Journal of Computer and System Sciences **62**, 216–235 (2001)
doi:10.1006/jcss.2000.1728, available online at http://www.idealibrary.com on IDEAL®

Computational Arithmetic Geometry

J. Maurice Rojas

Department of Mathematics, City University of Hong Kong, 83 Tat Chee Avenue, Kowloon, Hong Kong, China; and Department of Mathematics, Texas A&M University, College Station, Texas 77843
E-mail: rojas@math.tamu.edu
URL: http://www.math.tamu.edu/~rojas

Received June 23, 1999

THIS PAPER IS DEDICATED TO GRETCHEN DAVIS

We consider the average-case complexity of some otherwise undecidable or open Diophantine problems. More precisely, consider the following:

I. Given a polynomial $f \in \mathbb{Z}[v, x, y]$, decide the sentence $\exists v \, \forall x \, \exists y f(v, x, y) \stackrel{?}{=} 0$, with all three quantifiers ranging over $\mathbb{N}$ (or $\mathbb{Z}$).

II. Given polynomials $f_1, ..., f_m \in \mathbb{Z}[x_1, ..., x_n]$ with $m \geqslant n$, decide if there is a *rational* solution to $f_1 = \cdots = f_m = 0$.

We show that, for almost all inputs, problem (I) can be done within **coNP**. The decidability of problem (I), over $\mathbb{N}$ and $\mathbb{Z}$, was previously unknown. We also show that the *Generalized Riemann Hypothesis* (*GRH*) implies that, for almost all inputs, problem (II) can be done via within the complexity class $\mathbf{P}^{\mathbf{NP}^{\mathbf{NP}}}$, i.e., within the third level of the polynomial hierarchy. The decidability of problem (II), even in the case $m = n = 2$, remains open in general. Along the way, we prove results relating polynomial system solving over $\mathbb{C}$, $\mathbb{Q}$, and $\mathbb{Z}/p\mathbb{Z}$. We also prove a result on Galois groups associated to sparse polynomial systems, which may be of independent interest. A practical observation is that the aforementioned Diophantine problems should perhaps be avoided in the construction of cryptosystems.

1. INTRODUCTION AND MAIN RESULTS

The negative solution of Hilbert's Tenth Problem [Mat70, Mat93] has all but dashed earlier hopes of solving large polynomial systems over the integers. However, an immediate positive consequence is the creation of a rich and diverse garden of hard problems with potential applications in complexity theory, cryptology, and

[1] An extended abstract of this work appeared earlier in the "Proceedings of the 31st Annual ACM Symposium on Theory of Computing (STOC, May 1–4, 1999, Atlanta, Georgia)," pp. 527–536, ACM Press, 1999. This research was partially funded by a Hong Kong CERG Grant.

0022-0000/01 $35.00

logic. Even more compelling is the question of where the boundary to decidability lies.

From high school algebra we know that detecting and even finding roots in $\mathbb{Q}$ (or $\mathbb{Z}$ or $\mathbb{N}$) for polynomials in $\mathbb{Z}[x_1]$ is tractable. (We respectively use $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{Z}$, and $\mathbb{N}$ for the complex numbers, real numbers, rational numbers, integers, and positive integers.) However, in [Jon82], Jones showed that detecting roots in $\mathbb{N}^9$ for polynomials in $\mathbb{Z}[x_1, ..., x_9]$ is already undecidable. Put another way, this means that determining the existence of a positive integral point on a general algebraic hypersurface of (complex) dimension 8 is undecidable.

It then comes as quite a shock that decades of number theory still have not settled the complexity of the analogous question for algebraic sets of dimension 1 through 7. In fact, even the case of plane curves remains a mystery:[2] As of early 2001, the decidability of detecting a root in $\mathbb{N}^2$, $\mathbb{Z}^2$, or even $\mathbb{Q}^2$, for an *arbitrary* polynomial in $\mathbb{Z}[x_1, x_2]$, is still completely open.

