ISRAEL JOURNAL OF MATHEMATICS **85** (1994), 103–133

EFFECTIVE COUNTING OF THE POINTS OF DEFINABLE SETS OVER FINITE FIELDS*

BY

MICHAEL D. FRIED**

Department of Mathematics, University of California
Irivne, CA 92717 USA, e-mail: mfried@math.uci.edu

AND

DAN HARAN AND MOSHE JARDEN***

School of Mathematical Sciences
Raymond and Beverly Sackler Faculty of Exact Sciences Tel Aviv University
Ramat Aviv, Tel Aviv 69978, Israel
e-mail: haran@math.tau.ac.il and jarden@math.tau.ac.il

ABSTRACT

Given a formula in the language of fields we use Galois stratification to establish an effective algorithm to estimate the number of points over finite fields that satisfy the formula

Introduction

Chatzidakis, van den Dries and Macintyre [CDM] use model theoretic methods to generalize the Lang–Weil estimates for the number of rational points of a variety in a finite field:

---

* This work was partially done while all three authors were members of the Institute for Advanced Studies in Jerusalem.

** Parially supported by BSF grant #87-00038 and NSA grant MDA 904-91-H-0057.

*** Partially supported by grants from the German–Israeli Foundation for Scientific Research and Development.

Received May 24, 1990 and in revised form June 2, 1991

THEOREM: *Let $\varphi(\mathbf{X}, \mathbf{Y}) = \varphi(X_1, \ldots, X_m, Y_1, \ldots, Y_n)$ be a formula in the language of rings. There exists a finite sequence $\varphi_1(\mathbf{X}), \ldots, \varphi_k(\mathbf{X})$ of formulas in the language of rings, a positive constant C, positive rational numbers $\mu_1, \ldots, \mu_k$, and numbers $r_1, \ldots, r_k \in \{0, \ldots, n\}$, with the following property. For every finite field $\mathbb{F}_q$ and each $\mathbf{a} \in \mathbb{F}_q^m$ there exists a unique i, $1 \le i \le k$, such that $\mathbb{F}_q \models \varphi_i(\mathbf{a})$, and the number $N_q(\mathbf{a}) = |\{\mathbf{b} \in \mathbb{F}_q^n | \, \mathbb{F}_q \models \varphi(\mathbf{a}, \mathbf{b})\}|$ is either zero or it satisfies*

$$|N_q(\mathbf{a}) - \mu_i q^{r_i}| \le C q^{r_i - \frac{1}{2}}.$$

This work gives an algebraic proof of their result, which provides this estimate effectively. That is, it gives an algorithm to find the above formulas φ_i and the constants μ_i, r_i, and C explicitly.

The main tool we use is Galois Stratification [FJ]. This procedure eliminates quantifiers from formulas over certain types of fields (e.g., Frobenius fields and finite fields). Until now we have used this tool only to obtain results about sentences (formulas with no free variables). However, this method is so transparent that it immediately lends itself to a systematic treatment of results of the above type, although the *effective* computation of bounds is rather technical.

Another important ingredient in this work is the Non-regular Analog of the Chebotarev Density Theorem, which we prove in Section 5. This result generalizes [FS, Proposition 4.1].

0. Felgner's question

The following question of Ulrich Felgner at the Model Theory Conference in Oberwolfach in January 1990 motivated the main Theorem.

Is there a formula $\Phi(X)$ in the language of rings $\mathcal{L}$ that defines the field $\mathbb{F}_q$ in $\mathbb{F}_{q^2}$ for each prime power q?

Chatzidakis, van den Dries and Macintyre [CDM] observe that the Theorem implies that $\sqrt{q}$ can never be an asymptotic estimate for the number of points in $\mathbb{F}_q$ that satisfies a given formula. So, they answer Felgner's question negatively:

(*) No formula $\Phi(X)$ in $\mathcal{L}$ defines $\mathbb{F}_q$ in $\mathbb{F}_{q^2}$ for infinitely many prime powers q.

Galois Stratification as developed in [FJ], combined with the Chebotarev Density Theorem, is well suited to treat such questions. Here is a short proof of (*) based on [FJ]. (The concepts involved are reviewed in Section 1 below.)

Fix a formula $\Phi(X)$ in $\mathcal{L}$. We need the following notation. Let $\bar{t}$ be a transcendental element over $\mathbb{F}_q$, and let $E = \mathbb{F}_q(\bar{t})$.

(a) Identify the set P_1 of prime divisors of E of degree 1 with $\mathbb{F}_q \,\dot\cup\, \{\infty\}$; the prime divisor that corresponds to $a \in \mathbb{F}_q$ is given by $\bar{t} \mapsto a$.

(b) For a polynomial $g \in \mathbb{F}_q[X]$ denote $V(g) = \{a \in \mathbb{F}_q |\ g(a) = 0\}$.

(c) For a finite Galois extension F/E and a conjugacy class $\mathcal{C}$ of $\mathcal{G}(F/E)$ denote $C_1(F/E, \mathcal{C}) = \left\{\mathfrak{p} \in P_1 |\ \left(\frac{F/E}{\mathfrak{p}}\right) = \mathcal{C}\right\}$ [FJ, p. 59].

Claim: *There exist positive integers d, δ and q_0 with the following properties. For every $q \geq q_0$ there exists a Galois extension F/E of degree $\leq d$, distinct conjugacy classes $\mathcal{C}_1, \ldots, \mathcal{C}_e$ of $\mathcal{G}(F/E)$, where $e \geq 0$, and a polynomial $0 \neq g \in \mathbb{F}_q[X]$ of degree $\leq \delta$ such that*

$$\{a \in \mathbb{F}_q |\ \mathbb{F}_q \models \Phi(a)\} - V(g) = \bigcup_{j=1}^{e} C_1(F/E, \mathcal{C}_j) - (\{\infty\} \cup V(g)). \tag{1}$$

Assume that the Claim has been proved. By [FJ, Proposition 5.16, with $d = k = 1$] either $C_1(F/E, \mathcal{C}_j)$ is empty or

$$|C_1(F/E, \mathcal{C}_j)| \geq \frac{|\mathcal{C}_j|}{m} q - 4|\mathcal{C}_j| \cdot (1 + g_F + g_E + 1)\sqrt{q}. \tag{2}$$

Here m is some integer $\leq [F : E]$ [FJ, p. 59]. By [FJ, Corollary 4.8], $g_E = 0$ and $g_F \leq \frac{1}{2}(d-1)(d-2)$. Also, $1 \leq |\mathcal{C}_j| \leq d$. Hence, if (2) holds,

$$|C_1(F/E, \mathcal{C}_j)| \geq \frac{1}{d} q - 4d(2 + \frac{1}{2}(d-1)(d-2))\sqrt{q}.$$

Let $q \geq q_0$ and let $P(q) = \{a \in \mathbb{F}_q |\ \mathbb{F}_q \models \Phi(a)\}$. By (1) either $|P(q)| \leq \delta$ or

$$|P(q)| \geq \frac{q}{d} - 4d(2 + \frac{1}{2}(d-1)(d-2))\sqrt{q} - (\delta + 1).$$

If q is sufficiently large, then either $|P(q)| \leq \delta$ or $|P(q)|$ has more than $\frac{q}{d+1}$ elements. In particular $P(q^2) \neq \mathbb{F}_q$, for q large. Thus (*) follows from the Claim.

Proof of the Claim: We first prove the Claim for all q relatively prime to suitable $k \in \mathbb{Z}$. Then we show it for the powers of a fixed prime p. From these two cases the Claim follows.

As mentioned in [FJ, p. 425], $\Phi(X)$ is equivalent to a "Galois formula" over $R_0 = \mathbb{Z}[k^{-1}]$ for a suitable $k \in \mathbb{Z}$ (for all $\mathbb{F}_q$ with q prime to k). By [FJ, Proposition 26.8] we may assume that this formula is quantifier free, that is, it is of the form $\mathrm{Ar}(X) \subseteq \mathrm{Con}(\mathcal{B})$, where $\mathcal{B} = \langle \mathbb{A}^1,\ C_i/A_i,\ \mathrm{Con}(A_i) |\ i \in I\rangle$ is a Galois stratification of the affine line over R_0.

Since $\mathbb{A}^1 = \dot\bigcup_{i\in I} A_i$, exactly one of the A_i's, say A_1, is of dimension 1. Put $A = A_1$, $C = C_1$, and $R = R_0[A]$. Then $A = \mathbb{A}^1 - V(g)$ for some $g \in R_0[X]$, and hence $R = R_0[t, g(t)^{-1}]$, where t is transcendental over $\mathbb{Q}$. Furthermore, C has the form $R[z]$, where z is a primitive element for the cover C/A. Let $h(Z) = \mathrm{irr}(z, \mathbb{Q}(t))$; then $h(Z) \in R[Z]$.

Let q be prime to k and let $E = \mathbb{F}_q(\bar t)$. Extend the canonical homomorphism $R_0 \to \mathbb{F}_q$ to π: $R \to E$ by $t \mapsto \bar t$. Let $\bar z$ be a root of $\pi(h)$, put $F = E(\bar z)$, and extend π to ρ: $C \to F$ by $\rho(z) = \bar z$. Let ρ^*: $\mathcal{G}(F/E) \to \mathcal{G}(C/A)$ be the homomorphism induced by ρ [FJ, p. 137]. The set $\{\sigma \in \mathcal{G}(F/E) |\ \langle\rho^*(\sigma)\rangle \in \mathrm{Con}(A)\}$ is a union of conjugacy classes of elements in $\mathcal{G}(F/E)$. Write this union as $\mathcal{C}_1 \cup \cdots \cup \mathcal{C}_e$.

To verify (1), let $a \in \mathbb{F}_q$ such that $g(a) \neq 0$. Extend the canonical homomorphism $R_0 \to \mathbb{F}_q$ to a homomorphism φ: $R \to \mathbb{F}_q$ by $t \mapsto a$. Let $\bar\varphi$: $E \to \mathbb{F}_q \cup \infty$ be the $\mathbb{F}_q$-place defined by $\bar t \mapsto a$. Then $\varphi = \bar\varphi \circ \pi$. Extend $\bar\varphi$ to a place $\bar\psi$: $F \to \widetilde{\mathbb{F}}_q$, and let $\psi = \bar\psi \circ \rho$. Thus ψ extends φ. Now, a belongs to the left hand side of (1) if and only if $\mathrm{Ar}(C/A, \mathbb{F}_q, a) \subseteq \mathrm{Con}(A)$. The latter condition is equivalent to $\psi^*(G(\mathbb{F}_q)) \in \mathrm{Con}(A)$. But $\psi^* = \rho^* \circ \bar\psi^*$ and $G(\mathbb{F}_q)) = \langle \mathrm{Frob}(\mathbb{F}_q)\rangle$. Hence this can be written as $\bar\psi^*(\mathrm{Frob}(\mathbb{F}_q)) \in \bigcup \mathcal{C}_j$. This says that a belongs to the right hand side of (1).

Now fix a prime p, and let q be a power of p. By [FJ, Remark 25.8], $\Phi(X)$ is equivalent to a Galois formula over $R_0 = \mathbb{F}_p$. If q is large, [FJ, Proposition 26.8] shows that this formula is quantifier free. From this point on repeat the preceding arguments (replacing '$\mathbb{Q}$' by '$\mathbb{F}_p$', and 'q prime to k' by 'q large enough'). Notice that π and ρ are inclusions, and ρ^* is the restriction to C. ∎

1. Galois covers

The notion of a ring cover and the Artin symbol are the basic concepts of Galois stratification. For the convenience of the reader we redefine these concepts and state some of their basic properties.

Definition 1.1: Ring cover [FJ, Definition 5.4]. Let $R \subseteq S$ be integral domains, and let $E \subseteq F$ be their quotient fields. The extension S/R is a **ring cover** if R is integrally closed and there is $z \in S$ integral over R such that $S = R[z]$ and the discriminant $d_E(z)$ of z over E is a unit of R. We call such an element z a **primitive element** for S/R.

If F/E is a Galois extension, we say that S/R is a **Galois** ring cover. We sometimes write $\mathcal{G}(S/R)$ for the Galois group $\mathcal{G}(F/E)$.

If $R_0 \subseteq R$ and R_0 has quotient field K, we say that the ring cover S/R is **finitely generated** (resp., **regular**) over R_0 if R/R_0 is finitely generated (resp., E/K is regular). ∎

Remark 1.2: (i) The condition "$d_E(z)$ is a unit of R" in Definition 1.1 is equivalent to the following.

(1) There exists a monic polynomial $g \in R[X]$ such that $g(z) = 0$ and $g'(z) \in S^\times$.

Indeed, let $f = \mathrm{irr}(z, E) \in R[X]$. As $d_E(z) = \mathrm{Norm}_{F/E} f'(z)$, we have $d_E(z) \in R^\times$ if and only if $f'(z) \in S^\times$. Thus if $d_E(z)$ is a unit of R then (1) holds. Conversely, (1) implies that $g(X) = f(X)h(X)$ with $h \in R[X]$, and hence $g'(z) = f'(z)h(z)$. Thus if $g'(z) \in S^\times$, then also $f'(z) \in S^\times$.

(ii) Let S/R be a ring cover with primitive element z. Then $F = E(z)$ is a finite separable extension of E, and S is the integral closure of R in F [FJ, Lemma 5.3].

(iii) Let S/R be a (Galois) ring cover with primitive element z, and let $\bar{R}$ be an integrally closed integral domain. Any homomorphism $\varphi\colon R \to \bar{R}$ extends to a homomorphism ψ from S into the algebraic closure of the quotient field of $\bar{R}$ [L, Proposition 16 on p. 250]. Let $\bar{z} = \psi(z)$ and $\bar{S} = \bar{R}[\bar{z}]$. Then $\bar{S}/\bar{R}$ is also a (Galois) cover, with primitive element $\bar{z}$. Indeed, let E be the quotient field of R, let $f = \mathrm{irr}(z, E)$, and set $\bar{f} = \varphi(f) \in \bar{R}[Z]$. Then $\bar{f}(\bar{z}) = 0$ and $\bar{f}'(\bar{z}) = \psi(f'(z)) \in \psi(S^\times) \subseteq \bar{S}^\times$. By (i), $\bar{S}/\bar{R}$ is a cover. If S/R is Galois, then $\bar{S}/\bar{R}$ is Galois by Lemma 1.3(d) below. ∎

Let S/R be a Galois cover with primitive element z, and let F/E be the corresponding extension of the quotient fields. Let N/M be another Galois extension of fields and suppose $\psi\colon S \to N$ is a homomorphism such that $\psi(R) \subseteq M$. Let $\varphi\colon R \to M$ be the restriction of ψ to R.

