Diophantine statements over Residue fields: Galois Stratification and Uniformity

Michael D. Fried, Emeritus Professor of Mathematics
University of California at Irvine

We consider three general problems about Diophantine statements over finite fields that connect to the *Galois stratification* procedure for deciding such problems. To bring to earth the generality of these problems, we clarify each using the negative solution of a U. Felgner's simply stated question relating pairs of finite fields $\mathbb{F}_p$ and $\mathbb{F}_{p^2}$ for large primes p.

For a diophantine problem, D, interpretable for almost all primes p, the paper plays on attaching a Poincaré series, $P_{D,p}$, to (D, p). The rationality and computability of $P_{D,p}$ as p varies gives some aspects of continuity. Most interesting, though, is how the coefficients of $P_{D,p}$ vary with p. The paper notes three ways to give counts for those coefficients:

- points mod p achieving particular conjugacy classes in a Galois stratification;
- points mod p on absolutely irreducible varieties; or
- traces of the p Frobenius on a Chow motive.

The gist of this paper, using one explicit well-known dophantine problem, is that Galois stratification naturally tethers these three abstract approaches. [FrS76], [FrJ04], [DL98] and others (cited in §3) give a long history of the fundamental ideas. So, it is time for an introduction relating the ideas to Deligne's proof of the Weil Conjectures and Langland's Program applied to a specific recognizable problem.

1 Three general problems on finite field equations

Traditional diophantine statements consider algebraic subsets of affine space with blocks of variables with some, say $\boldsymbol{x} = (x_1, \dots, x_m)$, unquantified, and others, say $\boldsymbol{y} = (y_1, \dots, y_n)$, quantified by the symbols $\exists$ and $\forall$. Questions over finite fields often assume the equation coefficients are in $\mathbb{Z}$. For example, they might consider $\boldsymbol{x}$ and $\boldsymbol{y}$ taking values in the residue class fields $\mathbb{F}_p$, and ask if the statements are true for almost all p.

1.1 Introducing the three problems

Long time results on variants using *Galois stratification* (§2.1) have detailed literature as in [FrJ04, Chaps. 30-31]. There are, however, three topics inadequately treated there.

(1.1a) Testing how a quantified D over distinct residue fields cohere – *uniformity in p* – using equivalent data from reducing an unquantified object over $\mathbb{Q}$ mod most primes p.

(1.1b) Coordinating (*) affine space arguments and (**) arithmetic homotopy with scheme or *projective geometry* language (the natural domain of arithmetic geometry).

(1.1c) Considering statements with variables taking values in the algebraic closure of $\mathbb{F}_p$, but fixed by respective powers of the Frobenius Fr_p:

$$\text{for } \boldsymbol{x} \text{ (resp. } \boldsymbol{y})(\mathrm{Fr}_p^{d_1}, \dots, \mathrm{Fr}_p^{d_m}) \stackrel{\text{def}}{=} \mathrm{Fr}_p^{\boldsymbol{d}} \text{ (resp. } (\mathrm{Fr}_p^{e_1}, \dots, \mathrm{Fr}_p^{e_n}) = \mathrm{Fr}_p^{\boldsymbol{e}}). \tag{1.2}$$

To help understand aspects of all three problems we use Felgner's Problem:

Can we define the fields $\mathbb{F}_p$ within the theory of the fields $\mathbb{F}_{p^2}$.

Comments on (1.1a): For any prime p in (1.1a), a *Galois stratification* allows eliminating the quantifers on the variables, producing a quantifer free statement. The $\mathbb{Q}$ object in (1.1a) – a Galois stratification object, but over $\mathbb{Q}$ rather than over a finite field – has not been previously emphasized, though it has always been present. Though more general than a pure algebraic variety, it allows all the elimination theory and reductions mod primes.

At the heart of the Galois stratification procedure is its use of the *non-regular Chebotarev analog*. For this we use the acronym **NRC**. Both the non-regular adjective and the Chebotarev error term impact its use, as revealed by the negative solution of Felgner's Problem. It appears in two ways:

(1.3a) Eliminating quantifiers, the main reason we introduced the stratification procedure; and

(1.3b) estimating the unquantified variable values satisfying the diophantine conditions.

We can untangle the two steps of (1.3). So doing reveals two separate aspects of the stratification procedure. Its use in (1.3a) for collecting finite fields points. Then, its generalization of quantifier elimination over many other collections of fields, as appears in [FrJ04, Chap. 30] as well as the variant given in (1.1c).

Starting with an elementary diophantine statement (problem) D, the procedure generalizes elementary statements to Galois stratifications $\mathcal{S}$. In each generalizing case, every step of the stratification procedure produces a new Galois stratification. The number of steps depends on the number of blocks of quantified variables. §2.1 gives the notation and explains the main theorem as given in several sources starting from [FrS76].

That is, suppose there are k blocks of quantified variables. For each prime p this produces $\bar{\mathcal{S}}_p \stackrel{\text{def}}{=} \{\mathcal{S}_{p,k}, \dots, \mathcal{S}_{p,0}\}$, a sequence of Galois stratifications (starting at k going to 0), and a finite Galois extension $\hat{K}/\mathbb{Q}$ (with group G_P). Excluding a finite computable set of primes p these have the following property. For p a prime unramified in $\hat{K}$, denote an element of the conjugacy class of the Frobenius at p by Fr_p, and its fixed field in $\hat{K}$ by $\hat{K}_p$.

$$\begin{array}{c}\text{For each conjugacy class C of values of the Frobenius, } \mathrm{Fr}_p \in G_P, \\ \text{there is an object } \bar{\mathcal{S}}_{\mathrm{C}} \text{ over } \hat{K}_p \text{ whose reduction mod a prime above } p \text{ gives } \bar{\mathcal{S}}_p.\end{array} \quad (1.4)$$

That gives a start to many aspects of uniformity in p.

One form of the stratification procedure moves through field theory – after all, *Field Arithmetic* is the [FrJ04] title – based on *Frobenius fields*. While we still rely on details on the stratification procedure, §2.2 gives an overview hitting the most significant of those details. Especially it shows the role of the Chebotarev analog.

§2.3 emphasizes the word *non-regular* in that analog and its subtleties. For example, this gives the main distinctions, running over classes C in G, between the collections $\bar{\mathcal{S}}_{\mathrm{C}}$.

Comments on (1.1b): From the beginning there was an idea of attaching a more concise object, a Poincare series $P_p \stackrel{\mathrm{def}}{=} P_{D,p}$, to $\bar{\mathcal{S}}_p$. The stratification procedure was the main tool in showing this object to be a computable rational function. The tension between (*) and (**) in (1.1b) appeared long before [FrS76] as recounted in [Fr12] where this author's applications to finite field questions used Riemann's work and projective geometry. The tension continued:

- on one hand, in applying Bombieri's use of Dwork's affine/singular theory of the zeta function to explicitly compute stratification Poincaré series *characteristics*; and,
- on the other, the Denef-Loeser (and Nicaise) production of Poincaré series coefficients as Chow motives. Deligne's proof of the Weil conjectures is in the background.

Continuing the comments on (1.1a), the *nonregular* adjective shows in Thm. 2.11. It gives how the stratification procedure varies with either the prime p (or in applying it to a specific finite field, the extension $\mathbb{F}_q$ for q a power of p).

§2.3.3 applies the Main Thm. to Felgner's problem. Here – I suspect a careful reader will agree – a mere cardinality estimate, rather than some precise understanding of the variance with either the prime p or the extension $\mathbb{F}_q$ for q a power of p, seems inadequate.

Yet, there is considerable flexibility in how those Poincaré series capture information. §3.3.1 illustrates with an a diophantine example the author has used with undergraduates. (Proofs are another matter.) This example helps picture how the reference to Chow motives, as pieces of étale cohomology groups, works.

Comments on (1.1c): §1.2 explains Felgner's problem in very down-to-earth language. Felgner is a piece from the case $m = 1$, $d_1 = 1$, with all e_i s equal to 2. It poses for Galois stratifications – expanded by *Frobenius vectors* (like $\mathrm{Fr}_q^{\boldsymbol{d}}$) – the nature of corresponding Poincaré series. For example, when can they be derived from standard Poincaré series?

This latter story passes through work of D. Wan, who introduced a Zeta function in the unquantified case, generalizing Artin's zeta where all d_i s are 1, and Hrushovski and Tomasic who took a model theoretic approach, enhanced by Galois stratification.[1]

From constraints on space and time, we limit our responses to questions (1.1b) and (1.1c) to merely motivating seriously using these Poincaré series, as if their coefficients are

1 This starts with Ax and Kochen on the Artin Conjecture on p-adic points on forms of degree d in projective d^2-space. To understand my motivation, consider the down-to-earth problems I connected to classical arithmetic geometry as recounted in the partially expository [Fr05] and [Fr12].

Chow motives to which you apply the Frobenius Fr_p. Our goal is to ask questions about their variance with p. Especially for what p certain especially simple results occur, as given explicitly in our example. We expect to expand on parts of §4 in a later paper.

1.2 Felgner clarifies what are statements over finite fields

A traditional question in the theory of finite fields starts with blocks of variables $\boldsymbol{y}_i \in \mathbb{A}^{n_i}$, $i = 1, \dots, k$. Below we use the notation $\sum_{j=1}^{k} n_j \stackrel{\text{def}}{=} N_k$. Assume these blocks are respectively quantified by $Q_1, \dots, Q_k = \boldsymbol{Q}$. Also we have a separate unquantified block of variables $\boldsymbol{x} \in \mathbb{A}^m$ together with an algebraic set X described by

$$\{(\boldsymbol{x}, \boldsymbol{y}_1, \dots, \boldsymbol{y}_k) \mid \varphi(\boldsymbol{x}, \boldsymbol{y}_1, \dots, \boldsymbol{y}_k)\}.$$

Here φ is a collection of polynomial equalities and inequalities with coefficients in a ring R, defining a constructible subset of $\mathbb{A}^{m+N_k}$. A traditional question is, given φ and $Q_1, \dots, Q_k$, and no $\boldsymbol{x}$ variables, is there a useful procedure for deciding if the statement is true for *almost all* finite fields $\mathbb{F}_q$ in the following collections.