1.1. Dimensions One and Two

To reconsider the complexity of detecting integral points on algebraic sets of dimension $\geqslant 1$, one can consider subtler combinations of quantifiers, and thus subtler questions on the disposition of integral roots, to facilitate finding decisive results. For example, Matiyasevich and Julia Robinson have shown [MR74, Jon81] that sentences of the form $\exists u\, \exists v\, \forall x\, \exists x\, \exists y f(u, v, x, y) \stackrel{?}{=} 0$ (quantified over $\mathbb{N}$), for *arbitrary* input $f \in \mathbb{Z}[u, v, x, y]$, are already undecidable. As another example of the richnes's of Diophantine sentences, Adleman and Manders have shown that deciding a very special case of the prefix $\exists\, \exists$ (quantified over $\mathbb{N}$) is **NP**-complete [AM75]: they show **NP**-completeness for the set of $(a, b, c) \in \mathbb{N}^3$ such that $ax^2 + by = c$ has a solution $(x, y) \in \mathbb{N}^2$.

However, the decidability of sentences of the form $\exists v\, \forall x\, \exists y f(v, x, y) \stackrel{?}{=} 0$ (quantified over $\mathbb{N}$ or $\mathbb{Z}$) was an open question—until recently: In [Roj00a] it was shown that (over $\mathbb{N}$) these sentences can be decided by a Turing machine, once the input f is suitably restricted. Roughly speaking, deciding the prefix $\exists\, \forall\, \exists$ is equivalent to determining whether an algebraic surface has a slice (parallel to the (x, y)-plane) densely peppered with integral points. The "exceptional" f not covered by the algorithm of [Roj00a] form a very slim subset of $\mathbb{Z}[v, x, y]$.

We will further improve this result by showing that, under similarly mild input restrictions, $\exists\, \forall\, \exists$ can in fact be decided within **coNP**. (This improves a **PSPACE** bound which appeared earlier in the proceedings version of this paper [Roj99a].) To make this more precise, let us write any $f \in \mathbb{Z}[v, x, y]$ as $f(v, x, y) = \sum c_a v^{a_1} x^{a_2} y^{a_3}$, where the sum is over certain $a := (a_1, a_2, a_3) \in \mathbb{Z}^3$. We then define the *Newton polytope of* f, **Newt(*f*)**, as the convex hull of[3] $\{a \mid c_a \neq 0\}$. Also, when we say that a statement involving a set of parameters $\{c_1, ..., c_N\}$ is true *generically*,[4] we will mean that for any $M \in \mathbb{N}$, the statement fails for at most

[2] In particular, the major "solved" special cases so far have only extremely ineffective complexity and height bounds. (See, e.g., the introduction and references of [Roj00a].)

[3] I.e., smallest convex set in $\mathbb{R}^3$ containing....

[4] We can in fact assert a much stronger condition, but this one suffices for our present purposes.

$\mathcal{O}(N(2M+1)^{N-1})$ of the $(c_1, ..., c_N)$ lying in $\{-M, ..., M\}^N$. Finally, for an algorithm with a polynomial $f \in \mathbb{Z}[v, x, y]$ as input, speaking of the *dense encoding* will simply mean measuring the input size as $d + \sigma(f)$, where d (resp. $\sigma(f)$) is the total degree[5] (resp. maximum bit-length of a coefficient) of f.

THEOREM 1. *Fix the Newton polytope P of a polynomial $f \in \mathbb{Z}[v, x, y]$ and suppose that P has at least one integral point in its interior. Assume further that we measure input size via the dense encoding. Then, for a generic choice of coefficients depending only on P, we can decide whether $\exists v \forall x \exists y f(v, x, y) = 0$ (with all three quantifiers ranging over $\mathbb{N}$ or $\mathbb{Z}$) within* **coNP**. *Furthermore, we can check whether an input f has generic coefficients within* **NC**.