LEMMA 1.3:

(a) *Let $\tau_1, \tau_2 \in \mathcal{G}(F/E)$. If $\tau_1 \neq \tau_2$ then $\psi(\tau_1(z)) \neq \psi(\tau_2(z))$.*

(b) *There exists a unique map $\psi^*\colon \mathcal{G}(N/M) \to \mathcal{G}(F/E)$ such that*

$$\psi(\psi^*(\sigma)(s)) = \sigma(\psi(s)), \qquad \text{for all } \sigma \in \mathcal{G}(N/M) \text{ and } s \in S. \tag{2}$$

(c) *ψ^* is a group homomorphism.*

(d) *$M(\psi(z))/M$ is a Galois extension.*

Proof of (a): We have

$$\prod_{\tau\neq\tau'}\big(\psi(\tau(z))-\psi(\tau'(z))\big)^2=\psi\Big(\prod_{\tau\neq\tau'}(\tau(z)-\tau'(z))^2\Big)=\psi(d_E(z))\in\psi(R^\times)\subseteq M^\times.$$

In particular, none of the factors on the left hand side is zero.

Proof of (b): Let $f(X)=\mathrm{irr}(z,E)$. Then $F=E(z)$, $f(X)\in R[X]$ and $f(X)=\prod_{\tau\in\mathcal{G}(F/E)}(X-\tau(z))$. Hence $\prod_\tau(X-\psi(\tau(z)))=\psi(f)\in M[X]$. Let $\sigma\in\mathcal{G}(N/M)$. Then $\sigma(\psi(z))$ is a root of $\psi(f)=\prod_\tau(X-\psi(\tau(z)))$. Hence, there is $\tau\in\mathcal{G}(F/E)$ such that $\psi(\tau(z))=\sigma(\psi(z))$. By (a) such a τ is unique; put $\psi^*(\sigma)=\tau$. As $S=R[z]$, (2) follows.

Proof of (c): This follows from the uniqueness in (b2).

Proof of (d): The polynomial $\psi(f)=\prod_\tau(X-\psi(\tau(z)))$ splits in $\psi(S)=\psi(R[z])\subseteq M(\psi(z))$. ∎

We notice that ψ^* depends not only on ψ and S but also on R and M as well.

Lemma 1.4: (a) *If ψ is an inclusion of rings, then ψ^* is the restriction to F.*

(b) *If $N=M(\psi(z))$, then ψ^* is injective.*

(c) *Let $\bar S/\bar R$ be another Galois cover, and let ρ: $S\to\bar S$ and $\bar\psi$: $\bar S\to N$ be homomorphisms such that $\rho(R)\subseteq\bar R$ and $\bar\psi(\bar R)\subseteq M$. If $\psi=\bar\psi\circ\rho$, then $\psi^*=\rho^*\circ\bar\psi^*$. In particular, if $R\subseteq\bar R$ and $S\subseteq\bar S$ and $\bar\psi$ extends ψ then $\psi^*=\mathrm{res}_F\bar\psi^*$.*

(d) *Let $\tau\in\mathcal{G}(F/E)$. Then $(\psi\circ\tau)^*(\sigma)=\tau^{-1}\psi^*(\sigma)\tau$ for all $\sigma\in\mathcal{G}(N/M)$.*

(e) *The map $\tau\mapsto\psi\circ\tau$ is a bijection between $\mathcal{G}(F/E)$ and the set of homomorphisms $S\to N$ that extend φ.*

(f) *Let $\sigma\in\mathcal{G}(N/M)$. Then $\{\psi'^*(\sigma)|\ \psi'\colon S\to N$ extends $\varphi\}$ is the conjugacy class of $\psi^*(\sigma)$ in $\mathcal{G}(F/E)$.*

Proof of (a), (b), (c) and (d): Immediate from the uniqueness of ψ^* (Lemma 1.3(b)).

Proof of (e): The map is injective by Lemma 1.3(a). It is surjective by [L, Corollary 1 on p. 247].

Proof of (f): Apply (d) to (e). ∎

Definition 1.5: In the above setup let M be a finite field, $N = \widetilde{M}$ its algebraic closure, and $\mathrm{Frob} \in G(M) = \mathcal{G}(\widetilde{M}/M)$ the Frobenius automorphism of M. The conjugacy class

$$\mathrm{ar}(S/R, \varphi) = \mathrm{ar}(S/R, M, \varphi) = \{\psi'^*(\mathrm{Frob}) |\ \psi' \colon S \to \widetilde{M} \text{ extends } \varphi\}$$

of elements in $\mathcal{G}(F/E)$ is called the **Artin symbol** of φ. The conjugacy class

$$\mathrm{Ar}(S/R, \varphi) = \mathrm{Ar}(S/R, M, \varphi) = \{\psi'^*(G(M)) |\ \psi' \colon S \to \widetilde{M} \text{ extends } \varphi\}$$

of subgroups in $\mathcal{G}(F/E)$ is called the **Artin symbol (of groups)** of φ.

Notice that $\mathrm{Ar}(S/R, \varphi) = \{\langle\tau\rangle |\ \tau \in \mathrm{ar}(S/R, \varphi)\}$. ∎

A set of elements (resp., subgroups) of a group G is called a **conjugacy domain** if it is closed under conjugation. Let $\mathrm{Con}_G(\Omega)$ denote the smallest conjugacy domain of elements (resp., subgroups) of G generated by Ω. The following property of the Artin symbol follows from Lemma 1.4(c).

LEMMA 1.6: *Let S/R and $\bar{S}/\bar{R}$ be Galois covers, and let $\bar{\varphi} \colon \bar{R} \to M$ be a homomorphism. Let $\pi \colon R \to \bar{R}$ be a homomorphism, and let $\rho \colon S \to \bar{S}$ be an extension of π. Then $\mathrm{ar}(S/R, \bar{\varphi} \circ \pi) = \mathrm{Con}_{\mathcal{G}(S/R)}\rho^*(\mathrm{ar}(\bar{S}/\bar{R}, \bar{\varphi}))$ and $\mathrm{Ar}(S/R, \bar{\varphi} \circ \pi) = \mathrm{Con}_{\mathcal{G}(S/R)}\rho^*(\mathrm{Ar}(\bar{S}/\bar{R}, \bar{\varphi}))$. In particular, if $R \subseteq \bar{R}$ and $S \subseteq \bar{S}$, and F is the quotient field of S, then $\mathrm{ar}(S/R, \bar{\varphi} \circ \pi) = \mathrm{Con}_{\mathcal{G}(S/R)}\mathrm{res}_F \mathrm{ar}(\bar{S}/\bar{R}, \bar{\varphi})$.*

2. Algebraic geometry

In this section we recall some basic definitions and concepts from algebraic geometry.

Let R_0 be an integral domain and K its quotient field.

Definition 2.1: (i) An R_0**-algebraic set** $V = V(f_1, \ldots, f_m)$ in $\mathbb{A}^n$ is the set of common zeros of polynomials $f_1, \ldots, f_m \in R_0[X_1, \ldots, X_n]$ in $\widetilde{K}^n$. We say that V is **given** if $f_1, \ldots, f_m$ are explicitly given.

(ii) An R_0**-constructible set** in $\mathbb{A}^n$ is a Boolean combination of R_0-algebraic sets. It is **given** if the latter sets are given.

(iii) An R_0-**basic set** is an R_0-constructible set of the form $A = V - V(g)$, where $V = V(f_1, \ldots, f_m)$ is an R_0-algebraic set *irreducible* over K and $g \in R_0[X_1, \ldots, X_n]$ is a polynomial not vanishing on V. ∎

We identify a "given" R_0-constructible set with the underlying polynomials that define it. Below we define some notions for such sets, which may actually depend on the underlying polynomials.

Definition 2.2: Let $A = V(f_1, \ldots, f_m) - V(g)$ be an R_0-constructible set. Suppose that $\varphi_0\colon R_0 \to R$ is a homomorphism into an integral domain R. Denote the R-constructible set $V(\varphi_0(f_1), \ldots, \varphi_0(f_m)) - V(\varphi_0(g))$ by A_R. (We abuse notation in omitting reference to φ_0.) If M is a field containing R, let

$$A(M) = \{\mathbf{a} \in M^n \mid \varphi_0(f_1)(\mathbf{a}) = \cdots = \varphi_0(f_m)(\mathbf{a}) = 0,\ \varphi_0(g)(\mathbf{a}) \neq 0\}. \qquad \blacksquare$$

Definition 2.3: Let $A = V - V(g) \subseteq \mathbb{A}^n$ be an R_0-basic set. Then $\dim(A) = \dim(V)$ and $\deg(A) = \deg(V)$. Call $\deg(g)$ the **complementary degree** of A.

Let $\mathbf{x} = (x_1, \ldots, x_n)$ be a generic point of V over K. We associate to A three rings derived from $\mathbf{x}$: $R_0[A] = R_0[\mathbf{x}, g(\mathbf{x})^{-1}]$, $K[A] = K[\mathbf{x}, g(\mathbf{x})^{-1}]$, and $K(A) = K(\mathbf{x})$. Given a homomorphism $\varphi_0\colon R_0 \to M$ into a field M, there is an obvious bijection between the set $A(M)$ and

$$\{\varphi \in \mathrm{Hom}(R_0[A], M) \mid \varphi \text{ extends } \varphi_0\}.$$

We list some properties of A whose definitions involve these rings.

(i) A is R_0-**normal** if $R_0[A]$ is integrally closed.

(ii) A is **absolutely** R_0-**normal** if A_R is R-normal for every integrally closed integral domain R and every homomorphism $\varphi_0\colon R_0 \to R$, whenever A_R is an R-basic set and $\dim(A_R) = \dim(A)$. (In this case A_R will be absolutely R-normal.)

(iii) A is **absolutely irreducible** if V is absolutely irreducible (in which case V is called a **variety**). $\blacksquare$

LEMMA 2.4: *Assume that R_0 is integrally closed. Let $A = V - V(g)$ be an R_0-basic set.*

(a) *Suppose that $R_0[A]$ can be written as $R_0[z_1, \ldots, z_m]$, where for each $1 \leq i \leq m$ one of the following three cases occurs: either*

  (i) *$z_i = g(z_1, \ldots, z_{i-1})^{-1}$ for some $g \in R_0[Z_1, \ldots, Z_{i-1}]$; or*

  (ii) *$R_0[z_1, \ldots, z_i]/R_0[z_1, \ldots, z_{i-1}]$ is a ring cover [Definition 1.1]; or*

  (iii) *z_i is transcendental over the quotient field of $R_0[z_1, \ldots, z_{i-1}]$.*

Then A is absolutely R_0-normal.

(b) *Assume that R_0 is a given integrally closed integral domain, presented in its quotient field K (see [FJ, p. 229]). Then we can compute $h \in R_0[X_1, \dots, X_n]$ not vanishing on A such that $A' = A - V(h) = V - V(gh)$ is an absolutely R_0-normal basic set.*

Proof of (a): First notice that $R_0[z_1, \dots, z_m]$ is integrally closed. Indeed, let $R_i = R_0[z_1, \dots, z_i]$, and assume, by induction, that R_{i-1} is integrally closed. Then $R_i = R_{i-1}[z_i]$ is also integrally closed: in case (i) by [L, Proposition 8 on p. 242], in case (ii) by [FJ, Lemma 5.3], and in case (iii) by [ZS, p. 85, Thm. 29(a)].

Next let φ_0: $R_0 \to R$ be a homomorphism into an integrally closed integral domain R such that A_R is an R-basic set and $\dim(A_R) = \dim(A)$. Then φ_0 extends to a homomorphism φ: $R_0[A] \to R[A_R]$, and $R[A_R] = R[\bar{z}_1, \dots, \bar{z}_m]$, where $\bar{z}_i = \varphi(z_i)$. Conditions (i), (ii), (iii) still hold if we replace z_j by $\bar{z}_j$ and R_0 by R. Thus $R[A_R]$ is again integrally closed.

Proof of (b): If R_0 is a field, [FJ, Lemma 17.28] shows how to choose h so that $R_0[A']$ is integrally closed. The same arguments work if R_0 is only an integrally closed integral domain. Moreover, the h constructed is such that $R_0[A']$ has the structure given in (a), so A' is absolutely R_0-normal. ∎

Remark 2.5: In the setup of Lemma 2.4, if the ring R_0 is also regular [M, p. 140], then so is $R_0[A]$. In fact, as in the proof of Lemma 2.4(a), if R_{i-1} is regular, then so is R_i. In case (i) this is clear. In case (ii), R_i is an étale R_{i-1}-algebra [R, Proposition 8 on p. 18], and therefore regular by [R, Exercice on p. 75]. In case (iii) it follows from [M, (17.J)]. ∎

Definition 2.6: Ring/set cover. Let A be an R_0-normal basic set. If $S/R_0[A]$ is a (Galois) ring cover, then we say that S/A is a **(Galois) ring/set cover**.

Let S/A be a Galois ring/set cover, and let M be a finite field. A point $\mathbf{a} \in A(M)$ corresponds to a homomorphism φ: $R_0[A] \to M$ (Definition 2.3). The **Artin symbol** $\mathrm{ar}(S/A, M, \mathbf{a}) = \mathrm{ar}(S/A, \mathbf{a}) \subseteq \mathcal{G}(S/R_0[A])$ is defined as the Artin symbol $\mathrm{ar}(S/R_0[A], \varphi)$ (Definition 1.5). Similarly, $\mathrm{Ar}(S/A, M, \mathbf{a}) = \mathrm{Ar}(S/A, \mathbf{a}) = \mathrm{Ar}(S/R_0[A], \varphi)$. ∎

Remark 2.7: Degrees. Let V be a closed subset of the projective space $\mathbb{P}^n$, defined over an algebraically closed field K. Let $H \subseteq \mathbb{P}^n$ be a hypersurface defined by a polynomial of total degree d.