(1.5a) $R = \mathbb{F}_p$: q are powers of a given p.
(1.5b) $R = \mathcal{O}_K$, ring of integers of a number field K: $q = |\mathcal{O}_K/\boldsymbol{p}|$, orders of residue class fields.
(1.5c) $R = \mathbb{Z}$, the whole Universe case: All $\mathbb{F}_q$.

§2.1 explains the Main Theorem of Galois stratification. It is a stronger result than that above in that our starting statement usually includes unquantified variables $\boldsymbol{x}$. Then, the result is that the starting statement – with, excluding $\boldsymbol{x}$, all variables quantified – is equivalent to one with no quantified variables. That is, it gives an *elimination of quantifiers*. We use Felgner's problem [Fe90] to show its value and how it works.

In each case, in changing "almost all" to "all,", our method (and generalizations) leaves checking a finite number of prime powers. For some problems those exceptional qs could be accidents. For others – motivated by classical cases – they could be significant. The Poincaré series approach (§3.1), seeking a significant rational function, has been the gold standard.

Felgner – in language reminiscent of the above (with $m = 1$) – asks if given $x' \in \mathbb{F}_{p^2}$,

$$\text{is } (x', \boldsymbol{y}_1, \dots, \boldsymbol{y}_k) \in X \text{ true for } Q_1\boldsymbol{y}_1 \dots Q_k\boldsymbol{y}_k \in (\mathbb{F}_{p^2})^{N_k}, \text{ if and only if } x' \in \mathbb{F}_p?$$

Except we are asking about a different set – $\{\mathbb{F}_{p^2} \mid p \text{ prime }\}$ – of fields than those included in any of the lists (1.5). Our method easily tolerates such flexibility. Further, the negative conclusion holds even if we asked for its truth replacing p by prime-powers q ($\mathbb{F}_p \mapsto \mathbb{F}_q$, $\mathbb{F}_{p^2} \mapsto \mathbb{F}_{q^2}$) and just for *infinitely* many q.

The conclusion about the set of such x' opens territory that isn't hinted at by the list (1.5). Still, the nature of that set arising with actual problems in finite fields (as in §3.3), is the model for which the original result aimed. Here is an example of what we will exclude. Take $k = 2$, and $\boldsymbol{Q} = (\exists, \forall)$. Read this as follows.

(1.6a) Given $x' \in \mathbb{F}_q$, there exists $\boldsymbol{y}_1' \in (\mathbb{F}_{q^2})^{n_1}$ with $\boldsymbol{y}_2' \in (\mathbb{F}_{q^2})^{n_2}$, so that $(x', \boldsymbol{y}_1', \boldsymbol{y}_2') \in X$.

(1.6b) But if $x' \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$, then for any $\boldsymbol{y}'_1 \in (\mathbb{F}_{q^2})^{n_1}$ there is $\boldsymbol{y}'_2 \in (\mathbb{F}_{q^2})^{n_2}$ with $(x', \boldsymbol{y}'_1, \boldsymbol{y}'_2) \notin X$.

It seems so simple: $x \in \mathbb{F}_{q^2}$ is in $\mathbb{F}_q$ if and only if $\mathrm{Fr}_q(x) \stackrel{\text{def}}{=} x^q = x$.
How could it fail that some algebraic statement generalizing (1.6) would encapsulate this?

2 The Main Theorem of Galois Stratification

The main theorem inductively, §2.1, eliminates quantifiers for problems that

start as elementary statements interpretable over *any* extension of a residue class field of the ring of integers of a number field K. (2.1)

First we give the appropriate Main Theorem version that allows the elimination. This includes all possible statements that might have answered Felgner's question in the affirmative. To simpify discussing the procedure, take as fundamental the following problem.

Is a statement true for *almost all* residue class fields $\mathbb{Z}/p = \mathbb{F}_p$ (that is, $R = \mathbb{Z}$ in (1.5)).

Given the elementary statement start of (2.1), we expediently consider the *exceptional stratification* primes (Def. 2.2) not included in the phrase "almost all."[2] That thereby allows the procedure to consider if a statement holds for *all* primes or variants of that question.

The philosophical differences between [FrS76] and [FrJ04] are small, though there are more details in the latter. That is primed to handle – *Frobenius field* – results more general than the finite field case. It shows there is a *general Galois stratification* idea. Then, you adjust by using an **NRC** replacement for each collection of (so-called) Frobenius fields.

This approach produces the finite field case by observing, if q is large, then the collection of finite fields behaves like a collection of Frobenius fields.[3] We don't redo that. Rather we show a path through [FrJ04, Chap. 30] in §2.2 – with an example – that works.

2.1 Galois stratification and elimination of quantifiers

The starting field for the diophantine statement D here is either $\mathbb{Q}$ (or some fixed field K containing $\mathbb{Q}$) or a finite field $\mathbb{F}_q$ (usually $\mathbb{F}_p$). To simplify we assume that we start either with $\mathbb{Q}$ (or with coefficients in $\mathbb{Z}$) or with $\mathbb{F}_p$. Here is the procedure abstractly, starting with the definition of Galois stratification.

In the rest of this subsection our goal is consider residue class fields. Then, §2.2 generalizes, as done in [FrJ04], but with different emphasis, how that gives objects over $\mathbb{Q}$.

2 The word *exceptional* has two, incompatible uses in this paper, forced on us by the historical record. I have put the word *stratification* in this one to separate them.
3 That's no surprise since that was in the original motivations for [FrJ04].

(2.2a) There exists a stratification $\mathcal{S}_k$ (a disjoint union of normal algebraic sets)

$$\dot\cup_{j=1}^{l_k} X_{j,k}, \text{ covering } \mathbb{A}^{m+N_k}.$$

(2.2b) For each (j,k), $1 \le j \le \ell_k$, there is a Galois (normal) cover $\hat\varphi_{j,k} : \hat Y_{j,k} \to X_{j,k}$[4] with group $G_{j,k}$ and a collection, $\mathbf{C}_{j,k}$, of conjugacy classes of $G_{j,k}$.[5]

(2.2c) Then, in place of $(x', \boldsymbol{y}'_1, \boldsymbol{y}'_2) \in$ (or $\notin$)$X(\mathbb{F}_q)$ we ask this. For $(\boldsymbol{x}', \boldsymbol{y}'_1, \ldots, \boldsymbol{y}'_k) \in \mathcal{S}_k(\mathbb{F}_q)$,

if $(\boldsymbol{x}', \boldsymbol{y}'_1, \ldots, \boldsymbol{y}'_k) \in X_{j,k}$, then the Frobenius, $\mathrm{Fr}_{\boldsymbol{x}', \boldsymbol{y}'_1, \ldots, \boldsymbol{y}'_k} \in G_{j,k}$ at the point, is in $\mathbf{C}_{j,k}$.

Ambiguity in the coefficients of equations: In [FrJ04] the covers are always taken to be unramified, but the essential is whether having the Frobenius in the conjugacy classes is unambiguous. We have purposely left ambiguous the coefficients of the equations defining the ingredients of (2.2a) and (2.2b). Indeed, the procedure works like this.

(2.3a) $\mathrm{G}_{\mathrm{aap}}$: The original statement is over $\mathbb{Q}$ (or even over $\mathbb{Z}$), but we don't care, for finitely many p, if it is not true or even for (2.2c) applicable.

(2.3b) $\mathrm{G}_{\mathrm{allp}}$: The original statement is over $\mathbb{Z}$, meaningful for each prime p and we have the option of deciding if, after finding it true for a. a. p, whether it is true for all p.

Definition 2.1. For each Galois cover $\hat\varphi : \hat Y \to X$ in a Galois stratification $\mathcal{S}$, we need an affine space description of the underlying spaces, and of the group of the cover. Running over all possible (j,k) we refer to this collection as the *characteristics* of $\mathcal{S}$.

It is easiest to describe the characteristics when the spaces are described as explicit open subsets of affine hypersurfaces, as they are in [FrJ04]. There are two possible situations where we might apply the stratification procedure assuming our initial goal is to decide if we can interpret it over $\mathbb{F}_p$ by reduction mod p, and then if it is true for almost all p.

These situations are compatible with Main Theorem (2.4). It uses coefficients initially over $\mathbb{Q}$, producing a finite set, M_{k-1}, of primes for which (2.4) holds.

(2.4a) Either the resulting (over) $\mathbb{Q}$ equations don't make sense of (2.2c); or the fibers of the underlying stratification pieces are not flat over $\mathrm{Spec}(\mathbb{Z}_p)$; or

(2.4b) the Chebotarev estimates of (2.11) for some q divisible by p don't assure hitting all appropriate conjugacy classes.

The *flatness statement* means that reduction mod p preserves the characteristics of the stratification. In applying Denef-Löeser §3.3, what we call the characteristics is strengthened, but the idea is the same.

---

4 By putting a ˆ over φ we are reminding that this is a Galois cover with automorphisms defined over the field of definition of the cover.

5 For the problems in this paper it suffices to take *Frobenius classes*. Each is a union of conjugacy classes of $G_{j,k}$ where if g is in one of these, then so is g^u if $(u, \mathrm{ord}(g)) = 1$.

Definition 2.2. In the ith step of the induction procedure, refer to the respective primes, the *exceptional stratification primes* of (2.4), as $M_{i,a}$ and $M_{i,b}$, $i = k-1, \dots, 0$, and their union by M_i. We include in M_i the primes from M_{i+1}. So $M_0 \supset M_1 \supset \cdots \supset M_{k-1}$.

It is for the strong Poincaré series result of Thm. 3.1 that we have divided these considerations of primes. Following the stratification procedure format in Thm. 2.4, §2.3 gets into these significant issues: Reduction mod p; and the non-regular Chebotarev analog.