Remark 1. It is an open question whether membership in **coNP** for the problem above continues to hold relative to the *sparse* encoding. We will describe the latter encoding shortly. Recall also that $\mathbf{NC} \subseteq \mathbf{P} \subseteq \mathbf{coNP}$, and the properness of each inclusion is unknown [Pap95].

The generic choice above is clarified further in Section 3. It is interesting to note that the exceptional case to our algorithm for $\exists \forall \exists$ judiciously contains an extremely hard number-theoretic problem: determining the existence of a point in $\mathbb{N}^2$ on an algebraic plane curve. (That $\mathbb{Z}[v, y]$ lies in our exceptional locus is easily checked.) More to the point, James P. Jones has conjectured [Jon81] that the decidabilities of the prefixes $\exists \forall \exists$ and $\exists \exists$, quantified over $\mathbb{N}$, are equivalent. Thus, while we have not settled Jones's conjecture, we have at least shown that the decidability of $\exists \forall \exists$ now hinges on a sub-problem much closer to $\exists \exists$.

It would be of considerable interest to push these techniques further to prove a complexity-theoretic reduction from $\exists \forall \exists$ to $\exists \exists$, or from $\exists \forall \exists$ to $\forall \exists$. This is because these particular reductions would be a first step toward reducing $\exists \exists \forall \exists$ to $\exists \exists \exists$, and thus settling Hilbert's Tenth Problem in three variables. Evidence for such a reduction is provided by another result relating (a) the size of the *largest* positive integral point on an algebraic plane curve with (b) detecting whether an algebraic surface possesses *any* integral point: Roughly speaking, it was shown in [Roj00a] that the computability of the function alluded to in (a) implies that the undecidability of $\exists \exists \forall \exists$ occurs only in a family of inputs nearly equivalent to $\exists \exists \exists$.

As for algebraic sets of dimension zero, one can in fact construct **PSPACE** algorithms to find all *rational* points [Roj99a]. However, deciding the *existence* of rational points, even on algebraic sets of dimension zero, is not yet known to lie within the polynomial hierarchy. So let us now consider the latter problem.

1.2. Dimension Zero

We will show that deciding feasibility over $\mathbb{Q}$, for most polynomial systems, can be done within the polynomial hierarchy, assuming the *Generalized*[6] *Riemann*

[5] I.e., the maximum of the sum of the exponents in any monomial term.

[6] The *Riemann Hyptohesis* (*RH*) is an 1859 conjecture equivalent to a sharp quantitative statement on the distribution of primes. GRH can be phrased as a generalization of this statement to prime ideals in an arbitrary number field; further background on these RHs can be found in [LO77, BS96].

Hypothesis (*GRH*)—a famous conjecture from number theory. To clarify this statement, let us first fix some notation and describe a quantitative result depending on GRH.

Let $\mathbf{F} := (f_1, ..., f_m)$ be a system of polynomials in $\mathbb{Z}[x_1, ..., x_n]$ and let $\boldsymbol{Z_F}$ be the zero set of F in $\mathbb{C}^n$. Recall that $\pi(x)$ denotes the number of primes $\leqslant x$. Let $\pi_F(x)$ be the variation on $\pi(x)$ where we instead count the number of primes $p \leqslant x$ such that the mod p reduction of F has a root in $\mathbb{Z}/p\mathbb{Z}$. Also, let $N_F(x)$ be the *weighted* variant of $\pi_F(x)$, where we instead count the *total* number of distinct roots of the mod p reductions of F, summed over all primes $p \leqslant x$.

DEFINITION 1. The *size* of an integer c is $\mathbf{size}(\boldsymbol{c}) := 1 + \lceil \log_2(|c| + 1) \rceil$. Similarly, the (*sparse*) *size*, $\mathbf{size}(\boldsymbol{F})$, of the polynomial system F is simply the sum of the sizes of all the coefficients *and* exponents in its monomial term expansion. We also let $\boldsymbol{\sigma(F)}$ denote the maximum bit-length of any coefficient of the monomial term expansion of F.

Unless otherwise mentioned, we will use the sparse encoding throughout.

