \prod_{\zeta^a=1} Z_{\mathbb{F}_q}(\zeta u)$. The zeta functions of two curves are the same if and only if the jacobians of the curves are isogenous over $\mathbb{F}_q$ ([**Se2**; p.] for elliptic curves and [**ST**] in general).

§**3.5. Cryptology covers and zeta functions.** We use the notation of the proof of Statement 3.10. Even genus 1 median value curves present challenges. Still, they are suitably limited to allow us to make valuable statements.

Example 3.13. *X in Statement 3.11 has genus 1.* Consider the case when $g = 1$. With $t = 1$, $\alpha_1\alpha_2 = q$.

(3.7) $\alpha_1 = \sqrt{-1}\sqrt{q}$ and $\alpha_2 = -\sqrt{-1}\sqrt{q}$.

When (3.8) holds, $|X(\mathbb{F}_{q^t})| = q^t + 1 \bmod p$ for all t. Since $g = 1$, these points form a group. Conclude: X has no points of order p over any finite field, it is a *supersingular* elliptic curve [**R**, p. 239]. Also, condition (3.7) determines the zeta function of the curve. For a given p, up to endomorphisms between curves, there are only finitely many supersingular curves [**R**, p. 233, Theorem 2].

If $t \equiv 2 \bmod 4$, $|X(\mathbb{F}_{q^t})| = q^t+1+2\sqrt{q}$ over $\mathbb{F}_{q^t}$: the maximal number allowed by the Riemann Hypothesis for genus one. □

Example 3.14. *Elkies-v.d. Geer-vd v.d. Vlugt curves* [**GV**]. Take $q = p^m$. Concentrate on projective curves $C = C_R$ with affine equation

$$y^p - y = xR(x), \qquad R \in R_h = \{\sum_{i=0}^{h} a_i x^{p^i}, x \in \mathbb{F}_q\}.$$

The trace, $\mathrm{Tr} = \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}$ from $\mathbb{F}_q$ to $\mathbb{F}_p$, allows us to state the properties in [**GV**].

Take $p^{2h} \leq q$ and consider

$$W_R = W = \{x \in \mathbb{F}_q \mid \mathrm{Tr}[xR(u) + uR(x)] = 0 \ \forall u \in \mathbb{F}_q\}.$$

Result: With $w = |W|$, $|C(\mathbb{F}_q)| = q + 1$ if $m - w$ is odd, $q + 1 \pm (p-1)\sqrt{qp^w}$ if $m - w$ is even. Indeed, the genus $p^h(p-1)/2$ curve C_R has the genus $(p-1)/2$ curve $y^p - y = x^2$ as a quotient over the algebraic closure in p^h different ways. Final Conclusion of [**GV**, Prop. 14.4]: The Jacobian variety of C_R is isogenous over $\bar{\mathbb{F}}_p$ to a product of supersingular elliptic curves.

Take any C_R defined over $\mathbb{F}_{p^m}$ with $m - w$ odd. For values of t divisible by m, consider C_R over $\mathbb{F}_{p^t}$. Then, take $m_t = t - w_t$ where w_t is the value of W computed relative to the field $\mathbb{F}_{p^t}$. This presents the problem of calculating the values of t for which m_t is odd. Then, C_R is a median value curve exactly if m_t is odd for infinitely many t. □

As a subexample to Example 3.14, take the case $p = 3$ and consider the projective curve C with affine equation $y^3 - y = x^2$ over $\mathbb{F}_3$. It is isomorphic to the curve C' with equation $y^3 + y = x^2$ over the quadratic extension of $\mathbb{F}_3$: they are twists of one another (§3.4). Over $\mathbb{F}_3$, $y^3 + y$ is an exceptional polynomial. It is one-one over the odd degree extensions of $\mathbb{F}_3$. Thus C' is a median value curve from the fiber product construction of Example 3.9. Both C and C' have four rational points over $\mathbb{F}_3$, counting the point at ∞. The theory of Example 3.13 shows they have the same zeta function.

A Theorem of Tate says the zeta function determines the curve's isogeny class. Here we can see the isogeny. Take $\psi : C \to C'$ by $(x, y) \mapsto (x, \sqrt{-1}y)$. Although ψ isn't defined over $\mathbb{F}_3$, the sum of it and its conjugate ψ' gives us a map defined over $\mathbb{F}_3$. Call this $\Psi : C \to C'$: $\Psi(x, y) = (x, \sqrt{-1}y) \oplus (x, -\sqrt{-1}y)$ where $\oplus$ indicates we add the two points together using addition on C'. This illustrates the twists in Problem 3.12. Similar remarks apply to all curves in Example 3.14 from using $y^p - dy$ with $y^{p-1} - d$ having no zeros over $\mathbb{F}_q$.