The extra point, not discussed in [FrJ04, Chap. 31], is how the diophantine illuminating properties of the Poincaré series in Thm. 3.1 vary as a function of $p \notin M_i$. Especially, how they depend on the non-regular analog as illustrated by the §3.3.1 example.

Inductive stratification notation: Below some additional notation replaces k by the index i. For example, we replace N_k by $N_i = \sum_{j=1}^{i} n_j$. Assume the problem has one quantifier for each block of variables. Our original example, illustrating a possible answer in §1.2 for Felgner, used two quantifiers.

Galois stratification allows eliminating one quantified block of variables, at a time, using a general, enhanced, *Non-regular Chebotarev Density Theorem*. §2.3 explains how that contributes to Main Theorem (2.4) by which the elimination inductively forms a sequence of Galois stratifications: $\mathcal{S}_k, \dots \mathcal{S}_0$, with triples $(X_{\bullet,u}, G_{\bullet,u}, \mathbf{C}_{\bullet,u})$, $u = k, \dots, 0$.

For each u, the $\bullet$ indicates a sequence for $1 \le j \le \ell_u$ of underlying spaces in the stratification that satisfy the following properties.

As in (2.2b), saying $\mathrm{Fr}_{\boldsymbol{x}',\boldsymbol{y}'_1,\dots,\boldsymbol{y}'_i} \in \mathbf{C}_{\bullet,i}$ means that if the subscript point is in $X_{j,i}$, then $\mathrm{Fr}_{\boldsymbol{x}',\boldsymbol{y}'_1,\dots,\boldsymbol{y}'_i}$ refers to the conjugacy class value in the Galois cover $\hat{C}_{j,i} \to X_{j,i}$.

The variables $\boldsymbol{x}$ of the Galois stratification $(X_{\bullet,0}, G_{\bullet,0}, \mathbf{C}_{\bullet,0})$ of $\mathbb{A}^m$ are unquantified. For the ith stratification $\mathcal{S}_i$, the quantifiers are $Q_1, \dots, Q_i$; we suppress their notation.

Definition 2.3. For $\boldsymbol{x}' \in \mathbb{F}_q^m$, we say $\mathcal{S}_i(\boldsymbol{x}'; q)$ holds

$$\text{if } \mathrm{Fr}_{\boldsymbol{x}',\boldsymbol{y}'_1,\dots,\boldsymbol{y}'_i} \in \mathbf{C}_{\bullet,i} \text{ for } Q_1\boldsymbol{y}'_1 \cdots Q_i\boldsymbol{y}'_i \in \mathbb{A}(\mathbb{F}_q)^{N_i}. \tag{2.5}$$

A relative version concentrates at the ith position. For $\boldsymbol{x}', \boldsymbol{y}'_1, \dots, \boldsymbol{y}'_{i-1} \in \mathbb{F}_q^{m+N_{i-1}}$

$$\text{we say } \mathcal{S}_i(\boldsymbol{x}', \boldsymbol{y}'_1, \dots, \boldsymbol{y}'_{i-1}; q) \text{ holds if } \mathrm{Fr}_{\boldsymbol{x}',\boldsymbol{y}'_1,\dots,\boldsymbol{y}'_i} \in \mathbf{C}_{\bullet,i} \text{ for } Q_i\boldsymbol{y}'_i \in \mathbb{A}(\mathbb{F}_q)^{n_i}. \tag{2.6}$$

The notation $\bar{\mathcal{S}}_p \stackrel{\text{def}}{=} \{\mathcal{S}_{p,k}, \dots, \mathcal{S}_{p,0}\}$ from (1.4), for a sequence of Galois stratifications – with its attendent sequence of exceptional stratification primes $M_k \dots, M_0$ – appears at the end of the Thm. 2.4 statement. Also, Thm. 2.4 refers to the Frobenius in a finite Galois extension $\hat{K}/\mathbb{Q}$, and the Frobenius (conjugacy class), Fr_p attached to a prime p in this extension.

Theorem 2.4 (Main Theorem [FrS76])**.** *Assume quantifiers $Q_1, \dots, Q_k$ and, $\mathcal{S}_{k,p}$, an initial Galois stratification over $\mathbb{Q}$, in situation* (2.3a)*. Then, we may effectively form a stratification sequence $\bar{\mathcal{S}}_p$, as above, for each $p \notin M_0$ with the following properties.*

(2.7a) *Local property: Given $\boldsymbol{x}', \boldsymbol{y}'_1, \dots, \boldsymbol{y}'_{i-1} \in \mathbb{F}_p^{m+N_{i-1}}$, $\mathrm{Fr}_{\boldsymbol{x}',\boldsymbol{y}'_1,\dots,\boldsymbol{y}_{i-1}} \in \mathbf{C}_{\bullet,i-1}$ if and only if $\mathcal{S}_i(\boldsymbol{x}', \boldsymbol{y}'_1, \dots, \boldsymbol{y}'_{i-1}; p)$ holds.*

(2.7b) *Inductive Result: $\boldsymbol{x}' \in \mathbb{F}_p^m$, then $\mathrm{Fr}_{\boldsymbol{x}'} \in \mathbf{C}_0$ if and only if $S_k(\boldsymbol{x}', p)$ holds.*

Further, there is a finite Galois extension $\hat{K}/\mathbb{Q}$ with group $G \stackrel{\text{def}}{=} G_{\mathcal{S}_k}$ and a finite collection of stratification sequences ${}_j\bar{\mathcal{S}}, j = 1, \dots, \mu$, over $\hat{K}_p$ (see §2.2) with this property. For each $p \notin M_0$, $\bar{\mathcal{S}}_p$ is the reduction of ${}_j\bar{\mathcal{S}}$ mod p for some j depending only on Fr_p *in G.*

Remark 2.5. The last paragraph in Thm. 2.4 is there to compare the stratification procedure for a given p to a process that works uniformly in p. We are giving several approaches: the Frobenius field approach (§2.2); the finite field approach, and sometimes just deciding the truth of a diophantine statement for p. Still, all of them – including the ultimate count, as in the abstract, in the Poincaré series – depend on locating absolutely irreducible varieties related to the stratification procedure.

Remark 2.6 (Extend Thm. 2.4). For a given p, we may replace the quantification of the variables in $\mathbb{F}_p$ by quantification of its variables in $\mathbb{F}_q$ with q any power of p. Again, the correct ${}_j\bar{\mathcal{S}}$ depends only on $\mathrm{Fr}_q \in G$. See Rem. 2.7 for the adjustment that applies to considering powers of q divisible by $p \in M_0$.

Remark 2.7. Notation of Def. 2.2 gives a procedure starting with the subscript $i = k$, ending with $i = 0$. Even, however, for primes in M_0 under hypothesis $\mathrm{G}_{\mathrm{allp}}$ (2.3b). the equation coefficients are in $\mathbb{F}_p$. We may then perform the stratification procedure. That allows deciding for each such p if the statement is true over $\mathbb{F}_q$ for *almost all* powers q of p, so long as q is large enough for the Chebotarev conditions to hold. This extends Rem. 2.6. We cannot, however, expect the stratification to come from an object over $\mathbb{Q}$ (by reduction mod p) or to be related in any obvious way to one of the stratifications ${}_j\bar{\mathcal{S}}$ given in Thm. 2.4.

2.2 The General Stratification procedure

The qualitative point of the **NRC** is this.

$$\text{To know, for a Galois cover } \hat{\varphi} : \hat{Y} \to X \text{ over a finite field, what conjugacy classes (or cyclic subgroups) generate decomposition groups running over } \boldsymbol{x} \in X(\mathbb{F}_q). \tag{2.8}$$

§2.3 shows the role of the Chebotarev Theorem in Thm. 2.4. Especially that it gives a rough count of the $\boldsymbol{x}' \in \mathbb{F}_q^m$ for which $\mathcal{S}_k(\boldsymbol{x}', q)$ holds. This section gives outlines how [FrJ04, Chaps. 30-31] gives Thm. 2.4. We trace the general form of the stratification procedure.

Definition 2.8. A profinite group G has the *embedding property* if given covers[6] of groups $\psi_{G,A} : G \to A$ and $\psi_{B,A} : B \to A$, for which B *is a quotient of* G, then

$$\text{there is a cover } \psi_{G,B} : G \to B \text{ with } \psi_{G,A} \circ \psi_{G,B} = \psi_{G,A}.$$

The name *superprojective* is thus apt for a group that is projective – in the category of profinite groups – with the embedding property.

6 By a cover $\psi : H \to G$ of groups we mean an onto homomorphism.

That is, the embedding property is just projectivity with the extra condition that $\psi_{G,B}$ is a cover, given the necessary condition on B. This definition starts the analogy between finite fields and the very large class of Frobenius fields – again a reason for the existence of [FrJ04] – and whereby progress was achieved using Galois stratification [FrHJ84].

[FrJ04, §24.1] develops the theory of *Frobenius fields* M:

(2.9a) M is a **PAC** field (all absolutely irreducible varieties over M have M points), and;
(2.9b) its absolute galois group, G_M, has the embedding property.

If M is Frobenius, then G_M is *superprojective* [FrJ04, Prop. 24.1.5].

The point of Frobenius fields: [FrJ04, Prop. 24.1.4] is the replacement for Frobenius fields of the Chebotarev analog. This is applied to the Galois covers $\hat{\varphi} : \hat{Y} \to X$ with group $G_{\hat{\varphi}}$ that appear in a Galois stratification. This assumes $\hat{Y}$ is absolutely irreducible. Equivalently, $\hat{\varphi}$ is a *regular* cover, over M.

The conclusion of this Chebotarev analog is that we know precisely what *decomposition groups* – among the $H \le G_{\hat{\varphi}}$– that $\hat{\varphi}$ has over fibers of $X(M)$. They are:

All subgroups H that are quotients of the absolute Galois group G_M.