Let $\mathbf{O}$ and e_i respectively denote the origin and the ith standard basis vector of $\mathbb{R}^n$. Also, let $\#$ denote set cardinality.

THEOREM 2.[7] *Let K be the field $\mathbb{Q}(x_i \,|\, (x_1, ..., x_n) \in Z_F,\ i \in \{1, ..., n\})$, and let r_F be the number of maximal ideals in the ring $\mathbb{Q}[x_1, ..., x_n]/\langle f_1, ..., f_n \rangle$. (In particular, $r_F \geqslant 1$ for $\# Z_F \geqslant 1$, and for $m = n = 1$ the quantity r_F is just the number of distinct irreducible factors of f_1 over $\mathbb{Q}[x_1]$.) Then the truth of GRH implies the following two statements, for all $x > 33766$:*

1. *Suppose $\infty > \# Z_F \geqslant 2$ and $\mathrm{Gal}(K/\mathbb{Q})$ acts transitively on Z_F. Then*

$$\frac{\pi_F(x)}{\pi(x)} < \left(1 - \frac{1}{Z_F}\right)\left(1 + \frac{(Z_F! + 1)\log^2 x + Z_F!\, \mathcal{O}(Z_F \sigma(h_F)) \log x)}{\sqrt{x}}\right).$$

2. *Suppose $\# Z_F \geqslant 1$. Then independent of $\mathrm{Gal}(K/\mathbb{Q})$, we have*

$$\frac{\pi_F(x)}{\pi(x)} > \frac{1}{\delta}(r_F - b(F, x)) \qquad \text{and} \qquad \left|\frac{N_F(x)}{\pi(x)} - r_F\right| < b(F, x),$$

where $0 \leqslant b(F, x) < (4V_F \log^2 x + \mathcal{O}(\delta\sigma(\hat{h}_F)(1 + n\delta^5/\sqrt{x})) \log x)/\sqrt{x}$, $0 \leqslant \sigma(h_F) \leqslant \sigma(\hat{h}_F) \leqslant \mathcal{O}(e^n \sqrt{n}\, M_F(\sigma(F) + m(n \log d + \log m)))$, d is the maximum degree of any f_i, $\delta \leqslant V_F$, $V_F := \mathrm{Vol}_n(Q_F)$, Q_F is the convex hull of the union of $\{\mathbf{O}, e_1, ..., e_n\}$ and the set of all exponent vectors of F, M_F is no larger than the maximum number of lattice points in any translate of $(n+1)\, Q_F$, and we normalize n-dimensional volume so that the standard n-simplex (with vertices $\mathbf{O}, e_1, ..., e_n$) has n-volume 1. Furthermore, explicit formulae for the asymptotic estimates above appear in Remarks 9 and 10 of Section 4.2.

The polytope volume V_F above is more natural than one might think: It is an upper bound on the number of irreducible components of Z_F (cf. Theorem 5 of the

[7] In [Roj99a], r_F was incorrectly defined as the number of rational roots of F.

next section). It has already been observed at least since the mid-1970's (e.g., [Kus75]) that $V_F \leqslant d^n$, where d is the maximum degree of any f_i. (In fact, d^n frequently exceeds V_F by a factor exponential in n [Roj00b, Roj00c].) Assertion (2) of Theorem 2 thus significantly improves earlier conditional bounds, which had stronger hypotheses or smaller (looser) leading terms [Koi96, Mor97, Bür00]. The upper bound on $\frac{\pi_F(x)}{\pi(x)}$ from assertion (1) appears to be new.

Note that averaging over many primes (as opposed to employing a single sufficiently large prime) is essentially unavoidable if one wants to use mod p root counts to decide the existence of rational roots or to estimate the quantity r_F. For example, from basic quadratic residue theory [HW79], we know that the number of roots $x_1^2 + 1 \bmod p$ is *not* constant for sufficiently large prime p. Similarly, Galois-theoretic restrictions are also necessary before using mod p root counts to decided feasibility over $\mathbb{Q}$.