(a) $\deg(H) = d$ [H, Prop. I.7.6(d)].

(b) We say that V is of **pure dimension** r if all of its irreducible components Z are of dimension r. For such V we have $\deg(V) = \sum_Z \deg(Z)$ [H, Prop. I.7.6(b)].

(c) Let V be of pure dimension r. Assume that H contains no irreducible component of V. Then $V \cap H$ is of pure dimension $r-1$ and $\deg(V \cap H) \leq d \cdot \deg(V)$.

Indeed, let $V = \bigcup_i V_i$ and $V_i \cap H = \bigcup_j Z_{ij}$ be the decompositions into irreducible components. Then $V \cap H = \bigcup_i \bigcup_j Z_{ij}$. By the dimension theorem [H, Thm. 7.2], $\dim(Z_{ij}) = \dim(V_i) - 1 = r - 1$, hence $V \cap H$ is of pure dimension $r-1$. Furthermore, by (b), $\deg(V \cap H) \leq \sum_i \sum_j \deg(Z_{ij})$. By (a) and by Bézout's theorem [H, Thm. I.7.7], $\sum_j \deg(Z_{ij}) \leq d \cdot \deg(V_i)$, for each i. Summing up these inequalities over i and using (b) we get $\sum_i \sum_j \deg(Z_{ij}) \leq d \cdot \sum_i \deg(V_i) \leq d \cdot \deg(V)$.

The above facts remain true if we replace $\mathbb{P}^n$ by the affine space $\mathbb{A}^n$. Indeed, we may consider $\mathbb{A}^n$ as an open subset of $\mathbb{P}^n$; replacing the ambient sets by their Zariski closures in $\mathbb{P}^n$ changes neither degrees nor dimensions. ∎

Section 4 uses the following technical result.

Lemma 2.8: *Let K be an algebraically closed field. Let $V \subseteq \mathbb{A}^n$ and $W \subseteq \mathbb{A}^{n+e}$ be varieties over K with respective generic points $\mathbf{x}$ and $(\mathbf{x}, \mathbf{z})$, where $\mathbf{x} = (x_1, \ldots, x_n)$, $\mathbf{z} = (z_1, \ldots, z_e)$. Suppose that z_i is algebraic over $K(\mathbf{x})$ and fix $h_i \in K[X_1, \ldots, X_n, Z_i]$ such that $h_i(\mathbf{x}, Z_i) \neq 0$ and $h_i(\mathbf{x}, z_i) = 0$, for $1 \leq i \leq e$. Then $\dim(W) = \dim(V)$ and $\deg(W) \leq \deg(V) \cdot \prod_{i=1}^e \deg(h_i)$.*

Proof: The first assertion is clear.

To prove the second assertion let $t_1, \ldots, t_e$ be algebraically independent over $K(\mathbf{x})$. For every $0 \leq i \leq e$ let V_i be the variety in $\mathbb{A}^{n+e}$ defined by the generic point $(\mathbf{x}, z_1, \ldots, z_i, t_{i+1}, \ldots, t_e)$ over K. Thus V_i is of dimension $\dim(V) + e - i$, the variety $V_0 = V \times \mathbb{A}^e$ is of degree $\deg(V)$, and $V_e = W$. It suffices to show that $\deg(V_{i+1}) \leq \deg(V_i)\deg(h_{i+1})$ for $1 \leq i \leq e$.

Let $U = V_i \cap V(h_{i+1})$. We have $V_{i+1} \subseteq U \subseteq V_i$, and $\dim(V_{i+1}) = \dim(V_i) - 1 = \dim(U)$. Thus V_{i+1} is one of the irreducible components of U. By Remark 2.7(c), $\deg(U) \leq \deg(V_i)\deg(h_{i+1})$, and U is of pure dimension. Therefore, by Remark 2.7(b), $\deg(V_{i+1}) \leq \deg(U)$. Our claim follows from these two inequalities. ∎

3. Counting rational points on basic sets

We begin with a crude upper bound on the number of points in sets of pure dimension (Remark 2.7(b)). Cf. [LW, Lemma 1].

LEMMA 3.1:

(a) *Let A be a closed subset of $\mathbb{A}^n$ of pure dimension r and degree d defined over $\mathbb{F}_q$. Then $|A(\mathbb{F}_q)| \leq dq^r$.*

(b) *Let A be a closed subset of $\mathbb{P}^n$ of pure dimension r and degree d defined over $\mathbb{F}_q$. Then $|A(\mathbb{F}_q)| \leq d(q+1)^r \leq 2^r dq^r$.*

Proof of (b): By induction on r. We may assume that no proper linear variety $L \subset \mathbb{P}^n$ defined over $\mathbb{F}_q$ contains A. Otherwise choose a minimal L with this property, and change the coordinates so that L becomes a projective space.

Assume first that A is irreducible over $\mathbb{F}_q$. Then the absolutely irreducible components of A are conjugate over $\mathbb{F}_q$. For each $\mathbf{a} = (a_0{:}a_1) \in \mathbb{P}^1(\mathbb{F}_q)$ let $L_{\mathbf{a}}$ be the linear subvariety $V(a_0X_1 - a_1X_0)$ of $\mathbb{P}^1(\mathbb{F}_q)$. Then $A \not\subseteq L_{\mathbf{a}}$, and as $L_{\mathbf{a}}$ is defined over $\mathbb{F}_q$, it contains no absolutely irreducible component of A. By Remark 2.7(c), $A \cap L_{\mathbf{a}}$ is of pure dimension $r-1$ and $\deg(A \cap L_{\mathbf{a}}) \leq d$. By the induction hypothesis, $|(A \cap L_{\mathbf{a}})(\mathbb{F}_q)| \leq (q+1)^{r-1}$. We have $A(\mathbb{F}_q) = \bigcup_{\mathbf{a} \in \mathbb{P}^1(\mathbb{F}_q)} (A \cap L_{\mathbf{a}})(\mathbb{F}_q)$. Hence $|A(\mathbb{F}_q)| \leq d(q+1)^r$.

In the general case let $V_1, \ldots, V_s$ be the irreducible components of A over $\mathbb{F}_q$. Then $\sum_i \deg(V_i) = d$ [H, Prop. I.7.6(b)]. By the preceding case $|V_i(\mathbb{F}_q)| \leq \deg(V_i)(q+1)^r$. Hence $|A(\mathbb{F}_q)| \leq \sum_i \deg(V_i)(q+1)^r = d(q+1)^r$.

Proof of (a): Similar to the proof of (b). ∎

COROLLARY 3.2: *Let $V \subseteq \mathbb{P}^n$ be a projective variety of dimension r and degree d, and let H be a hypersurface of degree d' in $\mathbb{P}^n$ defined over $\mathbb{F}_q$, not containing V. Then $|(V \cap H)(\mathbb{F}_q)| \leq dd'(q+1)^{r-1} \leq 2^{r-1}dd'q^{r-1}$.*

Proof: By Remark 2.7(c), $V \cap H$ is of pure dimension $r-1$ and $\deg(V \cap H) \leq dd'$. ∎

Let V be a variety in the projective space $\mathbb{P}^n$ of dimension r and degree d defined over $\mathbb{F}_q$. Let $N_q = |V(\mathbb{F}_q)|$. The Lang-Weil [LW] estimate for N_q produces a constant $\alpha_0(n,r,d)$ such that

$$|N_q - q^r| \leq (d-1)(d-2)q^{r-\frac{1}{2}} + \alpha_0(n,r,d)q^{r-1}. \tag{1}$$

Their proof uses induction starting from $r = 1$. Wolfgang Litz [Li, p. 48] carefully follows the reduction steps and computes a suitable value for $\alpha_0(n, r, d)$:

$$\begin{aligned}\alpha_0(n,r,d) = {} & 2^{r-1}(d(d-1)^2+1) \\ & + r\left(1+(d-1)(d-2)+2^{2n+r-3}2^m m^{2^m} d^2\right),\end{aligned} \tag{2}$$

with $m = \binom{n+d}{n}^r$.

For the estimate of numbers of points on basic sets define

$$\alpha(n,r,d,\delta) = \alpha_0(n,r,d) + 2^{r-1}d(\delta+1). \tag{3}$$

Notice that α is a non-decreasing function in each of its variables.

Proposition 3.3: *Let $A \subseteq \mathbb{A}^n$ be a basic set of dimension r, degree d and complementary degree δ, defined over $\mathbb{F}_q$. Let $N_q = |A(\mathbb{F}_q)|$.*

(a) *If A is absolutely irreducible, then*

$$|N_q - q^r| \le (d-1)(d-2)q^{r-\frac{1}{2}} + \alpha(n,r,d,\delta)q^{r-1}. \tag{4}$$

(b) *If A is $\mathbb{F}_q$-normal but not absolutely irreducible, then $A(\mathbb{F}_q) = \emptyset$.*

Proof of (a): Write A as $A = V - V(g)$, where V is an absolutely irreducible variety defined over $\mathbb{F}_q$ and $g \in \mathbb{F}_q[X_1, \ldots, X_n]$ is a polynomial not vanishing on V. (When $r = 0$, then $A = V$, $d = 1$, and $|V(\mathbb{F}_q)| = 1$.) View $\mathbb{A}^n$ as the open subset of $\mathbb{P}^n$ defined by $X_0 \neq 0$. The Zariski closure of V in $\mathbb{P}^n$ is an absolutely irreducible projective variety $\bar{V}$ of degree d and dimension r defined over $\mathbb{F}_q$. Let $\bar{N}_q = |\bar{V}(\mathbb{F}_q)|$. Consider the homogenization

$$g^* = X_0^\delta g\left(\frac{X_1}{X_0}, \ldots, \frac{X_n}{X_0}\right) \in \mathbb{F}_q[X_0, \ldots, X_n],$$

of g [H, p. 11]. Then $A = \bar{V} - (\bar{V} \cap H)$, where $H = V(X_0 g^*)$. Therefore $\deg(H) = \deg(X_0 g^*) = \delta + 1$ (Remark 2.7(a)). Hence, by Corollary 3.2 and by (1) and (3)

$$\begin{aligned}|N_q - q^r| &\le |\bar{N}_q - q^r| + |(\bar{V} \cap H)(\mathbb{F}_q)| \\ &\le (d-1)(d-2)q^{r-\frac{1}{2}} + \alpha_0(n,r,d)q^{r-1} + 2^{r-1}d(\delta+1)q^{r-1} \\ &= (d-1)(d-2)q^{r-\frac{1}{2}} + \alpha(n,r,d,\delta)q^{r-1}.\end{aligned}$$

Proof of (b): Let L be the algebraic closure of $\mathbb{F}_q$ in the quotient field of $\mathbb{F}_q[A]$ (=the function field of A); by assumption $L \neq \mathbb{F}_q$. The elements of L are certainly integral over $\mathbb{F}_q[A]$ and hence $L \subseteq \mathbb{F}_q[A]$. If $A(\mathbb{F}_q) \neq \emptyset$, there exists an $\mathbb{F}_q$-homomorphism $\mathbb{F}_q[A] \to \mathbb{F}_q$. It restricts to an $\mathbb{F}_q$-homomorphism $L \to \mathbb{F}_q$, a contradiction. ∎

4. The special nonregular analog of the Chebotarev density theorem

We state and give a full proof of a more explicit version of [FS], Proposition 4.1.

Let K be a fixed finite field, let $\widetilde{K}$ be its algebraic closure, and let $G(K) = \mathcal{G}(\widetilde{K}/K)$ be the absolute Galois group of K. The Frobenius automorphism Frob over K generates $G(K)$.

Notation: Let S be an integrally closed domain containing K with quotient field F. Let F_0 denote the algebraic closure of K in F, that is, the integral closure of K in S. Let $\mathbb{A}(S)$ be the set of F_0-homomorphisms $\varphi: S \to F_0$.

Let S/R be a finitely generated regular Galois ring cover over K (Definition 1.1). Let E, F be the quotient fields of R, S, respectively, and let $L = F_0$ be the algebraic closure of K in F.

Observe that $\mathbb{A}(R) = \mathrm{Hom}_K(R, K)$. In particular, if R is the coordinate ring of an absolutely irreducible affine variety A defined over K, then we may identify $\mathbb{A}(R)$ with $A(K)$. ∎

Lemma 4.1: *Every $\varphi \in \mathbb{A}(R)$ extends to exactly $[F : LE]$ distinct L-homomorphisms $\psi: S \to \widetilde{K}$.*

Proof: First, φ extends to a unique L-homomorphism $\varphi': LR \to L$. Now, S/LR is a cover, so $S = RL[z]$, where $p(X) = \mathrm{irr}(z, LE) \in LR[X]$. The extensions of φ' to an L-homomorphism $S \to \widetilde{K}$ correspond bijectively to the mappings of z onto one of the $[F : LE]$ distinct roots of $\varphi'(p)(X) \in \widetilde{K}[X]$ in $\widetilde{K}$. ∎

Consider an L-homomorphism $\psi: S \to \widetilde{K}$ that satisfies $\psi(R) = K$. By Lemma 1.3 this induces a group homomorphism $\psi^*: G(K) \to \mathcal{G}(S/R) = \mathcal{G}(F/E)$ with:

$$\psi(\psi^*(\sigma)(s)) = \sigma(\psi(s)), \qquad \text{for all } s \in S \tag{1}$$

In particular, since ψ fixes L,

$$\mathrm{res}_L \psi^*(\mathrm{Frob}) = \mathrm{res}_L \mathrm{Frob}. \tag{2}$$

Notation: For $\tau \in \mathcal{G}(F/E)$ let

$$C(S/R,\tau) = \{\psi\colon S \to \widetilde{K} \mid \psi \text{ is an } L\text{-homomorphism}, \qquad \psi(R) = K \text{ and } \psi^*(\mathrm{Frob}) = \tau\}.$$

LEMMA 4.2: *Let $\mathcal{C}$ be a conjugacy class in $\mathcal{G}(F/E)$ and let $\tau \in \mathcal{C}$. Then*

$$|\{\varphi \in \mathrm{Hom}_K(R,K) \mid \mathrm{ar}(S/R,\varphi) = \mathcal{C}\}| = \frac{|\mathcal{C}|}{[F:LE]}\,|C(S/R,\tau)|\,.$$

Proof: Put $C = \{\varphi \in \mathrm{Hom}_K(R,K) \mid \mathrm{ar}(S/R,\varphi) = \mathcal{C}\}$. By Lemma 4.1, every $\varphi \in C$ extends to exactly $[F:LE]$ L-homomorphisms $S \to \widetilde{K}$. These extensions are the elements of $\dot{\bigcup}_{\sigma\in\mathcal{C}} C(S/R,\sigma)$. By Lemma 1.4(d), for each $\rho \in \mathcal{G}(F/E)$, $\psi \in C(S/R,\rho\tau\rho^{-1})$ if and only if $\psi \circ \rho \in C(S/R,\tau)$. Hence $|C(S/R,\sigma)| = |C(S/R,\tau)|$ for each $\sigma \in \mathcal{C}$. We conclude that

$$[F:LE]\cdot|C| = \left|\dot{\bigcup_{\sigma\in\mathcal{C}}} C(S/R,\sigma)\right| = |\mathcal{C}|\cdot|C(S/R,\tau)|\,. \qquad \blacksquare$$

The following theorem combines the field crossing argument [FJ, Section 23.1] and descent [FJ, Section 9.9]. It enables us to reduce the counting of points with a given Artin symbol to the counting of K-rational points in a basic set (Proposition 3.3).