The remainder of Chap. 30 through §30.5 is details of the Galois stratification procedure applied to the theory of *all* Frobenius fields containing a fixed given field [FrJ04, Thm. 30.6.1]. For simplicity assume we start over $\mathbb{Q}$. Much of what looks technical is the pairing of decomposition groups of a cover $\hat{\varphi}_i$ of $\mathcal{S}_i$ with the decompositions groups that extend these to a given cover $\hat{\varphi}_{i+1}$ of $\mathcal{S}_{i+1}$ above $\hat{\varphi}_i$.

For example, [FrJ04, conditions (2) of Lem. 30.2.1] has this situation: $n_{i+1} = 1$ and $\boldsymbol{y}_{i+1} = y_{i+1}$. We continue Ex. 2.9 in §3.3.1. Again, M is notation for a Frobenius field.

Example 2.9 (Pairing two covers)**.** Suppose X_2 is a hypersurface in $\mathbb{A}^{m+1}$ defined by the equation $\{(\boldsymbol{x}, y) \mid f(\boldsymbol{x}, y) = 0\}$ covered by $\hat{\varphi}_2 : \hat{C}_2 \to X_2$. Also, that $\text{proj}_{\boldsymbol{x}} : \mathbb{A}^{m+1} \to \mathbb{A}^m$ restricted to X_2 is generically onto. So, it is a cover – not likely Galois in a practical case – over an open set in the image. Assume f is absolutely irreducible of degree u in y.

Take a Zariski open set X_1 in $\mathbb{A}^m$ and a Galois cover $\hat{\varphi}_1 : \hat{C}_1 \to X_1$ having an open map $\varphi : \hat{C}_1 \to \hat{C}_2 \to X_2$ factoring through X_1. To satisfy other constraints in [FrJ04], like being unramified, it may not be surjective to X_2. Note: $G_{\hat{\varphi}_1}$ has a natural degree u permutation representation $T : G_{\hat{\varphi}_1} \to S_u$ from its birational factorization through $\hat{\varphi}_2$.

The essence: Take for $\hat{\varphi}_1$ the minimal Galois closure of the cover $\text{proj}_{\boldsymbol{x}} \circ \hat{\varphi}_2$. Here is what we want from the elimination of quantifiers, if say y was quantified by $\exists$.

Given a Frobenius field M, consider subgroups $H_1 \le G_{\hat{\varphi}_1}$ that are decomposition groups for $\hat{\varphi}_1$ over some $\boldsymbol{x}' \in X_1(M)$ that also fix a point $(\boldsymbol{x}', y') \in X_2(M)$. That is, H_1 fixes a letter in the representation T, so it restricts to a decomposition group H_2' of $\hat{\varphi}_2$. Then, consider $\mathcal{H}$, the conjugacy classes of groups $H_2 \le G_{\hat{\varphi}_2}$ in Galois stratification data already attached to this cover in the Frobenius field case.

How to decide – for eliminating the quantifier $\exists$ – if H_1 will be in the conjugacy classes attached to the cover $\hat{\varphi}_1$? It is, if the H_2' described above corresponding to H_1, is in $\mathcal{H}$.

Remark 2.10 (Finding H_1 in Ex. 2.9). The last line on finding those H_1 s is what the Chebotarev analog quoted above does. In detail, you construct an absolutely irreducible variety for which an M point corresponds to such an H_1. Here I allude to Chebotarev's *field crossing argument* – which is all over [FrJ04] starting on p. 107 – and again in §2.3.1 and §3.3.1.

Continuing the stratification procedure: Reducing the general situation to Ex. 2.9 consists of many, conceptually easy, steps. A large collection of Frobenius fields satisfies the general theory of Frobenius fields containing any Hilbertian field K.

To compare with finite fields [FrJ04, §30.6] cuts things back from all Frobenius fields to much smaller collections of Frobenius fields. It does so by starting with $\mathcal{C}$ some *full formation* of finite groups. Then, it limits G_M to be in the pro-$\mathcal{C}$ groups,

Cutting down further, [FrJ04, p. 720] considers a fixed superprojective group U. It restricts to those M containing K with G_M in the collection of quotients of U. Finally, it goes to the case totally compatible with finite fields: U is the profinite completion of $\mathbb{Z}$.

Restricting the full theory of Frobenius fields containing K to these special cases is quite conceptual. The final realization is that in this last case the stratification procedure is done entirely over $\mathbb{Q}$. Now reduce the whole stratification apparatus mod p for most primes p. This amounts to dealing with covers, over $\mathbb{Q}$ (or later, $\mathbb{F}_q$) especially those that aren't regular.

Thm. 2.11 [Fr74, Lem. 1] handles this. For a Galois cover $\hat{\varphi}: \hat{Y} \to X$ (again take both X and $\hat{Y}$ to be normal) with X absolutely irreducible having group $\hat{G}$ [Fr74, Lem1].[7] The §3.3.1 example shows why this non-regularity, not easily eliminated, occurs. Take $\hat{\varphi}$ to be a K irreducible cover, K a number field, with ring of integers $\mathcal{O}_K$.

Assume $\hat{K}$ is the minimal field over which $\hat{\varphi}$ breaks into absolutely irreducible (Galois) covers of X. Take any component $\varphi': Y' \to X$. It will be Galois with group identified with $G' \stackrel{\text{def}}{=} \{g \in \hat{G} \mid g \text{ maps } Y' \to Y'\}$. The Galois extension $\hat{K}/K$ has group $\hat{G}/G'$. For $\boldsymbol{p}$ a prime of $\mathcal{O}_K$ unramified in $\hat{K}$, denote an element of the conjugacy class of the Frobenius of $\boldsymbol{p}$ by $\text{Fr}_{\boldsymbol{p}}$, and its fixed field (resp. residue class field) in $\hat{K}$ by $\hat{K}_{\boldsymbol{p}}$ (resp. $\mathbb{F}_{\boldsymbol{p}}$). Then, let $\hat{\varphi}_{\boldsymbol{p}}: \hat{Y}_{\boldsymbol{p}} \to X$ be the union of the conjugates of $\varphi': Y' \to X$ by $\text{Fr}_{\boldsymbol{p}}$.

Theorem 2.11. *Excluding a finite set B of computable primes $\boldsymbol{p}$ of $\mathcal{O}_K$, reduction of $\hat{\varphi}$ mod $\boldsymbol{p}$ has an $\mathbb{F}_{\boldsymbol{p}}$ Galois cover component isomorphic to $\hat{\varphi}_{\boldsymbol{p}}$ by the reduction map. Take the conjugacy classes, $\mathbf{C}_{\boldsymbol{p}}$ associated to $\hat{\varphi}_{\boldsymbol{p}}$ to be those from $\mathbf{C}$ whose restriction to $\hat{K}_{\boldsymbol{p}}$ act trivially.*

Remark 2.12. The classes $\mathbf{C}_{\boldsymbol{p}}$ that appear in Thm. 2.11 are precisely those that can be realized as Frobenius elements, as in Comment on (2.12b) in §2.3.2.

Remark 2.13 (Proofsheet changes, Edition 2 vs Edition 3 of [FrJ04]). We list the two that concern the topic of this paper. In both editions a key stratification lemma repeats on consecutive pages as Lem. 30.2.6 and Lem. 30.3.1 (including the material in the 2nd edition that starts at the bottom of p. 711). Also, the references on p. 760 in Edition 2 between [W.D.

7 This lemma does do the curve case, but the details necessary to generalize are the elimination results typical in commutative algebra.

Geyer and M. Jarden] and [W. Kimmerle, R. Lyons, R. Sanding and D.N. Teaque] are missing in Edition 2, but appear in Edition 3 on pgs. 766–771.

2.3 Choices and the Non-regular Chebotarev

From the view of deciding diophantine statements, [FrS76] is driven by actual diophantine applications, while [FrJ04] is stronger on logic's theories of fields. This paper returns to the first viewpoint: Galois stratification as enhancing understanding specific problems.

The variance of one diophantine problem with the prime p starts with using the Weil estimate systematically in §2.3.1, including finishing off Felgner in §2.3.3. Variance gets enhancement from attaching to the problems a Poincaré series, the topic of §3.

2.3.1 Choices in stratifying

Being courser – not stratifying excessively – on the formation of Galois stratifications allows staying closer to classical problemsand explicit computation. At that, the original paper [FrS76] and [FrJ04] are at opposite ends of the spectrum, despite the latter's details.

The former suggests restricting to flat covers when appropriate, involving blocks of variables of maximal length when possible. The latter takes blocks with just one variable and insists on unramified covers given by $\mathrm{Spec}(S) \to \mathrm{Spec}(R)$ with S generated, as a polynomial ring, over R, by a single element having no discriminant.[8] §2.2 outlined using the finer stratification procedure, as does this section which relies only on the original Weil estimate.

On the other hand, §3.3.1 gives our main example, a general situation that concludes with a Galois stratification containing just one cover, and by which we see painlessly infinitely many of the Poincaré series coefficients.