EXAMPLE 1. Take $m = n = 1$ and $F = f_1 = (x_1^2 - 2)(x_1^2 - 7)(x_1^2 - 14)$. Clear, F has no rational roots. However, it is easily checked via Legendre symbols [Apo90, Chap. 9] that F has a root mod p for *all* primes p. In particular, the Galois group here does not act transitively: there is no automorphism of $\overline{\mathbb{Q}}$ which fixes $\mathbb{Q}$ and sends, say, $\sqrt{2}$ to $\sqrt{7}$.

We also point out that the truth of GRH has many other consequences in complexity theory. For example, the truth of GRH implies a polynomial time algorithm for deciding whether an input integer is prime [Mil76], an **AM** algorithm for deciding whether Z_F is empty [Koi96], and an **AM** algorithm for deciding whether Z_F is finite [Koi97].

Remark 2. Recall that $\mathbf{NP} \cup \mathbf{BPP} \subseteq \mathbf{AM} \subseteq \mathbf{coRP}^{\mathbf{NP}} \subseteq \mathbf{coNP}^{\mathbf{NP}} \subseteq \mathbf{P}^{\mathbf{NP}^{\mathbf{NP}}} \subseteq \cdots \subseteq \mathbf{PH} \subseteq \mathbf{P}^{\#\mathbf{P}} \subseteq \mathbf{PSPACE} \subseteq \mathbf{EXPTIME}$, and the properness of each inclusion is unknown [Zac86, BM88, BF91, Pap95].

Part (1) of Theorem 2 thus presents the main difference between feasibility testing over $\mathbb{C}$ and $\mathbb{Q}$: it is known [Koi96, Theorem 1] that the mod p reduction of F has a root in $\mathbb{Z}/p\mathbb{Z}$ for a density of primes p which is either positive or zero, according as F has a root in $\mathbb{C}$ or not. (See also [Roj00c, Theorem 4] for the best current quantitative bound along these lines.) The corresponding gap between densities is large enough to permit a coarse, but fast, approximate counting algorithm for $\#\mathbf{P}$ to be used to tell the difference, thus eventually yielding Koiran's **AM** algorithm for feasibility over $\mathbb{C}$ [Koi96]. (We point out that Koiran's algorithm actually relies on the behavior of the function N_F, which more amenable than that of π_F.) On the other hand, part (1) of Theorem 2 tells us that the mod p reduction of F has a root in $\mathbb{Z}/p\mathbb{Z}$ for a density of primes p which is either 1 or $\leqslant 1 - \frac{1}{V_F}$, and the lower density occurs if F is infeasible over $\mathbb{Q}$ in a strong sense.

However, the convergence of $\frac{\pi_F(x)}{\pi(x)}$ to its limit is unfortunately too slow to permit any obvious algorithm using subexponential work. So we will instead apply some Galois-theoretic tricks which allow to use the better behaved quantity $\frac{N_F(x)}{\pi(x)}$. Via a $\mathbf{P}^{\mathbf{NP}^{\mathbf{NP}}}$ constant factor approximate counting algorithm of Stockmeyer [Sto85], we then obtain the following result.

THEOREM 3.[8] *Following the notation and assumptions above, assume further that F fails to have a rational root $\Leftrightarrow$ [$Z_F = \varnothing$ or $\mathrm{Gal}(K/\mathbf{Q})$ acts transitively on Z_F]. Then the truth of GRH implies that deciding whether $Z_F \cap \mathbb{Q}^n$ is empty can be done within $\mathbf{P}^{\mathbf{NP}^{\mathbf{NP}}}$. Furthermore, we can check the emptiness and finiteness of Z_F unconditionally (resp. assuming GRH) within* **PSPACE** *(resp.* **AM**).