PROPOSITION 4.3: *Let $\tau \in \mathcal{G}(F/E)$ such that $\mathrm{res}_L\tau = \mathrm{res}_L\mathrm{Frob}$. Let $L' = K(\omega)$ be a finite Galois extension of K of degree e that contains L. Put $S' = L'S$ and $F' = L'F$. Then the following hold.*

(a) *L' is the algebraic closure of K in S'.*

(b) *There exists a unique $\tau' \in \mathcal{G}(F'/E)$ such that $\mathrm{res}_F\tau' = \tau$ and $\mathrm{res}_{L'}\tau' = \mathrm{res}_{L'}\mathrm{Frob}$. Moreover, $\mathrm{ord}(\tau') = \mathrm{lcm}(\mathrm{ord}(\tau), e)$.*

(c) *S' is the integral closure of R in F'.*

Now, assume that $\mathrm{ord}(\tau) \mid e$. Let E' be the fixed field of τ' in F' and let R' be the integral closure of R in E'. Then, these further conditions hold.

(d) *$E' \cap \widetilde{K} = K$ and $E'L' = F'$.*

(e) *$R' = R[y_1,\ldots,y_e]$, where $(y_1,\ldots,y_e) \in (F')^e$ is the solution of the system of linear equations*

$$\sum_{j=1}^{e} \mathrm{Frob}^i(\omega^j)y_j = \tau^i(z), \qquad i = 1,\ldots,e \tag{3}$$

over L'.

(f) *$S' = R'L'$ and S'/R' is a finitely generated regular Galois ring cover over K.*

(g) $|C(S'/R', \tau')| = |C(S/R, \tau)|$.

(h) $|C(S'/R', \tau')| = |\mathbb{A}(R')|$.

$$
\begin{tikzcd}
E' \arrow[rrr, dash] \arrow[dd, dash] & & & F' \arrow[dd, dash] \arrow[dl, dash] \\
& & F \arrow[dl, dash] & \\
E \arrow[r, dash] \arrow[d, dash] & EL \arrow[rr, dash] \arrow[d, dash] & & EL' \arrow[d, dash] \\
K \arrow[r, dash] & L \arrow[rr, dash] & & L'
\end{tikzcd}
\qquad
\begin{tikzcd}
R' \arrow[rrr, dash] \arrow[dd, dash] & & & S' \arrow[dd, dash] \arrow[dl, dash] \\
& & S \arrow[dl, dash] & \\
R \arrow[r, dash] \arrow[d, dash] & RL \arrow[rr, dash] \arrow[d, dash] & & RL' \arrow[d, dash] \\
K \arrow[r, dash] & L \arrow[rr, dash] & & L'
\end{tikzcd}
$$

Proof of (a): S is linearly disjoint from $\widetilde{K}$ over L. Hence $L'S$ is linearly disjoint from $\widetilde{K}$ over L'.

Proof of (b): From (a), $L' \cap F = L$. So $L'E \cap F = LE$. Therefore,

$$\text{(4)} \qquad \mathcal{G}(F'/E) \cong \mathcal{G}(F/E) \times_{\mathcal{G}(LE/E)} \mathcal{G}(L'E/E) \cong \mathcal{G}(F/E) \times_{\mathcal{G}(L/K)} \mathcal{G}(L'/K).$$

There is a unique $\tau' \in \mathcal{G}(F'/E)$ mapped by this isomorphism onto $(\tau, \mathrm{res}_{L'}\mathrm{Frob})$. The order of τ' is the least common multiple of $\mathrm{ord}(\tau)$ and $\mathrm{ord}(\mathrm{res}_{L'}\mathrm{Frob})$.

Proof of (c): It suffices to show that S' is the integral closure of S in F'. As ω is a primitive element for the ring cover S'/S (Definition 1.1), this follows by Remark 1.2(ii).

Proof of (d): The restriction map $\mathcal{G}(F'/E') \to \mathcal{G}(L'/K)$ sends the generator τ' of $\mathcal{G}(F'/E')$ onto the generator $\mathrm{res}_{L'}\mathrm{Frob}$ of $\mathcal{G}(L'/K)$. Therefore it is surjective. Moreover, it is an isomorphism: $[F' : E'] = \mathrm{ord}(\tau') = \mathrm{lcm}(\mathrm{ord}(\tau), e) = e = [L' : K]$ by (b). Hence, $E' \cap L' = K$ and $E'L' = F'$. Thus $E' \cap \widetilde{K} = E' \cap F' \cap \widetilde{K} = E' \cap L' = K$.

Proof of (e): As $\left(\mathrm{Frob}^i(\omega^j)\right)$ is an invertible $e \times e$ matrix over L' [L, p. 212], we have $y_1, \ldots, y_e \in L'S = S'$. Apply τ' to (3). By (b)

$$\sum_{j=1}^{e} \mathrm{Frob}^{i+1}(\omega^j)\tau'(y_j) = \tau^{i+1}(z), \qquad i = 1, \ldots, e.$$

Thus $(\tau'(y_1), \ldots, \tau'(y_e))$ also solves (3). Hence $\tau'(y_j) = y_j$ for each $1 \le j \le e$. It follows that $y_1, \ldots, y_e \in E'$. As S' is integral over R, it is also integral over R'. So $y_1, \ldots, y_e \in S' \cap E' \subseteq R'$.

Denote $R[y_1, \ldots, y_e]$ by R''. We have $R'' \subseteq R'$. By (3), $z \in R''L'$. Hence $R''L' = S'$, and therefore $R'L' = S'$. Since by (d) L' is linearly disjoint from E' over K, we have $R'' = R'$.

Proof of (f): We have shown above that $R'[\omega] = R'L' = S'$. Thus, $R'[\omega]/R'$ is a Galois cover (and ω its primitive element). Regularity follows from (d) and finite generation from (e).

Proof of (g): We show that the restriction map $\mathrm{res}_F\colon C(S'/R', \tau') \to C(S/R, \tau)$ is bijective. Applying Lemma 4.1 to the cover S'/S over L', we conclude that every $\psi \in C(S/R, \tau)$ extends to a unique L'-homomorphism $\psi'\colon S' \to \widetilde{K} = \widetilde{L}$. We must show that $\psi' \in C(S'/R', \tau')$.

Let us first verify that $\psi'(R') = K$. There exists $\sigma \in \mathcal{G}(F'/E)$ such that

$$\psi' \circ \sigma = \mathrm{Frob} \circ \psi'. \tag{5}$$

[L, Corollary 1, p. 247]. In particular, $\psi(\mathrm{res}_F \sigma(x)) = \mathrm{Frob}(\psi(x))$ for each $x \in S$. By (1), $\mathrm{res}_F \sigma = \psi^*(\mathrm{Frob}) = \tau$. Furthermore, $\mathrm{res}_{L'} \sigma = \mathrm{res}_{L'} \mathrm{Frob}$. Thus (b) implies $\sigma = \tau'$. We conclude from (5) that $\psi'(x) = \mathrm{Frob}(\psi'(x))$ for each $x \in R'$, and thus $\psi'(R') = K$.

By (5), $\psi'^*(\mathrm{Frob}) = \sigma = \tau'$. Thus, $\psi' \in C(S'/R', \tau')$.

Proof of (h): By Lemma 4.1, every $\psi \in \mathbb{A}(R')$ extends to a unique L'-homomorphism $\psi'\colon S' \to \widetilde{K} = \widetilde{L}$. By (2), $\mathrm{res}_{L'} \psi'^*(\mathrm{Frob}) = \mathrm{res}_{L'} \mathrm{Frob}$. From (d) we have determined the restriction of τ' to the field of constants of L'. Therefore (b) shows that τ' is the unique element of $G(F'/E')$ that restricts to $\mathrm{res}_{L'}\mathrm{Frob}$. Thus $\psi'^*(\mathrm{Frob}) = \tau'$, and $\psi' \in C(S'/R', \tau')$. ∎

To formulate the main result of this section, we fix the following data.

(6a) $A = V - V(g)$ is an $\mathbb{F}_q$-normal absolutely irreducible basic subset of $\mathbb{A}^n$ with $\dim(V) = r$, $\deg(V) = d$, $\deg(g) = \delta$, and $\mathbf{x}$ is a generic point of V over $\mathbb{F}_q$.

(6b) S/A is a regular Galois ring/set cover over $\mathbb{F}_q$ and F/E is the corresponding Galois extension of fields.

(6c) L is the algebraic closure of $\mathbb{F}_q$ in F.

(6d) $R = \mathbb{F}_q[A] = \mathbb{F}_q[\mathbf{x}, g(\mathbf{x})^{-1}]$ and $S = R[z]$.
(6e) $h(\mathbf{X}, Z) \in L[X_1, \ldots, X_n, Z]$ satisfies $h(\mathbf{x}, Z) \neq 0$ and $h(\mathbf{x}, z) = 0$.

THEOREM 4.4 ((): *Special nonregular analog of the Chebotarev density theorem) Let $\mathcal{C}$ be a conjugacy class of exponent e in $\mathcal{G}(F/E)$. Set*

$$N = |\{\mathbf{a} \in A(\mathbb{F}_q) |\ \mathrm{ar}(S/A, \mathbf{a}) = \mathcal{C}\}| = |\{\varphi \in \mathrm{Hom}_{\mathbb{F}_q}(R, \mathbb{F}_q) |\ \mathrm{ar}(S/R, \varphi) = \mathcal{C}\}|.$$

(a) *If $\mathrm{res}_L \mathcal{C} \neq \{\mathrm{res}_L \mathrm{Frob}\}$, then $N = 0$.*
(b) *If $\mathrm{res}_L \mathcal{C} = \{\mathrm{res}_L \mathrm{Frob}\}$, then*

$$|N - cq^r| \leq c(d'-1)(d'-2)q^{r-\frac{1}{2}} + c\alpha(n', r, d', \delta)q^{r-1}. \tag{7}$$

Here $c = \frac{|\mathcal{C}|}{[F:LE]}$, $n' = n + e$, $d' = d \cdot \deg(h)^e$, and α is defined by (3) of Section 3.

Proof: Choose $\tau \in \mathcal{C}$. By Lemma 4.2, $N = c|C(S/R, \tau)|$.

In case (a), $\mathrm{res}_L \tau \neq \mathrm{res}_L \mathrm{Frob}$. Hence $C(S/R, \tau) = \emptyset$ by (2). Thus, $N = 0$.

In case (b), $\mathrm{res}_L \tau = \mathrm{res}_L \mathrm{Frob}$. Let $K = \mathbb{F}_q$. As

$$[L : K] = \mathrm{ord}(\mathrm{res}_L \mathrm{Frob}) = \mathrm{ord}(\mathrm{res}_L \tau) \mid \mathrm{ord}(\tau) = e,$$

the unique extension L' of K of order e contains L. Thus, we may use the notation and the results of Proposition 4.3. By (g) and (h), $|C(S/R, \tau)| = |\mathbb{A}(R')|$. Therefore $N = c|\mathbb{A}(R')|$. Let $V' \subseteq \mathbb{A}^{n+e}$ be the absolutely irreducible variety defined over K that has $(\mathbf{x}, \mathbf{y})$ as generic point, and let $A' = V' - V(g)$. Then $K[A'] \cong_K R'$. We conclude that $|\mathbb{A}(R')| = |A'(K)|$. Below we show that $\deg(V') \leq d'$. This gives (7) by Proposition 3.3(a).

Finally we estimate $\deg(V')$. Denote $z_i = \tau^i(z)$ for each $1 \leq i \leq e$, and let $\mathbf{z} = (z_1, \ldots, z_e)$. Let $V'' \subseteq \mathbb{A}^{n+e}$ be the variety defined over $\widetilde{K}$ that has $(\mathbf{x}, \mathbf{z})$ as generic point. Equations (3) define a $\widetilde{K}$-linear automorphism of $\mathbb{A}^{n+e}$ that maps V' onto V''. Hence $\deg(V') = \deg(V'')$. So, by Lemma 2.8, $\deg(V') \leq d \cdot \deg(h)^e = d'$. ∎

5. The absolute nonregular analog of the Chebotarev density theorem

The absolute nonregular analog of the Chebotarev density theorem (Theorem 5.3) considers a situation similar to the special nonregular analog of the Chebotarev density theorem (Theorem 4.4). Both theorems deal with a Galois ring/set cover S/A and a conjugacy domain $\mathcal{C}$ of $\mathcal{G}(S/A)$. The differences are as follows.