Now we show how the Chebotarev analog works, with a corollary to Main Theorem 2.4 that counts $\boldsymbol{x}' \in \mathbb{F}_q^m$ for which $S_k(\boldsymbol{x}', q)$ holds (for $q \notin M_0$). First, consider going from $\mathcal{S}_{i+1}$ to $\mathcal{S}_i$, dealing with the restriction of the stratification for $\mathcal{S}_{i+1}$ along the fibers of the

$$\text{natural projection } \mathbb{A}^{m+N_{i+1}} \xrightarrow{\mathrm{pr}_{i+1,i}} \mathbb{A}^{m+N_i}. \tag{2.10}$$

With ℓ_0 the number of elements in $\mathcal{S}_0$, and each $1 \le j \le \ell_0$ this gives the following [FrHJ94, Thm. p. 104]: [9]

(2.11a) an integer r_j between 0 and N_k and $\mu_j \in \mathbb{Q}^+$, a function of elements in $\mathbf{C}_{j,0}$;
(2.11b) giving the count, B_j, of $\boldsymbol{x}' \in \mathbb{A}^m$ with $\boldsymbol{x}' \in X_{j,0}$ and $\mathrm{Fr}_{\boldsymbol{x}'} \in \mathbf{C}_{j,0}$.

$$\text{Either: } (\dagger)\ B_j \text{ is } 0;\ \textit{or}\ (\dagger\dagger)\ |B_j - \mu_j q^{r_j}|/q^{r_j - 1/2} \text{ is bounded in } q.$$

8 This guarantees that a Frobenius element is a well-defined conjugacy class, without demanding extra conditions on $\mathbf{C}$. In, however, classical problem settings, using flexibility on $\mathbf{C}$ may be a good idea.
9 Qualitatively [Fr74, Prop. 2] sufficed for [FrS76], but there are more details in the unspecified constants, especially the dependency on the characteristics of the covers, in this reference.

These estimates [FrHJ94, §3, especially Lem. 3.1] are based on [LW54]. They are explicit, much better than *primitive recursive*, as in the application concluding [FrS76]. In [FrHJ94, Thm. 6.1, 6.3 et. al.], the main ingredients is this. Apply a Chebotarev Density Theorem version (as in [Fr74, Prop. 2]) to a pair consisting of the Galois cover $\hat{\varphi} : \hat{C} \to X$ to estimate the number of points $\boldsymbol{x}' \in X(\mathbb{F}_q)$ for which $\mathrm{Fr}_{\boldsymbol{x}'}$ is in the conjugacy classes $\mathbf{C}$ attached to $\hat{\varphi}$. Comments on (2.12a) show why, in the inductive procedure, we are producing new covers with new Galois closures and corresponding conjugacy classes.

Tesselating X with hyperplane sections – akin to [LW54] – and using Chebotarev's own field crossing argument, reverts this to Weil's Theorem on projective nonsingular curves over finite fields. [FrHJ94, §4] explicitly traces these classical results. Yet, it still has an error estimate. So, it doesn't imply the rational function Poincaré series results in §3.1 or §3.3.

2.3.2 Other Chebotarev Points

(2.12a) The actual quantifier elimination moving from $\mathcal{S}_{i+1}$ and $\mathcal{S}_i$ also uses (2.11). Indeed, that shows why there is no elimination of quantifiers through *elementary* statements.

(2.12b) Possibilities (†) and (††) in (2.11b) give very different error estimate contributions.

(2.12c) The distinctions in (2.12b) arise in a host of problems as illustrated in §3.3.1.

Comment on (2.12a): Consider restriction of one of the terms of the stratification of $\mathcal{S}_{i+1}$ to the fibers $\mathrm{pr}_{i+1,i}$ of the projection (2.10). Much of the [FrS76] proof assures the elimination theory allows applying (2.11), so as to pick out the conjugacy classes that will appear in each of the terms of the $\mathcal{S}_i$ stratification. §2.2 has that, though using Frobenius fields there avoided reference, at that point, to the Weil result.

So, for the quantifier $\exists$, the Chebotarev analog is essentially to assure that any conjugacy class that should occur in $\mathcal{S}_i$ actually does. Likewise, for $\forall$, that no conjugacy class that could change the result of the problem is excluded. Nevertheless, Chebotarev is giving error estimates, and not *precise* values that contribute to refined invariants as in §3.

Comment on (2.12b) **:** The distinction between (†) and (††) is consequent on the adjective *non-regular* analog of the Chebotarev (any dimensional base) version. Before [Fr74, §2] it had been traditional to make an unwarranted assumption. That is, when considering a cover $\varphi : C \to X$ – say of normal varieties – defined and absolutely irreducible, say, over a field K, that some kind of manipulation would allow assuming that the functorially defined Galois closure $\hat{\varphi} : \hat{C} \to X$ of the cover could also be taken over K.

That won't work in considering the possibilities, based on one Galois stratification, in varying q, even in residue classes of a number field. Here is why (eschewing cautious details). Suppose a component of the the Galois closure cover, $\hat{\varphi}$, has definition field $\hat{K} \neq K$ (with K a perfect field). Assume K is a number field with ring of integers $\mathcal{O}_K$.

Then, as we vary the residue class field $R_{\boldsymbol{p}} = \mathcal{O}_K/\boldsymbol{p}$, the corresponding Frobenius $\mathrm{Fr}_{\boldsymbol{x}'}$ for $\boldsymbol{x}' \in \mathbb{F}_q^m$ must restrict to the Frobenius $\mathrm{Fr}_{\boldsymbol{p}}$ on the residue class field $R_{\boldsymbol{p}}$. Suppose, for example, the order of $\mathrm{Fr}_{\boldsymbol{p}}$ does not divide the order of an element $g \in \mathbf{C}_{j,0}$.

Then, that conjugacy class of g cannot possibly be $\mathrm{Fr}_{\boldsymbol{x}'}$.[10] That, however, is the only obstruction by the general Chebotarev result – the meaning in (2.4b) of hitting the correct classes – for realizing an element of $\mathbf{C}_{j,0}$ as a Frobenius, so long as q is sufficiently large.

Comment on (2.12c)**:** The comment on (2.12b) alludes, for $R = \mathcal{O}_K$, to the (†) and (††) conditions varying with the residue class field $R_{\boldsymbol{p}} = \mathcal{O}_K/\boldsymbol{p}$ in actual problems. Further, the value of the Frobenius in an extension of $\hat{K}/K$ attached to the characteristic of $R_{\boldsymbol{p}}$ measured this. The analog is true for problems over a given finite field: The Frobenius in an extension $\hat{\mathbb{F}}_q$ attached to the problem measures the variance with changing the extension of $\mathbb{F}_q$. Both justify the significance, and resistence to elimination, of the word *non-regular* in the Chebotarev analog. §3.3.1 is an example that makes this explicit.

2.3.3 Main Theorem 2.4 implies "No!" to Felgner

Back to Felgner's Question with $m = 1$ and running over elements of $\mathbb{F}_{q^2}$ (not $\mathbb{F}_q$). Then, the elimination of quantifiers has reduced Felgner's question to this.

(2.13a) Show the following is impossible for q large:

$$\text{with } M_w = |x' \in X_{w,0}(\mathbb{F}_{q^2}) \text{ and } \mathrm{Fr}_{x'} \in \mathbf{C}_{w,0}|,\ M_{\mathcal{S}_0} \stackrel{\text{def}}{=} \sum_{w=1}^{\ell_0} M_w = |\mathbb{F}_q| = q.$$

(2.13b) Main Theorem 2.4 and (2.11) implies for each w, M_w is either bounded (in q) or asymptotic to $t_w q^2$ for some nonzero t_w.

(2.13c) Neither is a bounded distance from q. Therefore, no elementary formula distinguishes $\mathbb{F}_q$ within $\mathbb{F}_{q^2}$, so long as q is large. [FrHJ94, §0]

Indeed, the same argument shows there is no need to take $m = 1$. No matter what formula, no matter the number of variables included in $\boldsymbol{x}$, you can't get q as the number of $\boldsymbol{x}'$ counted by (2.13a), so long as q is large.[11] So we used quantitative counting to *exclude* the elements of $\mathbb{F}_q$ as a result. This was rather than finding a qualitative device that eliminated existence of a formula that precisely nailed $\mathbb{F}_q$ among the elements of $\mathbb{F}_{q^2}$.[12]

Is that satisfactory? It gets to the heart of the Poincaré series/zeta function approach, which primarily aims to count points satisfying equations.

---

10 That is, there is no error estimate for non-achievement of that class as a Frobenius, say by a bounding constant; it is just not achieved.

11 [FrHJ94] exists because the authors of [CLM92] insisted in their first version that Galois stratification couldn't handle Felgner's question. This despite others at their conference, including one of the authors of [DL98] – I was not – telling them that was wrong, much akin to the end of [FrS76].

12 That the count is bounded by a constant can't be excluded; see the *exceptional covers* of §3.3.

3 Diophantine invariants

[Fr05, §7.3] discusses the history of attaching a Poincaré series (and zeta function) to diophantine problems attached to Galois stratifications. We refer to some of its highlights. This section amounts pushs Chebotarev into the background; replacing it by with questions about precise point counts. §3.1 gives the Poincaré series definition.

§3.2 goes through the series' properties, especially Rationality Thm. 3.1. These estimates use *Dwork cohomology* and specific results of Bombieri applied to it.

§3.3.1 ties together all threads of this paper with one specific problem – having a vast practical literature – that uses the Poincaré series. Then, §3.3.2 briefly discusses the artistic extension – of Denef and Lóeser – from Galois stratification to *Chow Motive* coefficients. Thus, §3.3 is in the service of enhancing uniformity in p.

3.1 Poincaré series vs coefficient estimates

We have already seen that the Galois stratification procedure is not canonical. So, it makes sense to address whether there is a *homotopy theoretic* approach based on the category of Galois stratifications that clarifies a natural equivalence on stratification. That is what these Poincaré series test.[13]

(3.1) is the definition of the Poincaré series attached to the Galois stratification $\mathcal{S}_k$ over $\mathbb{F}_q$ with triples $(X_{\bullet,k}, G_{\bullet,k}, \mathbf{C}_{\bullet,k})$, and its quantifiers $Q_1, \dots, Q_k$. Main Theorem 2.4 replaces this by quantifying those points of the last stratification term whose Frobenius values are inside the requisite conjugacy classes. Though more complicated than counting points on a variety over a finite field, it is sufficiently akin to naturally extend classical methods.