We thus obtain a new arithmetic analogue of Koiran's feasibility result over $\mathbb{C}$ [Koi96]. Indeed, just as we noted for the case of $\mathbb{Q}$, the best unconditional complexity bound for feasibility over $\mathbb{C}$ is **PSPACE** [Can88]. However, as we have seen, transferring conditional speed-ups from $\mathbb{C}$ to $\mathbb{Q}$ presents some unexpected subtleties.

Let us remark on the strength of our last two theorems: First note that our restrictions on the input F are actually rather gentle: In particular, if one fixes the monomial term structure of F and assumes $m \geqslant n$, then it follows easily from the theory of resultants [GKZ94, Stu98, Roj99b], that, for a generic choice of the coefficients, F will have only finitely many roots in $\mathbb{C}^n$. Furthermore, it is quite frequently the case that our hypothesis involving Z_F and $\mathrm{Gal}(K/\mathbb{Q})$ holds when F fails to have a rational root.

THEOREM 4. *Following the notation above, fix the monomial term structure of F and assume further that $m \geqslant n$ and the coefficients of F are integers of absolute value $\leqslant c$. Then the fraction of such F with $\mathrm{Gal}(K/\mathbb{Q})$ acting transitively on Z_F is at least $1 - \mathcal{O}(\log c/\sqrt{c})$. Furthermore, we can check whether $\mathrm{Gal}(K/\mathbb{Q})$ acts transitively on Z_F within* **EXPTIME** *or, if one assumes GRH, within $\mathbf{P}^{\mathbf{NP}^{\mathbf{NP}}}$.*

Thus, if $m \geqslant n$ and the monomial term structure of F is such that $\# Z_F \neq 1$ for a generic choice of the coefficients, it easily follows that at least $1 - \mathcal{O}(\log c/\sqrt{c})$ of the F specified above also have no rational roots. The case where the monomial term structure of F is such that $\# Z_F = 1$ for a generic choice of the coefficients is evidently quite rare, and will be addressed in future work.

Remark 3. A stronger version of the $m = n = 1$ case of Theorem 4 (sans complexity bounds) was derived by Gallagher in [Gal73]. The $m \geqslant n > 1$ case follows from a combination of our framework here, the Lenstra–Lenstra–Lovasz (LLL) algorithm [LLL82], and an effective version of Hilbert's Irreducibility Theorem from [Coh81].

It should also be clear that our assumption on Z_F by no means renders our feasibility problem trivial. The number of integral roots of F can already be exponential in the size of F, even when the number of complex roots of F is finite. A simple example is the system $(\prod_{i=1}^{d}(x_1 - i), ..., \prod_{i=1}^{d}(x_n - i))$, which has d^n integral roots and a size of $\mathcal{O}(nd \log d)$. Similarly, the integral roots of F can have coordinates of size exponential in size (F), thus obstructing their use as polynomial-size certificates of feasibility. For example, the system $(x_1 - 2, x_2 - x_1^2, ..., x_n - x_{n-1}^2)$ has size $\mathcal{O}(n)$ but has $(1, 2, ..., 2^{2^{n-2}})$ as a root.

[8] This version corrects an alleged bound of **AM**, which had an erroneous proof in [Roj99a].

On the other hand, when $n=1$, it is a pleasant surprise that one can find *all* rational roots in time polynomial in size (F) [Len98]. Nevertheless, we emphasize that it is still an open and intriguing question whether one can decide the existence of a rational root of F, unconditionally, within time polynomial in size (F). Even the case of systems of two polynomials in two variables is still completely open.

Theorems 2–4 may thus be of independent interest to number theorists, as well as complexity theorists. Aside from a geometric trick, the proofs of Theorems 2–4 share a particular tool with the proof of Theorem 1: All five proofs make use of some incarnation of effective univariate reduction.

Theorems 1–4 are respectively proved in Sections 3–6. However, let us first review some algorithmic tools that we will borrow from computational algebraic geometry and computational number theory.

2. BACKGROUND TOOLS

We begin with the following elementary fact arising from congruences.