Example 3.15. *Median value curves that aren't supersingular.* The examples above came from curves whose jacobians are isogenous to products of supersingular elliptic curves. Now, consider any ordinary (not supersingular) elliptic curve E over $\mathbb{F}_q$. Assume the curve is in Weierstrass normal form and let τ be the involution associated with the degree two projection to $\mathbb{P}^1_x$. Form a *quadratic twist* E' of E as follows. For $e \in E$, it is natural to identify $\tau(e)$ with $-e$, the inverse point on the elliptic curve.

Let Fr_q be the Frobenius endomorphism. It acts on the $\mathrm{Spec}(\mathbb{F}_q)$ scheme $V = E \otimes \mathrm{Spec}(\mathbb{F}_{q^2})$. This scheme is reducible over the algebraic closure of $\mathbb{F}_q$. Let e represent a geometric point of E and α a generator of $\mathbb{F}_{q^2}$ over $\mathbb{F}_q$. Then, geometric points of V are of form $(e \otimes \alpha)$ or $(e \otimes \alpha')$ with α' the conjugate of α over $\mathbb{F}_q$. These are the specializations of the generic point $(e^{\mathrm{gen}}, \alpha)$ where e^{gen} is a generic point of E. Now, define E' to be the absolutely irreducible $\mathbb{F}_q$ curve

whose points are the unordered pairs of points $\bar{e} = \{(e,\alpha), -e, \alpha')\}$. That is, E' is the quotient of V by the natural action (τ, Fr_q).

Suppose ℓ is prime to p. Then, the ℓ-adic Tate module of E' consists of the projective limit of those points $\bar{e}$ where e is an ℓ^n division point. Now apply Fr_q to such an ℓ-adic division point $\bar{e} = \{(e,\alpha), -e, \alpha')\}$ to get

$$\mathrm{Fr}_q(\bar{e}) = \{(\mathrm{Fr}_q(e), \alpha'), -\mathrm{Fr}_q(e), \alpha)\}.$$

(3.8) The eigenvalues of Fr_q on the Tate module for E' are minus those for Fr_q on the Tate module for E.

In particular, if C is a curve whose Jacobian is isogenous to $E \times E'$, then C is a median value curve.

An example of E has affine portion $\{(x,y) \mid y^2 = x^3 - x^2 - x\}$. Then, E has exactly two points over $\mathbb{F}_3$. So, with α_i, $i = 1, 2$, the eigenvalues of the Frobenius, the Weil polynomial is $(1-\alpha_1 t)(1-\alpha_2 t) = 1 - 2t + 3t^2$. The twist of this curve has affine equation $2y^2 = x^3 - x^2 - x$. It has six points and so its Weil polynomial is $1 - 2t + 3t^2$. □

References

[AGR] Cesar Alonso, Jaime Gutierrez and Tomas Recio, *A rational function decomposition algorithm by near-separated polynomials*, preprint (1993).

[ASp] A. Adolphson and S. Sperber, *p-adic estimates for exponential sums and the theorem of Chevalley-Warning*, Ann. Scient. E. N. Superior **4th series 20** (1987), 545–556.

[C] S. Cohen, *Permutation Polynomials and Primitive Permutation Groups*, Arch. Math. **57 #2992** (1991), 417–423.

[C2] S. Cohen, *Proof of a conjecture of Chowla-Zassenhaus*, Canadian Math. Bull **33** (1990), 230–234.

[C3] S. Cohen, *The distribution of polynomials over finite fields*, Acta. Arith. **17** (1970), 259–273.

[CM] S. Cohen and R. Matthews, *A Class of Exceptional Polynomials*, preprint (Jan. 1994).

[DFr] P. Debes and M.D. Fried, *Nonrigid constructions in Galois theory*, Pac. Jour. **163 #1** (1994), 81–122.

[D] L. E. Dickson, *The analytic representation of substitutions on a power of a prime number of letters with a discussion of the linear group*, Ann. Math. **11** (1897), 65–120, 161–183.

[Fr1] M. Fried, *Exposition on an Arithmetic-Group Theoretic Connection via Riemann's Existence Theorem*, A.M.S. Publications, Proceedings of Symposia in Pure Math: Santa Cruz Conference on Finite Groups,, vol. 37, 1980, pp. 571–601.

[Fr2] M. Fried, *On a conjecture of Schur*, Mich. Math. Journal **17** (1970), 41–55.

[Fr3] M. Fried, *On a theorem of MacCluer*, Acta Arith. **25** (1974), 122–127.

[Fr4] M. Fried, *Galois groups and complex multiplication*, TAMS **235** (1978), 141–162.

[Fr5] M. Fried, *The Nonregular Analogue of Čebotarev's Theorem*, PJM **113** (1984), 1–9.

[Fr6] M. Fried, *Arithmetical properties of function fields (II): the generalized Schur problem*, Acta Arith. **25** (1974), 225–258.