The Poincaré series, in a variable t, for a given q attached to Galois Stratification $\mathcal{S}_k$ has this form with the coefficients $\mu(\mathcal{S}_k, q, m)$ explained below:

$$P(\mathcal{S}_k)_q(t) = \sum_{m=1}^{\infty} \mu(\mathcal{S}_k, q, m) t^m.^{14} \tag{3.1}$$

Those $\mu(\mathcal{S}_k, q, m)$ s do depend on the quantifiers $\boldsymbol{Q}$. If the Galois stratification was an ordinary elementary statement, then to simplify we would abuse the notation by placing them outside reference to the variables. We mean each quantifer Q_i, respectively, applies to the variables $\boldsymbol{y}_i$, $i = 1, \dots k$. For example: $\boldsymbol{Q}\,\boldsymbol{x}\,\boldsymbol{y}_1\,\boldsymbol{y}_2$ is $\boldsymbol{x}\,Q_1\boldsymbol{y}_1 Q_2\boldsymbol{y}_2$.

So, similar to this, when quantifying the placement of the Frobenius elements, denote the quantified version by $\boldsymbol{Q}\mathrm{Fr}_{\boldsymbol{x}',\boldsymbol{y}'_1,\dots,\boldsymbol{y}'_k} \in \mathbf{C}_{j,k}$

$$\text{running over } (\boldsymbol{x}', \boldsymbol{y}'_1, \dots, \boldsymbol{y}'_k) \in X_{j,k}(\mathbb{F}_{q^m})(\boldsymbol{x}', \boldsymbol{y}'_1, \dots, \boldsymbol{y}'_k), 1 \le j \le \ell_k. \tag{3.2}$$

13 Take *homotopy theoretic* to mean that an outcome expressable in terms of some kind of cohomology. One that equivalences among structures related to Galois stratification or variants that result in the same cohomology results. In a sense that is the point of motivic cohomology.

14 The notation of §4 shows why we didn't use the simpler notation $\mu(\mathcal{S}_k, q^m)$.

Then, the coefficient $\mu(\mathcal{S}_k, q, m)$ in (3.1) is the point count of those $\boldsymbol{x'} \in X_{j,k}(\mathbb{F}_{q^m})$ for which $\boldsymbol{Q}\mathrm{Fr}_{\boldsymbol{x'},\boldsymbol{y}'_1,\dots,\boldsymbol{y}'_k} \in \mathbf{C}_{j,k}$ constrained by running over the quantified y-variables, $\boldsymbol{y}'_1, \dots, \boldsymbol{y}'_k$, with values in $\mathbb{F}_q$. Main Theorem (2.4) allows replacing $\mu(\mathcal{S}_k, q, m)$ by $\mu(\mathcal{S}_0, q, m)$: counting (rather than estimating as in (2.11b)) those

$$\boldsymbol{x'} \in X_{j,0}(\mathbb{F}_{q^m}) \text{ for which } \mathrm{Fr}_{\boldsymbol{x'}} \in \mathbf{C}_{j,0}, 1 \le j \le \ell_0. \tag{3.3}$$

3.2 Poincaré properties

[FrJ04, Chap. 30 and 31] (Chaps. 25 and 26 in the 1986 edition, pretty much the same) have complete details on the Poincaré and Zeta properties. A *Zeta function*, $Z(t)$, has an attached *Poincaré series* $\mathrm{P}(t)$. This is given by the logarithmic derivative:

$$t\frac{d}{dt}\log(Z(t)) = \mathrm{P}(t).$$

Add that $Z(0) = 1$, and each determines the other. The catch: $Z(t)$ rational (as a function of t) implies $\mathrm{P}(t)$ rational, but not always the converse.

Suppose D is an elementary diophantine statement, with quantifiers as we started this paper. Then, as earlier, take D in place of $\mathcal{S}_k$ in $P(\mathcal{S}_k)_q(t) = \sum_{m=1}^{\infty} \mu(\mathcal{S}_k, q, m)t^m$, and consider the coefficients referencing $(D, \boldsymbol{Q}, m)$ in place of $\mu(\mathcal{S}_k, q, m)$.

I don't know when Ax introduced considering such coefficients. He suggested to me meaningfully computing them at IAS in Spring '68. Originally, I introduced the Galois stratification procedure to do just that, and to conclude the following result. Again, suppress notation $\boldsymbol{Q}$ for the quantifiers and give the result explicitly just when $R = \mathbb{Z}$ in (1.5).

The adjustments are clear for when R is a given finite field, or ring of integers of a number field. Use the notation around Main Thm. 2.4.

Theorem 3.1 (Poincaré rationality)**.** *For each prime $p \notin M_0$, $P(\mathcal{S}_k)_p(t)$ is a rational function $\frac{n_p(t)}{d_p(t)}$, with $n_p, d_p \in \mathbb{Q}[t]$ and computable. The corresponding $Z(\mathcal{S}_k)_q(t)$ has the form $\exp(m^*_p(t))(\frac{n^*_p(t)}{d^*_p(t)})^{\frac{1}{u_p}}$ with $m^*_p, n^*_p, d^*_p \in \mathbb{Q}[t]$ and $u_p \in \mathbb{Z}^+$ computable. Further, there are bounds, independent of p, for the degrees of all those functions of t. For any particular prime p all functions are computable.*

Comments on the proof of Thm. 3.1: We start with highlights from [FrJ04, §31.3] (or 1986 edition, §26.3; essentially identical) titled: Near rationality of the Zeta function of a Galois formula. A similar result bounds the degrees even if $p \in M_0$, assuming (2.3b).

As, however, Rem. 2.7 notes, there won't be any expected relation with results for $p \notin M_0$. We cannot use the uniform estimate on the characteristics of the Galois stratification since they don't come from a reduction of a uniform stratification object as given in Thm. 2.11. Refer to the stratifications for $p \in M_0$ as *incidental*, with their incidential estimates. What we say here applies equally to uniform and incidental stratifications.

The conclusion of the Galois stratification procedure over the $\boldsymbol{x}$-space gives this computation for (3.3). Sum the number of $\boldsymbol{x}$ with values in $\mathbb{F}_{p^k}$ for which the Frobenius falls in conjugacy classes attached to the stratification piece going through $\boldsymbol{x}$.

The expression of that sum in *Dwork cohomology* is what makes the effectiveness statement in the Thm. 3.1 possible. That also suggests its direct relation to Denef-Loeser. An ingredient for that is a formula of E. Artin. It computes any function on a group G that is constant on conjugacy classes as a $\mathbb{Q}$ linear combination of characters induced from the identity on cyclic subgroups of G.

Additional historical comments: A function on G that is 1 on a union of conjugacy classes, 0 off those conjugacy classes, is an example. [FrJ04, p. 738-739] (1986 edition p. 432-433) recognizes L-series attached to that function as a sum of L-series attached to those special induced characters. I learned this from [CaF67, p. 222] and had already used it in [Fr74, §2]. Kiefe – working with Ax – learned it, as she used it in [Ki76], from me as a student during my graduate course in Algebraic Number Theory at Stony Brook in 1971. The core of the course were notes from Brumer's Fall 1965 course at UM.[15]

Kiefe, however, applied it to a list-all-Gödel-numbered-proof procedure; not to Galois stratifications I showed her (see my Math Review of her paper, Nov. 1977, p. 1454). Consider the identity representation induced from a cyclic subgroup $\langle g \rangle, g \in G$. This L-Series is the zeta function for the quotient cover by $\langle g \rangle$ (exp. 7-9, p. 433, 1986 edition of [FrJ04]).

We do use a zeta function: Given a rational function in t, its *total degree* is the sum of the numerator and denominator degrees; assuming those two are relatively prime. The 1986 edition, Lem. 26.13 refers to combining [Dw66] and [Bo78] to do the zeta function of the affine hypersurface case for explicit bounds – dependent only on the degree of the hypersurface – on the total degree of the rational functions that give these zeta functions.

Then, some devissage gets back to our case, given explicit computations dependent only on the degrees of the functions defining these algebraic sets. Lem. 26.14 assures the stated polynomials in t have coefficients in $\mathbb{Q}$, and it explicitly bounds their degrees. The trick is to take the logarithmic derivative of the rational function. Then, the Poincaré series coefficients are power sums of the zeta-numerator zeros minus those of the zeta-denominator zeros. Using allowable normalizations, once you've gone up to the coefficients of the total degree, you have determined the appropriate numerator and denominator of $\mathrm{P}(t)$.

One observation is left to uniformly bound in p the degrees of the zeta polynomials, etc. This follows from the comments above Thm. 2.11 giving the uniformity in p in the characteristics of the reduction of the stratification. Apply this to the degrees of polynomials describing the affine covers for Dwork-Bombieri.

3.3 Chow Motive Coefficients

As stated in §2.3.1, the error estimate that allowed the elimination of quantifiers isn't appropriate for concluding either the estimate of the degrees of the polynomials in the Poincaré series, or that it is a rational function.

15 I submitted my paper in 1971. It had five different referees.

It is sensible to use as coefficients of the Poincaré series actual Galois stratifications. For $p \notin M_0$ those coefficients sum over the Galois covers $\hat{\varphi} : \hat{Y} \to X$ in the stratification $\mathcal{S}_0$ those $\boldsymbol{x}' \in X(\mathbb{F}_q)$ for which $\mathrm{Fr}_{\boldsymbol{x}'} \in \mathbf{C}$. It also works to replace the count on the stratification pieces with absolutely irreducible algebraic varieties that give the same counts. This uses the field crossing argument mentioned several times previously, as in Rem. 2.10.

The topic here is enhancing the Poincaré series coefficients, extending them to *Chow motive coefficients*; the last of the coefficient choices given in the abstract. After the example of §3.3.1, §3.3.2 briefly discusses the abstract setup of [DL02] and [Ni07]. These have their own expositions on Galois Stratification. Further discussion of these will occur in the extended version of this paper.

3.3.1 Distinguishing special primes

We mean to produce an example where the associated Poincaré series over $\mathbb{F}_q$ has some coefficients that are *polynomials* in q, and others where something very different happens. [Fr05, §3] takes a general diophantine property and casts it as an umbrella over two seemingly distinct diophantine properties about general covers.