PROPOSITION 1. *If z is any rational root of some $g(x_1)=\alpha_0+\alpha_1 x_1+\cdots+\alpha_d x_1^d \in \mathbb{Z}[x_1]$, then $z=\pm\frac{b}{c}$ for some divisor b of α_0 and some divisor c of α_d.*

We will also need the following classical fact regarding the factors of a multivariate polynomial.

LEMMA 1. *Suppose $f\in\mathbb{Z}[x_1,\ldots,x_N]$ has total degree d and coefficients of absolute value $\leqslant c$. Then $g\in\mathbb{Z}[x_1,\ldots,x_N]$ divides $f\Rightarrow$ the coefficients of g have absolute value $\leqslant\sqrt{d+1}\cdot 2^d c$.*

The lemma above is a paraphrase of a similar statement from [Mig92].

We will also need some sufficiently precise quantitative bounds on the zero-dimensional part of an algebraic set, e.g., good bounds on the number of points and their sizes. A recent bound of this type, polynomial in V_F, is the following:

THEOREM 5 [Roj00c, Theorems 5 and 6]. *Following the notation of Section* 1.2, *Z_F has no more than V_F irreducible components. Also, assuming Z_F is finite, there is a univariate polynomial $h_F\in\mathbb{Z}[t]$ of degree $\leqslant V_F$ such that*

$$\sigma(h_F)=\mathcal{O}(M_F(\sigma(F)+m(n\log d+\log m)))$$

and the splitting field of h_F is exactly the field $\mathbb{Q}[x_i\,|\,(x_1,\ldots,x_n)\in\mathbb{C}^n$ is a root of $F]$. Similarly, letting Z'_F denote the zero-dimensional part of Z_F, we have that for any $i\in\{1,\ldots,n\}$, there is a univariate polynomial $P_i\in\mathbb{Z}[t]$ with degree $\leqslant V_F$, and $\sigma(P_i)\leqslant\sigma(h_F)$, such that $P_i(x_i)=0$ for any $(x_1,\ldots,x_n)\in Z'_F$. Explicit formulae for these bounds appear in Remarks 9 *and* 10 *of Section* 4.

A preliminary version of the theorem above was announced in the proceedings version of this paper [Roj99a]. Earlier quantitative results of this type, usually with stronger hypotheses or less refined statements, can be found starting with the work of Joos Heintz and his school from the late 80's onward. A good reference for these

earlier results is [KP96] and more recent bounds similar to the one above can be found in [KPS99, Proposition 2.11] and [Mai00, Corollary 8.2.3]. There are also more general versions of Theorem 5 applying even to quantifier elimination over algebraically closed fields [FGM90], but the bounds get looser and the level of generality is greater than we need.

An immediate corollary of our quantitative result above is the following upper bound on $\pi(x)-\pi_F(x)$, which may be of independent interest.

COROLLARY 1. *Following the notation of Theorem* 5, *assume F has a rational root. Then the corollary of primes p for which the* mod *p reduction of F has* no *roots in* $\mathbb{Z}/p\mathbb{Z}$ *is no greater than* $a_F^* := \sum_{i=1}^n (\sigma(P_i)+1) = \mathcal{O}(\sqrt{n}\, e^n V_F(\sigma(F)+m(n\log d+\log m)))$.

Proof. Consider the ith coordinate, x_i, of any rational root of F. By Theorem 5, and an application of Proposition 1, the log of the denominator of x_i (if x_i is written in lowest terms) can be no larger than $\sigma(P_i)$. In particular, this denominator must have no more than $\sigma(P_i)+1$ prime factors, since no prime power is smaller than 2. Since we are dealing with n coordinates, we can simply sum our last bound over i and conclude via Theorem 5. ∎

Let $\mathbf{Li}(x) := \int_2^x \frac{dt}{\log t}$. The following result from analytic number theory will be of fundamental importance in our quantitative discussions on prime densities.