In Theorem 4.4, S/A is defined over a finite field $\mathbb{F}_q$. In Theorem 5.3, S/A is defined over an integrally closed integral domain R_0, which may have characteristic 0. Theorem 4.4 estimates the number of points $\mathbf{a} \in A(\mathbb{F}_q)$ for which $\mathrm{ar}(S/A, \mathbf{a}) = \mathcal{C}$ for the particular base field $\mathbb{F}_q$. Theorem 5.3 estimates this number for each field $\mathbb{F}_q$ such that there exists a homomorphism $\varphi_0\colon R_0 \to \mathbb{F}_q$.

Lemma 5.1: *Let $R \subseteq R' \subseteq S$ be rings such that both S/R and S/R' are Galois covers. Let $\varphi\colon R \to \mathbb{F}_q$ be a homomorphism. Let $G = \mathcal{G}(S/R)$, $G' = \mathcal{G}(S/R')$ and $\mathcal{C} = \mathrm{ar}(S/R, \varphi)$. Then*

$$\left|\{\varphi'\colon R' \to \mathbb{F}_q \mid \mathrm{res}_R \varphi' = \varphi\}\right| = \frac{|G|}{|\mathcal{C}|}\frac{|G' \cap \mathcal{C}|}{|G'|} .$$

Proof: Consider the set

$$\mathbb{A} = \{\psi\colon S \to \widetilde{\mathbb{F}_q} \mid \mathrm{res}_R \psi = \varphi,\ \psi^*(\mathrm{Frob}) \in G'\}.$$

(By Lemma 1.4(c), $\psi*$ is the same, whether defined with respect to the cover S/R or S/R'.) Each $\varphi'\colon R' \to \mathbb{F}_q$ that satisfies $\mathrm{res}_R \varphi' = \varphi$ extends to exactly $|G'|$ elements of $\mathbb{A}$ (Lemma 1.4(e)), and each element of $\mathbb{A}$ is obtained this way. Thus we have to show that $|\mathbb{A}| = (|G| \,/\, |\mathcal{C}|) \cdot |G' \cap \mathcal{C}|$.

If $G' \cap \mathcal{C} = \emptyset$, then $\mathbb{A} = \emptyset$. Otherwise we can choose an extension $\psi\colon S \to \mathbb{F}_q$ of φ such that $\tau = \psi^*(\mathrm{Frob}) \in G'$. Then, apply Lemma 1.4(e) and (d) to get

$$\mathbb{A} = \{\psi \circ \sigma \mid \sigma \in G,\ (\psi \circ \sigma)^*(\mathrm{Frob}) \in G'\} = \{\psi \circ \sigma \mid \sigma \in G,\ \tau^\sigma \in G'\}.$$

This last set corresponds bijectively with the set $\{\sigma \in G \mid \tau^\sigma \in G'\}$, which has

$$\left|C_G(\tau)\right| \cdot \left|\{\tau^\sigma \in G' \mid \sigma \in G\}\right| = (|G| \,/\, |\mathcal{C}|) \cdot |G' \cap \mathcal{C}|$$

elements. ∎

Lemma 5.2: *Let $\kappa\colon G \to G_0$ be a homomorphism of finite groups and let $\mathcal{C}$ be a conjugacy class in G. For each $\tau \in \kappa(\mathcal{C})$ let $\mathcal{C}_\tau = \{\sigma \in \mathcal{C} \mid \kappa(\sigma) = \tau\}$. Then $\mathcal{C}_\tau$ is a conjugacy domain (i.e., a union of conjugacy classes) of $H_\tau = \kappa^{-1}(\langle\tau\rangle)$, and $|\mathcal{C}_\tau| = |\mathcal{C}|/|\kappa(\mathcal{C})|$.*

Proof: Indeed, $\mathcal{C}_\tau \subseteq \kappa^{-1}(\{\tau\}) \subseteq H_\tau$. If $\sigma \in \mathcal{C}_\tau$ and $h \in H_\tau$, then $\kappa(\sigma^h) = \tau^{\kappa(h)} = \tau$ (because $\kappa(h) \in \langle\tau\rangle$). Hence $\mathcal{C}_\tau$ is a conjugacy domain in H_τ.

If $\tau' \in \kappa(\mathcal{C})$, then $\mathcal{C}_{\tau'}$ and $\mathcal{C}_\tau$ are conjugate in G. Therefore $|\mathcal{C}_{\tau'}| = |\mathcal{C}_\tau|$. Furthermore, $\mathcal{C} = \bigcup_{\tau' \in \kappa(\mathcal{C})} \mathcal{C}_{\tau'}$. Thus $|\mathcal{C}| = |\kappa(\mathcal{C})| \cdot |\mathcal{C}_\tau|$. ∎

To formulate the main result of this section, we fix the following data:

(1) R_0 is an integral domain with quotient field K.

(2a) $A = V - V(g)$ is an absolutely normal (Definition 2.3(ii)) R_0-basic subset of $\mathbb{A}^n$ with $\dim(V) = r$ and $\deg(V) = d$, and $\mathbf{x}$ is a generic point of V over K.

(2b) S/A is a Galois ring/set cover, and F/E is the corresponding Galois extension of fields.

(2c) L is the algebraic closure of K in F, and S_0 is the integral closure of R_0 in L (hence $S_0 \subseteq S$).

(2d) L_1 is the maximal purely inseparable extension of L and S_1 is the integral closure of S_0 in L_1.

(2e) $R = R_0[A] = R_0[\mathbf{x}, g(\mathbf{x})^{-1}]$ and $S = R[z]$.

(2f) $h(\mathbf{X}, Z) \in S_0[X_1, \ldots, X_n, Z]$ is a polynomial that satisfies $h(\mathbf{x}, z) = 0$.

(3a) S_0/R_0 is a Galois cover, L/K the corresponding Galois cover of fields, and $G_0 = \mathcal{G}(L/K)$.

(3b) $K' = E \cap L$ is the algebraic closure of K in E, and R_0' is the integral closure of R_0 in K', and $G_0' = \mathcal{G}(L/K')$. As R is integrally closed, $R_0' \subseteq R$.

(3c) The absolutely irreducible component V_0 of V containing $\mathbf{x}$ is defined by polynomials whose coefficients generate a ring R_0'' integral over R_0.

(3d) $x_1, \ldots, x_r$ is a transcendence base of E/K (renumerate $x_1, \ldots, x_n$, if necessary), y is a primitive element for $L_1F/L_1(x_1, \ldots, x_r)$, and f is an absolutely irreducible polynomial in $S_1[X_1, \ldots, X_r, Y]$ with $f(x_1, \ldots, x_r, y) = 0$.

THEOREM 5.3: *Let $\mathcal{C}$ be a conjugacy class of exponent e in $\mathcal{G}(F/E)$. Let $\mathcal{C}_0' = \mathrm{res}_L \mathcal{C}$ and $\mathcal{C}_0 = \mathrm{Con}_{G_0}(\mathcal{C}_0')$.* (These are conjugacy classes in G_0' and G_0, respectively.) *Let $\varphi_0\colon R_0 \to \mathbb{F}_q$ be a homomorphism. Denote the reduction of objects via φ_0 by a bar. Assume further the following:*

(4a) $\dim(\bar{A}) = r$ *and* $\deg(\bar{A}) = d$*;*

(4b) *each extension of φ_0 to a homomorphism $R_0'' \to \widetilde{\mathbb{F}_q}$ maps V_0 onto an absolutely irreducible variety $\bar{V}_0$ of dimension r such that $\bar{g}$ does not vanish on all $\bar{V}_0$;*

(4c) *each extension of φ_0 to a homomorphism $S_1 \to \widetilde{\mathbb{F}_q}$ maps f onto an absolutely irreducible polynomial $\bar{f} \in \widetilde{\mathbb{F}_q}[X_1, \ldots, X_n, Y]$ such that* $\deg_Y(f) =$

$\deg_Y(\bar{f})$.

Let $\mathbb{A} = \{\mathbf{a} \in A(\mathbb{F}_q) |\ \mathrm{ar}(S/R, \mathbf{a}) = \mathcal{C}\}$, *and let* $N = |\mathbb{A}|$. *Then*

$$|N - \beta\gamma q^r| \le \beta\gamma(d'-1)(d'-2)q^{r-\frac{1}{2}} + \beta\gamma \cdot \alpha(n', r, d', \delta)q^{r-1}, \tag{5}$$

where

$$\beta = \frac{|G_0|}{|G_0'|}\frac{|G_0' \cap \mathcal{C}_0|}{|\mathcal{C}_0|} = [K' : K]\frac{|G_0' \cap \mathcal{C}_0|}{|\mathcal{C}_0|},$$
$$\gamma = \begin{cases} \frac{|\mathcal{C}|}{[F:LE]}\frac{1}{|\mathrm{res}_L\mathcal{C}|} & \text{if } \mathcal{C}_0 = \mathrm{ar}(S_0/R_0, \varphi_0) \iff \mathrm{res}_L\mathcal{C} \subseteq \mathrm{ar}(S_0/R_0, \varphi_0), \\ 0 & \text{otherwise,} \end{cases}$$

$n' = n + e$, *and* $d' = d \cdot \deg(h)^e$.

Proof: We may identify $\mathbb{A}$ with

$$\{\varphi \in \mathrm{Hom}(R, \mathbb{F}_q) |\ \mathrm{res}_{R_0}\varphi = \varphi_0 \text{ and } \mathrm{ar}(S/R, \varphi) = \mathcal{C}\}$$

(Definition 2.6). Let $\widehat{K}$ be the purely inseparable closure of K, and let $\widehat{R}_0$ be the integral closure of R_0 in $\widehat{K}$. Replacing R_0, R_0', S_0, R, S and K, K', L, E, F by $\widehat{R}_0$, $R_0'[\widehat{R}_0]$, $S_0[\widehat{R}_0]$, $R[\widehat{R}_0]$, $S[\widehat{R}_0]$ and $\widehat{K}$, $K'\widehat{K}$, $L\widehat{K}$, $E\widehat{K}$, $F\widehat{K}$, respectively, does not change β, γ, and $|\mathbb{A}|$ because each φ: $R \to \mathbb{F}_q$ uniquely extends to $\hat{\varphi}$: $R[\widehat{R}_0] \to \mathbb{F}_q$, etc. Thus we may assume that K is perfect, $L_1 = L$ and $S_1 = S_0$ (We also have to replace V by its irreducible component $\widehat{V}$ over $\widehat{K}$, but $\dim(\widehat{V}) = \dim(V)$ and $\deg(\widehat{V}) \le \deg(V)$, by [H, Proposition 7.6(b) on p. 52].) In this case E/K' is a regular extension, $R_0'' \subseteq R_0'$, and $\mathcal{C}_0 = \mathrm{res}_L\mathcal{C}$.

By Lemma 5.1, φ_0 has β extensions to homomorphisms φ_0': $R_0' \to \mathbb{F}_q$. Suppose we fix one such φ_0' and prove (5) with $\beta = 1$ and with

$$\mathbb{A} = \{\varphi \in \mathrm{Hom}(R, \mathbb{F}_q) |\ \mathrm{res}_{R_0'}\varphi = \varphi_0' \text{ and } \mathrm{ar}(S/R, \varphi) = \mathcal{C}\}.$$

Then (5) will hold for the original β and $\mathbb{A}$. So, we assume without loss of generality that $K = K'$, $R_0 = R_0'$. Thus K is algebraically closed in E, and $V = V_0$ is absolutely irreducible. By (4b), $\bar{V}$ is an absolutely irreducible variety defined over $\mathbb{F}_q$.

If $\mathcal{C}_0 \ne \mathrm{ar}(S_0/R_0, \varphi_0)$, then $\gamma = 0$. We must show that $\mathbb{A} = \emptyset$. But if $\varphi \in \mathbb{A}$, then Lemma 1.6 implies $\mathrm{ar}(S_0/R_0, \varphi_0) = \mathrm{Con}_{G_0}\mathrm{res}_L\mathrm{ar}(S/R, \varphi) = \mathrm{Con}_{G_0}\mathrm{res}_L\mathcal{C} = \mathcal{C}_0$, This is a contradiction.

Assume that $\mathcal{C}_0 = \mathrm{ar}(S_0/R_0, \varphi_0)$. Let $\bar{\mathbf{x}} = (\bar{x}_1, \ldots, \bar{x}_n)$ be a generic point of $\bar{V}$ over $\mathbb{F}_q$. Clearly $\bar{\delta} = \deg(\bar{g}) \le \deg(g) = \delta$. By (4b), $\bar{g}(\bar{\mathbf{x}}) \ne 0$. Let $\bar{A} = \bar{V} - V(\bar{g})$ and $\bar{R} = \mathbb{F}_q[\bar{A}] = \mathbb{F}_q[\bar{\mathbf{x}}, \bar{g}(\bar{\mathbf{x}})^{-1}]$. Then $\mathbf{x} \to \bar{\mathbf{x}}$ extends to a homomorphism $\pi\colon R \to \bar{R}$ which extends φ_0. By (2a) and (4a), $\bar{A}$ is normal: $\bar{R}$ is integrally closed. Extend π to a homomorphism ρ of S into the algebraic closure of $\mathbb{F}_q(\bar{\mathbf{x}})$. Then $\bar{z} = \rho(z)$ is a primitive element for the Galois ring cover $\bar{S} = \bar{R}[\bar{z}]$ of $\bar{R}$ (Remark 1.2(iii)). Denote the quotient field of $\bar{R}$ by $\bar{E}$ and that of $\bar{S}$ by $\bar{F}$. Then $\bar{F}/\bar{E}$ is a Galois extension.