These properties fit a *birational* rubric, or what we call *monodromy precision*. That is, the Galois closure of the covers alone, together with the corresponding permutation representations attached to their geometric and arithmetic monodromy, guaranties, precisely, their defining diophantine property. The **NRC** – as always – gives the count of achieved conjugacy classes *roughly*. Here, though, there will be no error term – unlike the Comment on (2.12b) in §2.3.2 – even though there is achievement of nontrivial conjugacy classes.

That allows stating, should we start with such a cover over a number field K, what are the primes for which the diophantine property has a precise formulation over a given residue class field $\mathcal{O}_K/\boldsymbol{p} = \mathbb{F}_{\boldsymbol{p}}$, as in [Fr05, Def. 3.5 and Cor. 3.6]. Our example uses the simplest case: the *exceptional cover* property.

For this, in Ex. 2.9, take the following special case over K. The hypersurface in $\mathbb{A}^{m+1}$ is still defined by an equation $X_2 = \{(\boldsymbol{x}, y) \mid f(\boldsymbol{x}, y) = 0\}$, with f absolutely irreducible (over K) of degree $u > 1$ in y. Now, though, the cover $\hat{\varphi}_2$ is trivial (of degree 1). As before consider $\mathrm{proj}_{\boldsymbol{x}} : \mathbb{A}^{m+1} \to \mathbb{A}^m$ restricted to X_2 and, these diophantine statements:

$$\begin{aligned} D_{\boldsymbol{p}}(\boldsymbol{x}) :& \quad \exists\, y \in \mathbb{F}_{\boldsymbol{p}} && \mid f(\boldsymbol{x}, y) = 0; \\ D_{\boldsymbol{p}} :& \quad \forall\, \boldsymbol{x} \in \mathbb{F}_{\boldsymbol{p}}^m\ \exists\, y \in \mathbb{F}_{\boldsymbol{p}} && \mid f(\boldsymbol{x}, y) = 0; \\ D :& \quad D_{\boldsymbol{p}} \text{ is true for } \infty\text{-ly many } \boldsymbol{p}. \end{aligned} \tag{3.4}$$

Continue with the Ex. 2.9 notation, and the formation of the Galois cover $\hat{\varphi}_1 : \hat{C}_1 \to X_1$ with X_1 Zariski open in $\mathbb{A}^m$, and with group $G_{\hat{\varphi}_1}$ having its natural and faithful, transitive, degree u permutation representation T. Consider the projective normalization, $\hat{C}_1^\dagger$, (resp. $X_2^\dagger$) of $\hat{\varphi}_1$ (resp. X_2) in the function field of $\hat{C}_1$ (resp. of X_2)

$$\hat{\varphi}_1^\dagger : \hat{C}_1^\dagger \to X_2^\dagger \to \mathbb{P}^m, \mathbb{P}^m \supset \mathbb{A}^m.[16]$$

16 $\hat{C}_1^\dagger$ is the projective normalization of $\mathbb{P}^m$ in the function field of $\hat{C}_1$; a canonical process.

Now extend the diophantine expressions of (3.4) to include $X_2^\dagger$. For example, $D_{\boldsymbol{p}}(\boldsymbol{x})$, for $\boldsymbol{x} \in \mathbb{P}^m(\mathbb{F}_q)$ means $\exists$ a point of $X_1^\dagger(\mathbb{F}_q)$ above $\boldsymbol{x}$. A similar meaning is given to $D_{\boldsymbol{p}}$.

We make a simplifying assumption to match up with §3.3.2.

$$\text{Not only is } X_2 \text{ normal, but } X_2^\dagger \text{ is nonsingular.} \tag{3.5}$$

Though the spaces are given by projective, not affine, coordinates, we form a single cover that we may regard as a Galois stratification $\mathcal{S}_0$, with one stratification piece: $\hat{\varphi}_1^\dagger : \hat{C}_1^\dagger \to \mathbb{P}^m$ with attached conjugacy classes

$$\mathbf{C}_1 = \{g \in G_{\hat{\varphi}_1} \mid T(g) \text{ fixes a letter in the representation}\}.$$

Proposition 3.2. *Assume* (3.5). *There is a finite set, M_0, of primes $\boldsymbol{p}$ of $\mathcal{O}_K$ for which, given $\boldsymbol{p} \notin M_0$, then $D_{\boldsymbol{p}}$ is true if and only the following equivalent conditions hold:*

(3.6a) $\mathrm{Fr}_{\boldsymbol{x}'} \in \mathbf{C}_1$ *for each $\boldsymbol{x}' \in \mathbb{P}^m(\mathbb{F}_{\boldsymbol{p}})$.*
(3.6b) *There are infinitely many $\boldsymbol{p}$ for which the equivalence of* (3.6a) *holds.*

Assume (3.6). *Then for some finite set $M_0' \supset M_0$, for each $\boldsymbol{p} \notin M_0'$ for which* (3.6a) *holds,*

$$\begin{gathered}\textit{if } \mathbb{F}_{\boldsymbol{p}} = \mathbb{F}_{q_0}, \text{ (3.6a) } \textit{holds with } \mathbb{F}_{q_0^m} \textit{ replacing } \mathbb{F}_{\boldsymbol{p}}. \textit{ Then, for } \infty\textit{-ly many } m, \\ \textit{the } m\textit{th coefficient of the Poincaré series } P(\mathcal{S}_0)_{\boldsymbol{p}}(t) \textit{ for } \mathcal{S}_0 \textit{ is } \tfrac{q_0^{m+1}-1}{q_0-1}.\end{gathered} \tag{3.7}$$

Definition 3.3 (Exceptional primes)**.** The primes $\boldsymbol{p}$ for which (3.7) holds are called the *exceptional primes*, $E_{\hat{\varphi}_1^\dagger}$, of $\hat{\varphi}_1^\dagger$ (or of any other object natural attached to it). The Main point is there are infinitely many of them, and their Poincaré series gives them away. Such a cover is called an *exceptional cover* over K.

Note, however, this is a case of a Galois closure of a regular cover that is *not* regular. What this says in (3.6b) is that only the elements of $\mathbf{C}_1$ are achieved as Frobenius elements for the primes satisfying the conditions (3.6).

[DaLe63] considered this hyperelliptic pencil with parameter λ: $y^2 - f(x) + \lambda$, $f \in \mathbb{F}_p(x)$. The difference between the expected number, p, of $\{(x,y) \in (\mathbb{Z}/p)^2\}$ and the actual value, $V_{p,\lambda}$, given by Weil's theorem caused them draw the following conclusion. There is a constant $c_f > 0$ such that:

$$\text{Running over } \lambda \in \mathbb{F}_p, \sum_{\lambda \in \mathbb{F}_p} (p - V_{p,\lambda})^2 > c_f p^2, \text{ if and only if } f \text{ is not exceptional.}$$

[Ka88] (recounted in [Fr05, §7]) used a generalization of the Davenport-Lewis error term to count the summed squares of the multiplicity of (completely reducible) components of the monodromy (fundamental group) action on the 1st complex cohomology of a fiber of any family of nonsingular curves over a base S. His technique – also coming upon the exceptionality condition – used reduction mod p to get to the results of [De74].

Remark 3.4. It has long been known that there are many exceptional covers. Between [Fr78, §2], [GMS03] and [Fr05, §6.1 and 6.2] those with $m = 1$ and $f(x,y) = f(y) - x$, f a rational function over a number field. The 1st and 3rd of these connect to Serre's Open Image Theorem. That paper also introduced natural zeta function test cases of the Langland's program. One problem is a standout. For the wide class of these related to the GL_2 case (and only these) of Serre's Open Image Theorem, the precise set $E_{\hat{\varphi}_1^\dagger}$ is a mystery appropriate for the nonabelian class field theory of the Langland's program [Fr05, §6.3].

3.3.2 Denef-Löser and Chow motives

The comments on Thm. 3.1 show we can express the coefficients in the Poincaré series from the trace of Frobenius iterates acting on the p-adic cohomology that underlies Dwork's zeta rationality result. Positive: The computation is effective. Negative: The cohomology underlying Dwork's construction varies with p. Nothing in 0 characteristic represents it.

Even, however, Dwork's cohomology [Dw60] deals with stratifying your original variety. By "combining" the different pieces you conclude the rationality of the zeta function from information on the Frobenius action from the hypersurface case.

Denef and Loeser [DL98] applied Galois stratification (see the arXiv version of [Ha07, App.]) to eliminate quantifiers in their p-adic problem goals. Their technique, as in [DL02], applies to consider – for almost all p – how to express those Poincaré series, as stated in the abstract to this paper, as elements in the Grothendieck group generated by ℓ-adic cohomology – twisted by Tate Modules; a tensoring of the group by some power of the cyclotomic character – of *nonsingular projective* varieties. Thus, the coefficients – as in the previous cases – derive from the trace applied to restricing powers of the Frobenius for p to these coefficients.

The word *motive* refers to the weighted pieces – rather than (pure) mth cohomology of a projective nonsingular variety – being a summand of this, tensored by a Tate twist. A correspondence – cohomologically idempotent – is attached to indicate the source of the projector that detaches a summand from the pure weighted cohomology.

They use Galois stratification, but relegate covers and conjugacy classes to the background. Yet, this artistic enhancement to the uniformity in p in the uniform stratification (Comments on the proof of Thm. 3.1) is still akin to the previous methods.

For one, from the main theorem of [De74], the absolute values of the eigenvalues of the Frobenius on these pieces are known. That allows more carefully considering any cancelation of these eigenvalues. For example, [De74, Thm. 8.1] gives a definitive result on the eigenvalues of a complete intersection of dimension n. The error term there is $O(q^{n/2})$ by contrast to the usual expection that an error term is $O(q^{n-1/2})$ as in (2.11).