[Fr7] M. Fried, *On Hilbert's irreducibility theorem*, J. Number Theory **6** (1974), 211–232.

[FJ] M.D. Fried and M. Jarden, *Field Arithmetic*, Ergebnisse der Mathematik III, vol. 11, Springer Verlag, Heidelberg, 1986.

[FHJ] M.D. Fried, D. Haran and M. Jarden, *Counting points on definable sets over finite fields*, Israel J. **85** (1994), 103–133.

[FV1] M.D. Fried and H. Völklein, *The inverse Galois problem and rational points on moduli space*, Math. Ann. **290** (1991), 771–800.
[FV2] M.D. Fried and H. Völklein, *The embedding problem over a Hilbertian PAC-field*, Annals of Math. **135** (1992), 469–481.
[FrV3] M. Fried and H. Völklein, *Explicit realization of geometric/arithmetic monodromy group pairs over finite fields and excluded primes*, in preparation..
[FGS] M. Fried, R. Guralnick and J. Saxl, *Schur Covers and Carlitz's Conjecture*, Thompson Volume, Israel J. **82** (1993), 157–225.
[FrMa] M. Fried and R. MacRae, *Variables separated curves*, Math. Ann. **180** (1969), 220–226.
[Fu] W. Fulton, *Hurwitz schemes and irreducibility of moduli of algebraic curves*, Annals of Math. **90** (1969), 542-575.
[GV] v.d. Geer and v.d. Vlugt, *Reed-Muller Codes and Superingular Curves*, Compositio Math. **84** (1992), 256–272.
[GV2] v.d. Geer and v.d. Vlugt, *Generalized Hamming Weights of Codes and Curves over Finite Fields with Many Points*, preprint, Jan. 1994..
[Gr] A. Grothendieck, *Géométrie formelle et géométrie algébrique*, Seminaire Bourbaki **182** (1958/59), t. 11.
[GS] R. Guralnick and J. Saxl, *Monodromy groups of polynomial*, preprint, Jan. 1994.
[Ha] D. Harbater, *Abhyankar's conjecture on Galois groups over curves*, to appear, Invent. Math. (1994).
[H] D. R. Hayes, *A geometric approach to permutation polynomials over a finite field*, Duke Math. J. **34** (1967), 293–305.
[K] N. M. Katz,, *On a theorem of Ax*, Amer. J. Math. **93** (1971), 485–499.
[LN] R. Lidl and H. Niederriter, *Finite Fields*, Encyclopedia of Mathematics and its applications, vol. 20, Addison-Wesley, Reading, 1983.
[LPS] M. Liebeck, C. Praeger, J. Saxl, *Mem. AMS #432*, vol. 86, 1990.
[M] B. Mazur, *Frobenius and Hodge Filtration*, Annals of Math. **98** (1973), 58–95.
[M2] B. Mazur, *Lecture Notes in Mathematics*, vol. 601, Springer-Verlag, 1977, pp. 107–148.
[MM] O. Moreno and C.J. Moreno, *A p-adic Serre Bound*, preprint , July 1993 (1993).
[Mu] P. Müller, *New examples of exceptional polynomials*, Proceedings of 2nd Internat. conference on Finite Fields, CM, G.L. Mullen and P.J. Shiue (eds), 1994.
[Mum] D. Mumford, *Introduction to algebraic geometry*, Harvard Notes, 1968.
[Ra] M. Raynaud, *Revêtements de la droite affine en caractéristique $p > 0$ et conjecture d'Abhyankar*, to appear, Invent. Math. (1994).
[R] A. Robert, *Elliptic curves*, Lecture notes in Mathematics, vol. 326, Springer-Verlag, Berlin • Heidelberb • New York, 1973.
[Se] J.-P. Serre, *Sur le nombre des points rationnels d'une courbe algébrique sur un corps fin*, C.R. Acad. Sci.Paris, sèrie I **296** (1983), 397–402.
[Se2] J.-P. Serre, *Abelian ℓ-adic representations and elliptic curves*, 1st ed., McGill University Lecture Notes, Benjamin, New York • Amsterdam, in collaboration with Willem Kuyk and John Labute..
[ST] J.-P. Serre and J. Tate, *Good reduction of abelian varieties* **78** (1968), 492–517.
[W] D. Wan, *Permutation polynomials and resolution of singularities over finite fields*, Proc. Amer. Math. Soc. **110** (1990), 03–309.
[V] P. Vojta, *Lecture Notes in Mathematics*, vol. 1239, Springer-Verlag, 1987.
[We] H. Wielandt, *Primitive Permutationsgruppen von Grad $2p$*, Math. Z. **63** (1956), 478–485.

UC Irvine, Irvine, CA 92717, USA

E-mail address: mfried@math.uci.edu