Now let $\bar{L} = \mathbb{F}_q[\rho(S_0)]$ and $\bar{\rho} = \rho(f)$. Put $M = L(x_1, \ldots, x_r)$, let $\bar{M} = \bar{L}(\bar{x}_1, \ldots, \bar{x}_r)$, and let $\bar{F}' = \bar{L}(\bar{x}_1, \ldots, \bar{x}_r, \bar{y})$. Then $\bar{x}_1, \ldots, \bar{x}_r$ are algebraically independent over $\bar{L}$. By (4c), $\bar{f}$ is an absolutely irreducible polynomial with coefficients in $\bar{L}$ and with the same degree in Y as f and $\bar{f}(\bar{x}_1, \ldots, \bar{x}_r, y) = 0$. Hence $\bar{L}$ is the algebraic closure of F in $\bar{F}'$ and $[\bar{F}' : \bar{L}\bar{E}] \cdot [\bar{L}\bar{E} : \bar{M}] = [\bar{F}' : \bar{M}] = \deg_Y \bar{f} = \deg_Y f = [F : M] = [F : LE] \cdot [LE : M]$. But $[F : LE] \ge [\bar{F} : \bar{L}\bar{E}] \ge [\bar{F}' : \bar{L}\bar{E}]$ and $[LE : M] \ge [\bar{L}\bar{E} : \bar{M}]$. Hence $\bar{F}' = \bar{F}$ and $[F : LE] = [\bar{F} : \bar{L}\bar{E}]$. Let $\bar{h} = \rho(h)$.

With this we have defined data as in (6) of Section 4 with a bar on each object (except r, d and γ). The barred data satisfies all the requirements imposed there.

Denote the restriction of ρ to S_0 by ρ_0. This gives a commutative diagram of short exact sequences

$$\text{(6)}\qquad \begin{tikzcd} 1 \arrow[r] & \mathcal{G}(F/LE) \arrow[r] & \mathcal{G}(F/E) \arrow[r, "\kappa=\mathrm{res}_L"] & \mathcal{G}(L/K) \arrow[r] & 1 \\ 1 \arrow[r] & \mathcal{G}(\bar{F}/\bar{L}\,\bar{E}) \arrow[r] \arrow[u, "\rho^*"] & \mathcal{G}(\bar{F}/\bar{E}) \arrow[r] \arrow[u, "\rho^*"] & \mathcal{G}(\bar{L}/\mathbb{F}_q) \arrow[r] \arrow[u, "\rho_0^*"] & 1. \end{tikzcd}$$

The vertical arrows are injective by Lemma 1.4(b). The left one is bijective, because $[\bar{F} : \bar{L}\,\bar{E}] = [F : LE]$. Chase diagram (6) to get

$$\text{(7)}\qquad \rho^*(\mathcal{G}(\bar{F}/\bar{E})) = \kappa^{-1}(\rho_0^*(\mathcal{G}(\bar{L}/\mathbb{F}_q))) = \kappa^{-1}(\langle\tau\rangle),$$

where $\tau = \rho_0^*(\mathrm{res}_{\bar{L}}\mathrm{Frob})$. Notice that $\tau \in \mathrm{ar}(S_0/R_0, \varphi_0) = \mathcal{C}_0 = \kappa(\mathcal{C})$. Let

$$\bar{\mathcal{C}} = \{\sigma \in \mathcal{G}(\bar{F}/\bar{E}) |\ \rho^*(\sigma) \in \mathcal{C} \text{ and } \mathrm{res}_{\bar{L}}\sigma = \mathrm{res}_{\bar{L}}\mathrm{Frob}\}.$$

It follows from the commutativity of (6) and from (7) that $\rho^*(\bar{\mathcal{C}}) = \{\sigma \in \mathcal{C} |\ \kappa(\sigma) = \tau\}$. So, $\rho^*(\bar{\mathcal{C}}) = \mathcal{C}_\tau$, in the notation of Lemma 5.2. Hence, by that lemma, $\rho^*(\bar{\mathcal{C}})$

is a conjugacy domain of $\rho^*(\mathcal{G}(\bar{F}/\bar{E}))$. Therefore $\bar{\mathcal{C}}$ is a conjugacy domain of $\mathcal{G}(\bar{F}/\bar{E})$, and

$$|\bar{\mathcal{C}}| = |\rho^*(\bar{\mathcal{C}})| = |\mathcal{C}|/|\mathrm{res}_L \mathcal{C}| = \gamma[F : LE] \ . \tag{8}$$

Furthermore, every element of $\bar{\mathcal{C}}$ is of order e.

Observe that if $\bar{\varphi} \in \mathrm{Hom}_{\mathbb{F}_q}(\bar{R}, \mathbb{F}_q)$, then $\varphi = \bar{\varphi} \circ \pi$ is a homomorphism from R to $\mathbb{F}_q$ whose restriction to R_0 is φ_0. Extend $\bar{\varphi}$ to a homomorphism $\bar{\psi}$: $\bar{S} \to \widetilde{\mathbb{F}_q}$ and let $\psi = \bar{\psi} \circ \rho$. Then ψ: $S \to \widetilde{\mathbb{F}_q}$ extends φ, and, by Lemma 1.4(c), $\psi^*(\mathrm{Frob}) = \rho^*(\bar{\psi}^*(\mathrm{Frob}))$. If we show that the map $\bar{\varphi} \mapsto \bar{\varphi} \circ \pi$ is a bijection between

$$\overline{\mathbb{A}} = \{\bar{\varphi} \in \mathrm{Hom}_{\mathbb{F}_q}(\bar{R}, \mathbb{F}_q) |\ \mathrm{ar}(\bar{S}/\bar{R}, \bar{\varphi}) \subseteq \bar{\mathcal{C}}\}$$

and $\mathbb{A}$, then $N = |\overline{\mathbb{A}}|$.

Indeed, if $\bar{\varphi} \in \overline{\mathbb{A}}$, then

$$\psi^*(\mathrm{Frob}) = \rho^*(\bar{\psi}^*(\mathrm{Frob})) \in \rho^*(\mathrm{ar}(\bar{S}/\bar{R}, \bar{\varphi})) \subseteq \rho^*(\bar{\mathcal{C}}).$$

From the definition of $\bar{\mathcal{C}}$ above, $\psi^*(\mathrm{Frob}) \in \mathcal{C}$. Hence, $\varphi \in \mathbb{A}$. Conversely, if $\varphi \in \mathbb{A}$, let $\mathbf{a} = \varphi(\mathbf{x})$. Then $\mathbf{a} \in A(\mathbb{F}_q)$, and $\bar{\mathbf{x}} \to \mathbf{a}$ uniquely extends to an $\mathbb{F}_q$-homomorphism $\bar{\varphi}$: $\bar{R} \to \mathbb{F}_q$ such that $\varphi = \bar{\varphi} \circ \pi$. Now,

$$\rho^*(\bar{\psi}^*(\mathrm{Frob})) = \psi^*(\mathrm{Frob}) \in \mathrm{ar}(S/R, \varphi) = \mathcal{C}.$$

Since $\mathrm{res}_{\bar{L}} \psi^*(\mathrm{Frob}) = \mathrm{res}_{\bar{L}}\mathrm{Frob}$ (by (2) of Section 4), $\bar{\psi}^*(\mathrm{Frob}) \in \bar{\mathcal{C}}$. Thus $\bar{\varphi} \in \overline{\mathbb{A}}$.

The restriction of each element of $\bar{\mathcal{C}}$ to $\bar{L}$ is $\mathrm{res}_{\bar{L}}\mathrm{Frob}$. So, Theorem 4.4 gives the estimate

$$|N - \bar{c}q^r| \le \bar{c}(\bar{d}' - 1)(\bar{d}' - 2)q^{r-\frac{1}{2}} + \bar{c} \cdot \alpha(n', r, \bar{d}', \bar{\delta})q^{r-1}, \tag{9}$$

where $\bar{c} = \frac{|\bar{\mathcal{C}}|}{[\bar{F}:\bar{L}\,\bar{E}]}$, $n' = n + e$ and $\bar{d}' = d \cdot \deg(h)^e \le d \cdot \deg(h)^e = d'$. As α is nondecreasing, this together (8) gives the desired estimate. ∎

Remark 5.4: Good reduction. Let $(S_0/R_0,\ S/A)$ satisfy (1), (2), and (3). If it also satisfies condition (4), we say that $(S_0/R_0,\ S/A)$ has **good reduction** with respect to φ_0. Notice that (4) is an elementary statement about the parameters that define V, V_0, h, and g. So, if (R_0, S_0, A, S) satisfies (1), (2), and (3), constructive elimination of quantifiers for the theory of algebraically closed fields [FJ, Theorem 8.39] gives a nonzero element $r_0 \in R_0$ such that $(S_0[r_0^{-1}]/R_0[r_0^{-1}],\ S[r_0^{-1}]/A')$, where $A' = A - V(r_0)$, has good reduction with respect to each homomorphism φ: $R_0 \to \mathbb{F}_q$. ∎

6. Galois stratification

There are several slightly different definitions of the concept of Galois stratification ([FJ], [FS], [FHJ], [HJ], [J1], and elsewhere). All of them keep track of some objects attached to the Galois groups of Galois ring/set covers. In [FS] and [J1] these objects are conjugacy classes of elements, whereas in [FJ] they are conjugacy classes of subgroups of these groups. We use here the version of [FJ, Chapter 26] (over both a finite field and a localization of $\mathbb{Z}$). This may be the most accessible version. We recall the definition below.

To apply the preceding results about conjugacy classes of elements, we introduce the following notation. For a conjugacy class $\mathcal{C}$ of a group G, let $\widetilde{\mathcal{C}} = \{\langle\tau\rangle|\ \tau \in \mathcal{C}\}$. Observe that $\widetilde{\mathcal{C}}$ is a conjugacy class of subgroups of G; moreover, every conjugacy class of cyclic subgroups of G is of this form. A **conjugacy domain** $\mathcal{D}$ of subgroups of G is a union of conjugacy classes of subgroups of G. We say that $\mathcal{D}$ is **full** if $\mathcal{D}$ contains all subgroups of each group in $\mathcal{D}$.

Let Λ_0 denote either a localization $\mathbb{Z}[k_0^{-1}]$ of $\mathbb{Z}$ or a finite field $\mathbb{F}_{q_0}$. Let $\mathcal{F}(\Lambda_0)$ be the set of finite fields $\mathbb{F}_q$ for which there exists a homomorphism $\Lambda_0 \to \mathbb{F}_q$. In the first case $\mathcal{F}(\Lambda_0) = \{\mathbb{F}_q|\ q \text{ is relatively prime to } k_0\}$; in the second case $\mathcal{F}(\Lambda_0) = \{\mathbb{F}_q|\ q \text{ is a power of } q_0\}$.

A **Galois stratification** of the affine space $\mathbb{A}^n$ over Λ_0

$$\mathcal{B} = \langle \mathbb{A}^n,\ D_j/B_j,\ \mathrm{Con}(B_j)|\ j \in J\rangle \tag{1}$$

is a partition $\mathbb{A}^n = \dot\bigcup_{j\in J} B_j$ of $\mathbb{A}^n$ as a finite union of disjoint absolutely normal Λ_0-basic sets B_j, each equipped with a Galois ring/set cover D_j/B_j and with a conjugacy domain $\mathrm{Con}(B_j)$ of cyclic subgroups of $\mathcal{G}(D_j/B_j)$. Here 'disjoint' means that for each $\mathbb{F}_q \in \mathcal{F}(\Lambda_0)$ and for every $\mathbf{b} \in \mathbb{F}_q^n$ there is a unique $j = j(\mathbf{b}) \in J$ such that $\mathbf{b} \in B_j(\mathbb{F}_q)$.

A quantifier free **Galois formula** associated with $\mathcal{B}$ is an expression of the form $\mathrm{Ar}(\mathbf{X}) \subseteq \mathrm{Con}(\mathcal{B})$. This formula interpretes as follows. Let $\mathbb{F}_q \in \mathcal{F}(\Lambda_0)$, and let $\mathbf{b} \in \mathbb{F}_q^n$. Let $j = j(\mathbf{b})$. Then $\mathbb{F}_q \models \mathrm{Ar}(\mathbf{b}) \subseteq \mathrm{Con}(\mathcal{B})$ if and only if $\mathrm{Ar}(\mathbf{b}) \subseteq \mathrm{Con}(B_j)$.

The general Galois formulas are formed from quantifier free Galois formulas by quantification with the obvious interpretation.

Proposition 6.1: *For each Galois formula $\theta(\mathbf{X},\mathbf{Y}) = \theta(X_1,\dots,X_m,Y_1,\dots,Y_n)$ in $m+n$ free variables over Λ_0 we can effectively compute the following:*

(a) *positive integers k and q_1, such that $k \neq 0$ in Λ_0;*
(b) *a Galois stratification (1) of $\mathbb{A}^n$ over $\Lambda = \Lambda_0[k^{-1}]$; and*
(c) *for each $j \in J$ and for each conjugacy class $\mathcal{D}$ of cyclic subgroups of $\mathcal{G}(D_j/B_j)$, an integer $0 \leq r = r(j,\mathcal{D}) \leq m$, and rational numbers $\varepsilon = \varepsilon(j,\mathcal{D}) \geq 0, \mu = \mu(j,\mathcal{D})$,*

such that if $\mathbb{F}_q \in \mathcal{F}(\Lambda)$ with $q \geq q_1$, $\mathbf{b} \in B_j(\mathbb{F}_q)$ and $\mathrm{Ar}(D_j/B_j, \mathbb{F}_q, \mathbf{b}) = \mathcal{D}$ (Definition 2.6), then $N_q(\mathbf{b}) = |\{\mathbf{a} \in \mathbb{F}_q^m | \, \mathbb{F}_q \models \theta(\mathbf{a},\mathbf{b})\}|$ satisfies

$$|N_q(\mathbf{b}) - \mu q^r| \leq \mu\varepsilon q^{r-\frac{1}{2}}. \tag{2}$$

Moreover, $\mu = 0$ if and only if $\mathcal{D} \not\subseteq \mathrm{Con}(B_j)$.

Proof: Apply [FJ, Prop. 26.7 and Prop. 26.8] to compute k and q_1 in $\mathbb{N}$, and a quantifier free Galois formula θ', which is equivalent to θ for all $\mathbb{F}_q \in \mathcal{F}(\Lambda_0[k^{-1}])$ with $q \geq q_1$. Thus we may assume that θ is quantifier free. Let

$$\mathcal{A} = \langle \mathbb{A}^{m+n}, \ C_i/A_i, \ \mathrm{Con}(A_i) | \, i \in I \rangle \tag{3}$$

be the Galois stratification of $\mathbb{A}^{m+n}$ over Λ that corresponds to θ. The conjugacy domains $\mathrm{Con}(A_i)$ consist of cyclic groups. Take $\pi\colon \mathbb{A}^{m+n} \to \mathbb{A}^n$ to be the projection on the first n coordinates.