The §3.3.1 example problem has a naturally attached projective nonsingular variety, $X_2^\dagger$ to express the Poincaré series coefficients for a Galois stratification $\mathcal{S}_0$ for (almost) all p, not just for those in the exceptional set. Even this example shows an aspect of using Denef-Löser that the previous two approaches don't seem to have:

Using (Chow) motive pieces to relate uniform stratification primes and incidental primes.

The archetype for such a consideration is the classically considered use of minimal models to describe appropriate Hasse-Weil zeta functions of elliptic curves, one that includes factors for the primes of bad reduction. I say this even though their stratification replacement uses resolution of singularities in 0 characteristic. That is, their method won't directly touch the primes of the incidental stratification.

For good reason, I should consider how my viewpoint can properly and practically tackle the motivic aspects; also what [Ni07] gains using Voevodsky's motives.

4 Generalizing Felgner to Frobenius Vector problems

Denote an algebraic closure of $\mathbb{F}_q$ by $\bar{\mathbb{F}}_q$. We regard such a generalization as considering whether there could be analogous results in quantifying our variables according to Def. 4.1.

Definition 4.1. For a given prime-power q, and $d_1, \ldots, d_m$ an m-tuple of integers, refer to $\mathrm{Fr}_q^{\boldsymbol{d}} \stackrel{\mathrm{def}}{=} (\mathrm{Fr}_q^{d_1}, \ldots, \mathrm{Fr}_q^{d_m})$ as a *Frobenius vector*. Then, $\mathrm{Fr}_q^{\boldsymbol{d}}$ acts on $\bar{\mathbb{F}}_q^m$ coordinate-wise, allowing us to speak of the elements $\boldsymbol{x} \in \bar{\mathbb{F}}_q^m$ fixed by a Frobenius vector. Denote these $\bar{\mathbb{F}}_q^m(\mathrm{Fr}_q^{\boldsymbol{d}})$.

Notice we may write the elements – in $\mathbb{F}_{p^2}$, referenced by Felgner's problem, as $\bar{\mathbb{F}}_q^m(\mathrm{Fr}_q^{\boldsymbol{d}})$ with $\boldsymbol{d} = (2, \cdots, 2)$. Frobenius vectors allow generalizing elementary statements (and Galois stratifications) to where variables have values in differing extensions of $\mathbb{F}_q$. With the notation above, consider two Frobenius vectors: $\mathrm{Fr}_q^{\boldsymbol{d}}$ of length m; and $\mathrm{Fr}_q^{\boldsymbol{e}}$ given by $\boldsymbol{e} = (\boldsymbol{e}_1, \ldots, \boldsymbol{e}_k)$ with $\boldsymbol{e}_i$ of length n_i. Thus, $\boldsymbol{e}$ has length $N_k = \sum_{i=1}^k n_i$.

Here are some basic questions.

(4.1a) Are the corresponding Poincaré series of Galois stratifications, with no quantified variables, rational?

(4.1b) Are there Bombieri-Dwork bounding degrees of the involved rational functions?

(4.1c) Does the Galois stratification procedure generalize to give rational functions? That is, given quantiers, can we eliminate them to be at (4.1a) with bounds from (4.1b)?

(4.1d) If the above, when are these Poincaré series new; not expressed from series associated to our previous Galois stratifications?

As with our last subsection, we are here brief, expecting to return to the subject later.

Wan's zeta functions: There are no Galois stratifications or quantified variables in [W03]. Just the definition of a zeta function defined by a Frobenius vector. That is coefficients defined from counting points $\boldsymbol{x} \in \bar{\mathbb{F}}_q^m(\mathrm{Fr}_q^{\boldsymbol{d}})$ as above, a la Dwork, on an affine variety in $\mathbb{A}^m$.

Here are its contributions to (4.1a). Following a preliminary result by Faltings, documented in [Wa01], [W03, Thm. 1.4] shows the zeta is a rational function.

Then it considers (4.1b) on the total degree of the zeta function akin to what Thm. 3.1 uses. There is a preliminary result for special Frobenius vectors with $d_1|d_2|\cdots|d_m$ (consecutive ds dividing the next in line) in [FuW03] based on Katz's explicit bound for ℓ-adic Betti numbers in [Ka01]. Then, [W03, Conj. 1.5] has a conjecture that there is an explicit total degree bound in general.

Logicians Hrushovski and Tomasovic: Both [H12] and [To16] deal with the theory of difference fields, and the generalization of Galois formulas (akin to [FrJ04]) over difference rings. Difference fields include the field $\bar{\mathbb{F}}_q$ together with the Frobenius automorphism. Both apply to (4.1c) on eliminations of quantifiers, though neither directly goes after the Poincaré series. The definitions and applications need more space than I can give them here, especially with (4.1a) still open. This exposition has aimed to show those are feasible questions.

I am most interested in contributing to the production of Poincaré series with those Chow motive coefficients that enhance what it means for these series to cohere as a function of p. Still, I recognize that this difference equation approach may apply to situations beyond our original finite field view of diophantine statements. Especially since Felgner's question offered so many peeks at attractive questions.

References

[Bo78] E. Bombieri, *On exponential sums in finite fields, II*, Inv. math. **47** (1978), 29–39.

[CaF67] J.W.S. Cassals and A. Frölich, *Algebraic Number Theory*, Acad. Press, London, 1967.

[CLM92] Z. Chatzidakis, L.v.d. Dries, A. Macintyre, *Definable sets over finite fields*, J. reine angew. Math. **427** (1992), 107–135.

[Ch36] C. Chevalley, *Demonstration d'une hypothèse de E. Artin*, Abhundlungen aus dem Mathematischen Seminar Hamburg, **11** (1936), 73–75.

[DaLe63] H. Davenport and D.J. Lewis, *Notes on Congruences (I)*, Quart. J. Math. Oxford (2) *14* (1963), 51–60.

[De74] P. Deligne, *La Conjecture de Weil I*, IHES Pub. Math. **43** (1974), 273–307.

[DL98] J. Denef and F. Loeser, *Motivic Igusa zeta functions*, J. Algebraic Geom. 7 (1998), no. 3, 505–537.

[DL02] ______ and ______, *Motivic integration and the Grothendieck group of pseudo-finite fields*, Proc. Int. Congress of Math, (ICM 2002) **2** (2002), 13Ð23.

[Dw60] B. Dwork, *On the rationality of the zeta function of an algebraic variety*, Amer. J. Math **82** (1960), 631–648.

[Dw66] ______, *On the zeta function of a hypersurface III*, Ann. of Math. **83** (1966), 457–519.

[Fe90] U. Felgner, *Posed at the Model Theory Conference in Oberwolfach*, January 1990.

[Fr74] M. D. Fried, *On Hilbert's Irreducibility Theorem*, J.of No. Th. **6** (1974), 211–231.

[Fr78] ______, *Galois groups and Complex Multiplication*, Trans. A.M.S. **235** (1978), 141–162.

[Fr05] ______, *The place of exceptional covers among all diophantine relations*, J. Finite Fields **11** (2005) 367–433, arXiv:0910.3331v1 [math.NT]

[Fr12] ______, *Variables separated equations: Strikingly different roles for the Branch Cycle Lemma and the Finite Simple Group Classification*, arXiv:1012.5297v5 [math.NT] (DOI 10.1007/s11425-011-4324-4). Sci. China Math., vol. **55** (2012) 1–72.

[FrS76] ______ and G. Sacerdote, *Solving diophantine problems over all residue class fields of a number field ...*, Annals Math. **104** (1976), 203–233.

[FrHJ84] ______, D. Haran and M. Jarden, *Galois stratification over Frobenius fields*, Advances in Math. **51** (1984), 1–35.

[FrHJ94] ______, ______, ______, *Effective counting of the points of Definable Sets over Finite Fields*, Israel J. of Math **85** (1994), 103–133.

[FrJ04] ______ and M. Jarden, *Field arithmetic*, Ergebnisse der Mathematik III, vol. **11**, Springer Verlag, Heidelberg, 1st Edition 1986 (455 pgs); 2nd Edition 2004 (780 pgs) ISBN 3-540- 22811-x. Our cites here are from the 2nd Edition, 1986 is similar.

[FuW03] L. Fu and D. Wan, *Total degree bounds for Artin L-functions and partial zeta functions*, Math. Res. Lett. **10** (2003) 33–41.

[GMS03] R. Guralnick P. Müller and J. Saxl, *The rational function analoque of a question of Schur and exceptionality of permutations representations*, Memoirs of the AMS **162** 773 (2003), ISBN 0065-9266.

[Ka88] N.M. Katz, *Local-to-global extensions of representations of fundamental groups*, Ann. Inst. Fourier **36**, No. 4 (1988), 69–106.

[Ka01] N. Katz, *Sums of Betti numbers in arbitrary characteristic*, Finite Fields & Appl. **7** (2001) 29–44.

[Ha07] T. Hales, *What is motivic measure?*, the version WhatIsMotivicMeasure.pdf arXiv0511276v2 with an appendix discussing Galois stratification.

[H12] E. Hrushovski, *The Elementary Theory of Frobenius Automorphisms*, July 24, 2012.

[Ki76] E. Kiefe, *Sets definable over finite fields, their zeta functions*, TAMS **223** (1976), 171–194.

[LW54] S. Lang and A. Weil, *Number of points of varieties in finite fields*, American Journal of Mathematics 76 (1954), 819Ð827.

[Ni07] J. Nicaise, *Relative Motives and the Theory of Pseudo-finite Fields*, Int. Math. Res. Papers, (2007), Article ID rpm001, 70 pages. doi:10.1093/imrp/rpm001.

[To16] I. Tomasic, *Twisted Galois Stratification*, Nagoya Math. J., **222** (1) (2016), 1–60 DOI 10.1017/nmj.2016.9

[Wa01] D. Wan, *Partial zeta functions of algebraic varieties over finite fields*, Finite Fields & Appl. **7** (2001) 238–251.

[W03] D. Wan, *Rationality of partial zeta functions*, Indag. Math. N.S., **14** (2) (2003), 285–292.