Use the Stratification Lemma [FJ, Lemma 17.26], as in the proof of [FJ, Lemma 25.6], to replace $\mathcal{A}$ by an appropriate refinement (possibly multiplying k by another factor) and to construct a Galois stratification (1) of $\mathbb{A}^n$ over Λ with the following properties.

For each $j \in J$ the set B_j is absolutely Λ-normal (see Lemma 2.4(b)),
each absolutely irreducible component of B_j is defined by polynomials with coefficients integral over Λ,
$\pi^{-1}(B_j) = \bigcup_{i \in I(j)} A_i$, and $\pi(A_i) = B_j$ for each $i \in I(j)$.

We may also assume that $D_j \subseteq C_i$ for each $i \in I(j)$; otherwise replace C_i by $C_i' = C_iD_j$ (use the Stratification Lemma once more to make C_i'/A_i a Galois cover), and $\mathrm{Con}(A_i)$ by the collection of all cyclic subgroups of $\mathcal{G}(C_i'/A_i)$ whose restrictions to C_i are in $\mathrm{Con}(A_i)$. Moreover, $(D_j/\Lambda[B_j], \ C_i/A_i)$ has good reduction with respect to each homomorphism $\Lambda \to \mathbb{F}_q$ (Remark 5.4), for each $i \in I(j)$. Furthermore, set

$$\mathrm{Con}(B_j) = \bigcup_{i \in I(j)} \mathrm{Con}_{\mathcal{G}(L_j/K_j)}(\mathrm{res}_{L_j} \mathrm{Con}(A_i)), \tag{4}$$

where L_j/K_j is the Galois extension of the quotient fields corresponding to the cover D_j/B_j. Then $\mathrm{Con}(B_j)$ also consists of cyclic groups. For later use we observe that if $\mathrm{Con}(A_i)$ is full, for each $i \in I(j)$, then $\mathrm{Con}(B_j)$ is also full.

Let now $j \in J$ and let $\mathcal{D}$ be a conjugacy class of cyclic subgroups of $\mathcal{G}(D_j/B_j)$. Let $\mathbb{F}_q \in \mathcal{F}(\Lambda)$ with $q \geq q_1$ and $\mathbf{b} \in B_j(\mathbb{F}_q)$ such that $\mathrm{Ar}(D_j/B_j, \mathbf{b}) = \mathcal{D}$. For $i \in I(j)$ and for a conjugacy class $\mathcal{C} \subseteq \mathcal{G}(C_i/A_i)$ denote

$$P(\mathcal{C}, \mathbf{b}) = \{(\mathbf{a}, \mathbf{b}) \in A_i(\mathbb{F}_q) |\ \mathrm{ar}(C_i/A_i, (\mathbf{a}, \mathbf{b})) = \mathcal{C}\} \quad \text{and} \quad N_{q,i,\mathcal{C}} = |P(\mathcal{C}, \mathbf{b})|.$$

By the choice of $\mathcal{A}$, for each $i \in I$ and for each $(\mathbf{a}, \mathbf{b}) \in A_i(\mathbb{F}_q)$ we have $\mathbb{F}_q \models \theta(\mathbf{a}, \mathbf{b})$ if and only if $\mathrm{Ar}(C_i/A_i, (\mathbf{a}, \mathbf{b})) \subseteq \mathrm{Con}(A_i)$. By definition (Section 1), $\mathrm{ar}(C_i/A_i, (\mathbf{a}, \mathbf{b})) = \mathcal{C}$ implies $\mathrm{Ar}(C_i/A_i, (\mathbf{a}, \mathbf{b})) = \tilde{\mathcal{C}}$. Hence,

$$\{(\mathbf{a}, \mathbf{b}) \in \mathbb{F}_q^{m+n} |\ \mathbb{F}_q \models \theta(\mathbf{a}, \mathbf{b})\} = \dot{\bigcup_{i \in I(j)}} \dot{\bigcup_{\substack{\mathcal{C} \\ \tilde{\mathcal{C}} \subseteq \mathrm{Con}(A_i)}}} P(\mathcal{C}, \mathbf{b}),$$

and therefore

$$N_q(\mathbf{b}) = \sum_{i \in I(j)} \sum_{\substack{\mathcal{C} \\ \tilde{\mathcal{C}} \subseteq \mathrm{Con}(A_i)}} N_{q,i,\mathcal{C}}. \tag{5}$$

However, if $\mathrm{res}_{L_j} \mathcal{C} \not\subseteq \mathrm{ar}(D_j/B_j, \mathbf{b})$, then $N_{q,i,\mathcal{C}} = 0$ by Theorem 5.3. This happens, in particular, if $\mathrm{res}_{L_j} \tilde{\mathcal{C}} \not\subseteq \mathcal{D}$. Hence,

$$N_q(\mathbf{b}) = \sum_{(i,\mathcal{C}) \in \Omega} N_{q,i,\mathcal{C}}, \tag{5'}$$

where

$$\Omega = \{(i, \mathcal{C}) |\ i \in I(j),\ \tilde{\mathcal{C}} \subseteq \mathrm{Con}(A_i),\ \mathrm{res}_{L_j} \tilde{\mathcal{C}} \subseteq \mathcal{D}\}.$$

Thus $\Omega = \emptyset$ if and only if $\mathcal{D} \not\subseteq \mathrm{Con}(B_j)$. In this case $N_q(\mathbf{b}) = 0$, and we set $\mu = \varepsilon = 0$ in (2). Assume therefore that $\Omega \neq \emptyset$. Let

$$r = \max\{\dim_{K_j}(A_i) |\ (i, \mathcal{C}) \in \Omega\}.$$

It suffices for each $(i, \mathcal{C}) \in \Omega$ to find rational numbers $\mu_{i,\mathcal{C}} \geq 0$, $\varepsilon_{i,\mathcal{C}} \geq 0$, independent of q and $\mathbf{b}$, such that

$$|N_{q,i,\mathcal{C}} - \mu_{i,\mathcal{C}} q^r| \leq \varepsilon_{i,\mathcal{C}} q^{r - \frac{1}{2}}, \tag{6}$$

and $\mu_{i,\mathcal{C}} > 0$ for at least one $(i,\mathcal{C}) \in \Omega$. Once this has been done, then from (5′),

$$|N_q(\mathbf{b}) - \sum_{(i,\mathcal{C})\in\Omega} \mu_{i,\mathcal{C}} q^r| \le \sum_{(i,\mathcal{C})\in\Omega} \varepsilon_{i,\mathcal{C}} q^{r-\frac{1}{2}}.$$

Set $\mu = \sum \mu_{i,\mathcal{C}}$ and $\varepsilon = (1/\mu)\sum \varepsilon_{i,\mathcal{C}}$ in (2). These are independent of q and $\mathbf{b}$.

Fix $(i,\mathcal{C}) \in \Omega$. Theorem 5.3 applies to the pair $(C_i/A_i,\ D_j/B_j)$ and the class $\mathcal{C}$. More precisely, let $(F/E,\ L/K)$ be the pair of Galois extensions of the corresponding quotient fields, and let K' be the algebraic closure of K in E. Let $r_i = \dim(A_i)$, $d = \deg(A_i)$, and let δ be the complementary degree of A_i. Put $G_0 = \mathcal{G}(D_j/B_j) = \mathcal{G}(L/K)$ and $G_0' = \mathcal{G}(L/K')$. Let $\mathcal{C}_0' = \mathrm{res}_L\mathcal{C}$ and $\mathcal{C}_0 = \mathrm{Con}_{G_0}\mathcal{C}_0'$. Let e be the exponent of $\mathcal{C}$, and $d' = d\cdot[F : LE]^e$. Then let

$$\beta = [K' : K]\frac{|G_0' \cap \mathcal{C}_0|}{|\mathcal{C}_0|} \qquad \text{and} \qquad \gamma = \frac{|\mathcal{C}|}{[F : LE]}\frac{1}{|\mathcal{C}_0'|}\ .$$

There are two cases to consider:

(7a) $r_i = r$. Then by Theorem 5.3

$$\begin{aligned}|N_{q,i,\mathcal{C}} - \beta\gamma q^r| \le& \beta\gamma(d'-1)(d'-2)q^{r-\frac{1}{2}} + \beta\gamma\cdot\alpha(m+n+e,r,d',\delta)q^{r-1}\\ &\le \beta\gamma\big((d'-1)(d'-2) + \alpha(m+n+e,r,d',\delta)\big)q^{r-\frac{1}{2}}\ .\end{aligned}$$

Notice that $\beta > 0$, $\gamma > 0$. By the definition of r, this case occurs for at least one $(i,\mathcal{C}) \in \Omega$.

(7b) $r_i < r$. Clearly $N_{q,i,\mathcal{C}} \le |\bar{A}_i(\mathbb{F}_q)|$, where $\bar{A}_i$ is the Zariski closure of A_i. By Lemma 3.1(a), $|\bar{A}_i(\mathbb{F}_q)| \le dq^{r_i} \le dq^{r-1}$. Thus

$$|N_{q,i,\mathcal{C}} - 0\cdot q^r| \le dq^{r-\frac{1}{2}}. \qquad \blacksquare$$

Remarks 6.2: (a) Proposition 6.1 is also true, if $\theta = \theta(\mathbf{X},\mathbf{Y})$ is a formula in the language of rings. Indeed, by [FJ, p. 425] we can compute $k_1 \in \mathbb{Z}$ and a Galois formula $\theta'(\mathbf{X},\mathbf{Y})$ over $\mathbb{Z}[k_1^{-1}]$, which is equivalent to θ over each $\mathbb{F}_q$ with q prime to k_1. Thus if $\Lambda_0 = \mathbb{Z}[k_0^{-1}]$, apply Proposition 6.1 to θ' over $\Lambda_0[k_1^{-1}]$. If Λ_0 is a field, then by [FJ, Remark 25.8] we can compute a Galois formula $\theta''(\mathbf{X},\mathbf{Y})$ over Λ_0, which is equivalent to θ over each extension $\mathbb{F}_q$ of Λ_0. Now apply Proposition 6.1 to θ''.

Both θ' and θ'' have the same quantifier prefix as θ. The groups of the Galois stratifications associated with θ' and θ'' are of order 1.

(b) Assume that $\theta(\mathbf{X},\mathbf{Y})$ is a quantifier free Galois formula. Proposition 6.1 says that (for suitable k and q_1) we have $N_q(\mathbf{b})>0$ if and only if $\mathbf{b}$ satisfies the quantifier free Galois formula $\theta'(\mathbf{Y})$ associated with $\mathcal{B}$. In other words, $(\exists\mathbf{X})\theta(\mathbf{X},\mathbf{Y})$ is equivalent to $\theta'(\mathbf{Y})$. In this way we get an eliminaton procedure for the theory of finite fields in the language of Galois formulas. This algorithm eliminates a block of quantifiers at each step, as in the original procedure of [FS], rather than only one quantifier at a time as in [FJ]. ∎

LEMMA 6.3: *Let D/B be a Galois cover over Λ_0. Assume that*

$$B=V(f_1,\dots,f_m)-V(g)\subseteq\mathbb{A}^n,$$

where $f_1,\dots,f_m,g\in\mathbb{Z}[\mathbf{Y}]$. For each conjugacy domain $\mathcal{D}$ of cyclic subgroups of $\mathcal{G}(D/B)$ there is a formula $\theta_{\mathcal{D}}(\mathbf{Y})$ in the language of rings, such that for every $\mathbb{F}_q\in\mathcal{F}(\Lambda_0)$

$$\{\mathbf{b}\in B(\mathbb{F}_q)|\ \mathrm{Ar}(D/B,\mathbb{F}_q,\mathbf{b})\subseteq\mathcal{D}\}=\{\mathbf{b}\in\mathbb{F}_q^n|\ \mathbb{F}_q\models\theta_{\mathcal{D}}(\mathbf{b})\}. \tag{8}$$

Moreover, if $\mathcal{D}$ is full, there is $h(\mathbf{Y},Z)\in\mathbb{Z}[\mathbf{Y},Z]$ such that $\theta_{\mathcal{D}}(\mathbf{Y})$ can be taken to be

$$\bigwedge_{i=1}^{m}f_i(\mathbf{Y})=0\wedge g(\mathbf{Y})\neq 0\wedge(\exists Z)h(\mathbf{Y},Z)=0. \tag{9}$$

Proof: It suffices to prove the assertion for $\mathcal{D}$ full. Indeed, if $\mathcal{D}$ is a single conjugacy class of groups, then $\mathcal{D}=\mathcal{D}'-\mathcal{D}''$, where $\mathcal{D}'$ is the conjugacy domain of all subgroups of the groups in $\mathcal{D}$, and $\mathcal{D}''$ is the conjugacy domain of all proper subgroups of the groups in $\mathcal{D}$. Then put $\theta_{\mathcal{D}}=\theta_{\mathcal{D}'}\wedge\neg\theta_{\mathcal{D}''}$. In the general case write $\mathcal{D}$ as a union of conjugacy classes $\bigcup\mathcal{C}$, and put $\theta_{\mathcal{D}}=\bigvee\theta_{\mathcal{C}}$.

So assume that $\mathcal{D}$ is full. Let $\mathbf{y}$ be a generic point of $V(f_1,\dots,f_m)$ over the quotient field of Λ_0. Thus $\Lambda_0[B]=\Lambda_0[\mathbf{y},g(\mathbf{y})^{-1}]$. Let F/E be the extension of quotient fields corresponding to D/B. For each subgroup H of $\mathcal{G}(D/B)$ fix $\zeta_H\in D$, such that $E(\zeta_H)$ is the fixed field of H in F, and such that $\zeta_{H^\sigma}=(\zeta_H)^\sigma$, for all $\sigma\in\mathcal{G}(D/B)$. We may take ζ_H integral over $\Lambda_0[\mathbf{y}]$ and, if Λ_0 is a localization of $\mathbb{Z}$, even integral over $\mathbb{Z}[\mathbf{y}]$. For each conjugacy class $\mathcal{C}$ of subgroups of $\mathcal{G}(D/B)$ let $h_{\mathcal{C}}(\mathbf{Y},Z)\in\mathbb{Z}[\mathbf{Y},Z]$ such that $h_{\mathcal{C}}(\mathbf{y},Z)=\mathrm{irr}(\zeta_H,E)$ for each $H\in\mathcal{C}$. Then let $h_{\mathcal{C}}(\mathbf{y},Z)=\prod_{H\in\mathcal{C}}(Z-\zeta_H)$. Finally let $h=\prod_{\mathcal{C}}h_{\mathcal{C}}(\mathbf{Y},Z)$, where $\mathcal{C}$ runs through the conjugacy classes of maximal subgroups in $\mathcal{D}$.

We show that h has the required property. Let $\mathbb{F}_q \in \mathcal{F}(\Lambda_0)$, and let $\mathbf{b} \in B(\mathbb{F}_q)$. The specialization $\mathbf{y} \mapsto \mathbf{b}$ gives rise to a homomorphism ψ: $D \to \widetilde{\mathbb{F}_q}$ such that $\psi(\Lambda_0[B]) \subseteq \mathbb{F}_q$. We have to show that $\psi(h)(\mathbf{b}, Z)$ has a root in $\mathbb{F}_q$ if and only if $\psi^*(G(\mathbb{F}_q)) \in \mathcal{D}$. The first of these two conditions says that there is a maximal $H \in \mathcal{D}$ such that $\psi(\zeta_H) \in \mathbb{F}_q$. As $\mathcal{D}$ is full, the second condition says that there is a maximal $H \in \mathcal{D}$ such that $\psi^*(G(\mathbb{F}_q)) \leq H$. But for every $H \leq \mathcal{G}(D/B)$ we have $\psi(\zeta_H) \in \mathbb{F}_q$ if and only if $\psi^*(G(\mathbb{F}_q))$ fixes ζ_H, that is, $\psi^*(G(\mathbb{F}_q)) \leq H$. Thus the two conditions are equivalent. ∎

Theorem 6.4: *For each formula $\theta(\mathbf{X}, \mathbf{Y}) = \theta(X_1, \ldots, X_m, Y_1, \ldots, Y_n)$ in $m+n$ free variables in the first order language of rings we can effectively compute a finite set $\{(\theta_i, \mu_i, \epsilon_i, r_i) |\ i \in I\}$ with the following properties.*

(a) *$\theta_i(\mathbf{Y})$ is a formula in the language of rings, $\mu_i > 0$ and $\epsilon_i \geq 0$ are rational numbers, and $r_i \in \{0, \ldots, n\}$, for each $i \in I$.*

(b) *For each finite field $\mathbb{F}_q$ and each $\mathbf{b} \in \mathbb{F}_q^n$ there exists a unique $i \in I$ such that $\mathbb{F}_q \models \theta_i(\mathbf{b})$.*

(c) *The number $N_q(\mathbf{b}) = |\{\mathbf{a} \in \mathbb{F}_q^m |\ \mathbb{F}_q \models \theta(\mathbf{a}, \mathbf{b})\}|$ satisfies*

$$|N_q(\mathbf{b}) - \mu_i q^{r_i}| \leq \mu_i \varepsilon_i q^{r_i - \frac{1}{2}} \tag{10}$$

Proof: By Proposition 6.1 and Remark 6.2(a) we can compute $k \in \mathbb{Z}$, a Galois stratification (1) over $\mathbb{Z}[k^{-1}]$, and numbers r_i, μ_i, and ε_i for each i in the set

$$I_k = \{(j, \mathcal{D}) |\ j \in J,\ \mathcal{D} \text{ is a conjugacy class of subgroups of } \mathcal{G}(D_j/B_j)\},$$

with the following property. Given $i = (j, \mathcal{D}) \in I_k$, q prime to k, and $\mathbf{b} \in B_j(\mathbb{F}_q)$ such that $\mathrm{Ar}(D_j/B_j, \mathbb{F}_q, \mathbf{b}) = \mathcal{D}$, we have $|N_q(\mathbf{b}) - \mu_i q^{r_i}| \leq \mu_i \varepsilon_i q^{r_i - \frac{1}{2}}$. By Lemma 6.3 we find a formula $\theta_i = \theta_{\mathcal{D}}$, for each $i \in I_k$, such that (8) holds for q, $\mathbf{b}$ as above. Then (a), (b), and (c) hold for every q prime to k. Without loss of generality, each θ_i holds only for such q's, (replace θ_i by $\theta_i \wedge k{\neq}0$).

Observe that if $\mathcal{D}$ is full, then θ_i has the form (9). Replacing $g(\mathbf{Y}) \neq 0$ by $(\exists Z) Z \cdot g(\mathbf{Y}) = 1$, we can write θ_i as $\bigwedge_{s \in S(i)} (\exists Z) h_{is}(\mathbf{Y}, Z) = 0$, with $h_{is}(\mathbf{Y}, Z) \in \mathbb{Z}[\mathbf{Y}, Z]$.

Let p be a prime. Put $\Lambda_0 = \mathbb{F}_p$. By Proposition 6.1, Remark 6.2(a), and Lemma 6.3 we can compute an integer $\nu(p) \geq 1$ and a finite set $\{(\theta_i, \mu_i, \epsilon_i, r_i) |\ i \in I'_p\}$, such that (a), (b), and (c) hold for every $q = p^\nu$ with $\nu \geq \nu(p)$. Without loss of generality, each θ_i holds only for such q's; otherwise replace θ_i by

$\theta_i \wedge p{=}0 \wedge (\exists Z) f(Z){=}0$, where $f(Z) = \frac{Z^{\nu(p)}-Z}{Z^{\nu(p)-1}-Z} \in \mathbb{Z}[Z]$. Again, if $\mathcal{D}$ is full, then θ_i is $\bigwedge_{s\in S(i)}(\exists Z)h_{is}(\mathbf{Y},Z)=0$, with $h_{is}(\mathbf{Y},Z)\in\mathbb{Z}[\mathbf{Y},Z]$.

Let q be a power of a prime p, say $q=p^\nu$. Find a finite set $\{(\theta_i,\mu_i,\epsilon_i,r_i)|\ i\in I'_{p,\nu}\}$, such that (a), (b), (c) hold for this q. Without loss of generality, each θ_i holds only for this q, otherwise replace θ_i by $\theta_i\wedge\lambda_q$, where λ_q says that the field has exactly q elements.

Let $I = I_k \cup \bigcup_{p|k} I'_p \cup \bigcup_{p|k}\bigcup_{\nu<\nu(p)} I'_{p,\nu}$. The set $\{(\theta_i,\mu_i,\epsilon_i,r_i)|\ i\in I\}$ clearly satisfies the requirements of the theorem. ∎

If θ is quantifier free, we can say more about the θ_i's. Let us follow the above proof more carefully in this case.

First, use Remark 6.2(a) to replace θ by a Galois formula. The groups of the corresponding Galois stratification $\mathcal{A}$ are trivial. Apply the proof of Proposition 6.1. There we have first to replace $\mathcal{A}$ by a refinement. Thus for each Galois cover C/A in $\mathcal{A}$ either $\mathrm{Con}(A)$ is empty or consists of all cyclic subgroups of $\mathcal{G}(C/A)$; in particular, $\mathrm{Con}(A)$ is full. By (4) the conjugacy domains $\mathrm{Con}(B_j)$ of $\mathcal{B}$ are full. Therefore for $i\in I_k$ and for $i\in I'_p$ we can write the formula θ_i as $\bigwedge_{s\in S(i)}(\exists Z)h_{is}(\mathbf{Y},Z)=0$, with $h_{is}(\mathbf{Y},Z)\in\mathbb{Z}[\mathbf{Y},Z]$. with $h_{is}(\mathbf{Y},Z)\in\mathbb{Z}[\mathbf{Y},Z]$.

Put $I' = \{i\in I_k\cup\bigcup_{p|k}I'_p|\ \mu_i>0\}$. Then for almost all finite fields $\mathbb{F}_q$, and all $\mathbf{b}\in\mathbb{F}_q^n$ we have $N_q(\mathbf{b})\ge 1$ if an only if $\mathbb{F}_q\models\bigvee_{i\in I'}\theta_i(\mathbf{b})$. Therefore the existential formula $(\exists\mathbf{X})\theta(\mathbf{X},\mathbf{Y})$ is equivalent to $\bigvee_{i\in I'}\theta_i(\mathbf{Y})$, for almost all finite fields. The latter formula can be written as $\bigwedge_f(\exists Z)\prod_{i\in I'}h_{if(i)}(\mathbf{Y},Z)=0$, where f ranges over the set $\prod_{i\in I'}S(i)$.

This gives the following result of van den Dries:

THEOREM 6.5 ([D], (3.4)): *Let $\theta(\mathbf{X},\mathbf{Y})$ be a quantifier free formula in the language of rings. There exist $g_1,\dots,g_r\in\mathbb{Z}[\mathbf{Y},Z]$ (here Z is a single variable) such that $(\exists\mathbf{X})\theta(\mathbf{X},\mathbf{Y})\}$ is equivalent to $\bigwedge_i^r(\exists Z)g_i(\mathbf{Y},Z)=0$ for all sufficiently large finite fields.*

Remark 6.6: There exists a stronger variant of Galois stratification, in which conjugacy domains of elements are used instead of conjugacy domains of subgroups (see [FS], [J1] or [HJ]). Everywhere replace 'Ar' by 'ar' and '$\tilde{\mathcal{C}}$' by '$\mathcal{C}$', and let $\mathcal{D}$ be a conjugacy class of $\mathcal{G}(D_j/B_j)$. Then the assertion and the proof of Proposition 6.1 go through. This variant of Proposition 6.1 is strictly stronger than Theorem 6.3. This is because there are Galois formulas in this stronger language that are not equivalent to formulas in the language of rings [HJ, Corollary

1.12]. ∎

As an application consider the following result (cf. [W, Theorem 1.3]).

THEOREM 6.7: *Let $\theta(\mathbf{X}) = \theta(X_1, \ldots, X_m)$ be a formula in m free variables in the language of rings augmented by elements of a finite field $\mathbb{F}_q$ (or a Galois formula over $\mathbb{F}_q$). Let $N^{(k)} = |\{\mathbf{a} \in \mathbb{F}_{q^k}^m | \ \mathbb{F}_{q^k} \models \theta(\mathbf{a})\}|$. Then there is an a periodic sequence of numbers (r_k, μ_k), where $0 \le r_k \le m$ are integers and $0 \le \mu_k \in \mathbb{Q}$, such that*

$$N^{(k)} = \mu_k q^{kr_k} + O(q^{k(r_k - \frac{1}{2})}).$$

Proof: By [FJ, Remark 25.8] we may assume that θ is a Galois formula. By Proposition 6.1 (with $n = 0$), there exist $q_1 \ge 1$, a finite (cyclic) Galois extension $L/\mathbb{F}_q$, a set of subgroups Con of $\mathcal{G}(L/\mathbb{F}_q)$, and for each $H \le \mathcal{G}(L/\mathbb{F}_q)$ an integer $0 \le r_H \le m$ and rational numbers $\mu_H, \varepsilon_H \ge 0$, such that if $q^k \ge q_1$ and $\mathcal{G}(L/(L \cap \mathbb{F}_{q^k})) = H$, then

$$|N^{(k)} - \mu_H q^{r_H}| \le \mu_H \varepsilon_H q^{r_H - \frac{1}{2}}. \tag{11}$$

Let τ be the Frobenius automorphism of $\mathbb{F}_q$. Then $G(\mathbb{F}_{q^k}) = \langle \tau^k \rangle$, and hence $\mathcal{G}(L/(L \cap \mathbb{F}_{q^k})) = \langle \mathrm{res}_L \tau^k \rangle$. In particular, (11) holds, if $\langle (\mathrm{res}_L \tau)^k \rangle = H$. This condition is periodic modulo $[L : \mathbb{F}_q]$. ∎

References

[CDM] Z. Chatzidakis, L. van den Dries, and A. Macintyre, *Definable sets over finite fields,* to appear in Journal für die reine und angewandte Mathematik.

[D] L. van den Dries, *A remark on Ax' theorem on solvability modulo primes,* Mathematische Zeitschrift **208** (1991), 65–70.

[FHJ] M.D. Fried, D. Haran and M. Jarden, *Galois stratification over Frobenius fields,* Advances of Mathematics **51** (1984), 1–35.

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

[FS] M.D. Fried and G. Sacerdote, *Solving diophantine problems over all residue class fields of a number field and all finite fields,* Annals of Mathematics **104** (1976), 203–233.

[HJ] D. Haran and M. Jarden, *Bounded statements in the theory of algebraically closed fields with distinguished automorphisms,* Journal für die reine und angewandte Mathematik **337** (1982), 1–17.

[H] R. Hartshorne, *Algebraic Geometry*, Graduate Texts in Mathematics **52**, Springer, New York, 1977.

[J1] M. Jarden, *Galois stratification for the elementary theory of finite prime fields*, a manuscript, Tel Aviv, 1990.

[J2] M. Jarden, *Algebraic dimension over Frobenius fields*, to appear in Forum Mathematicum.

[L] S. Lang, *Algebra*, Addison-Wesley, Reading, 1970.

[Li] W. Litz, *Die Anzahl der rationalen Punkte von Varietäten über einem endlichen Körper*, Diplomarbeit, Heidelberg, 1975.

[LW] S. Lang and A. Weil, *Number of points of varieties in finite fields*, American Journal of Mathematics **76** (1954), 819–827.

[M] H. Matsumura, *Commutative Algebra*, second edition, Benjamin/Cummings, Reading, Mass., 1980.

[R] M. Raynaud, *Anneaux Locaux Henséliens*, LNM **169**, Springer, New York, 1970.

[W] D. Wan, *Hilbert sets and zeta function over finite fields*, to appear in Journal für die reine und angewandte Mathematik.

[ZS] O. Zariski and P. Samuel, *Commutative Algebra II*, Springer, New York, 1975.