THEOREM 6. *The truth of RH implies that, for all* $x>2$, $\pi(x)$ *is within a factor of* $1+\frac{7}{\log x}$ *of* $x(\frac{1}{\log x}+\frac{1}{\log^2 x})-\frac{2}{\log 2}$. *Furthermore, independent of RH, for all* $x>2$, $\mathrm{Li}(x)$ *is within a factor of* $1+\frac{6}{\log x}$ *of* $x(\frac{1}{\log x}+\frac{1}{\log^2 x})-\frac{2}{\log 2}$.

The proof can be sketched as follows: One first approximates $\mathrm{Li}(x)$ within a multiple of $1+\frac{6}{\log x}$ by $x(\frac{1}{\log x}+\frac{1}{\log^2 x})-\frac{2}{\log 2}$, using a trick from [Apo90, p. 80]. Then, a (conditional) version of the effective Chebotarev Density Theorem, due to Oesterlé [Oes79, BS96], tells us that the truth of RH implies

$$|\pi(x)-\mathrm{Li}(x)| < \sqrt{x}\log x, \qquad \text{for all} \quad x>2.$$

So, dividing through by $x(\frac{1}{\log x}+\frac{1}{\log^2 x})-\frac{2}{\log 2}$ and applying the triangle inequality, we obtain our theorem above.

The remaining facts we need are more specific to the particular main theorems to be proved, so these will be mentioned as the need arises.

Remark 4. Henceforth, we will use a stronger definition of genericity: A statement involving a set of parameters $\{c_1, ..., c_N\}$ holds *generically* iff the statement is true for all $(c_1, ..., c_N) \in \mathbb{C}^N$ outside of some *a priori fixed* algebraic hypersurface. That this version of genericity implies the simplified version mentioned earlier in our theorems is immediate from Schwartz' Lemma [Sch80].

3. GENUS ZERO VARIETIES AND THE PROOF OF THEOREM 1

In what follows, we will make use of some basic algebraic geometry. A more precise description of the tools we use can be found in [Roj00a]. Also, we will

always use *geometric* (as opposed to arithmetic) genus for algebraic varieties [Har77].

Let us begin by clarifying the genericity condition of Theorem 1. Let Z_f be the zero set of f. What we will initially require of f (in addition to the assumptions on its Newton polytope) is that Z_f be irreducible, nonsingular, and non-ruled. Later, we will see that a weaker and more easily verified condition suffices.

Remark 5. Ruled surfaces include those surfaces which contain an infinite family of lines, for example: planes, cones, one-sheeted hyperboloids, and products of a line with a curve. More precisely, an algebraic surface $S \subseteq \mathbb{P}^N_{\mathbb{C}}$ is called *ruled* if there is a projective curve C, and a morphism $\varphi : S \to C$, such that every fiber of φ is isomorphic to $\mathbb{P}^1_{\mathbb{C}}$. We then call a surface $S' \subseteq \mathbb{C}^3$ (the case which concerns us) *ruled* iff S' is isomorphic to an open subset of some ruled surface in $\mathbb{P}^N_{\mathbb{C}}$.

LEMMA 2. *Following the notation and hypotheses of Theorem* 1, *write* $f(v, x, y) := \sum_{(a_1, a_2, a_3) \in A} c_a v^{a_1} x^{a_2} y^{a_3}$. *Then, for a generic choice of the coefficients* $(c_a)_{a \in A}$, Z_f *is irreducible, non-singular, and non-ruled. In particular, for a generic choice of the coefficients, the set* $\sum_f := \{0\} \cup \{v_0 \in \mathbb{C} \mid \{(x, y) \in \mathbb{C}^2 \mid f(v_0, x, y) = 0\}$ *is singular or reducible*$\}$ *is finite.*

Proof. That Z_f is irreducible and nonsingular for a generic choice of coefficients follows easily from the Jacobian criterion for singularity [Mum95]. (One can even write the conditions explicitly via $\mathscr{A}$-discriminants [GKZ94], but this will not concern us here.)

That Z_f is also non-ruled generically follows easily from a result of Khovanskii relating integral points in Newton polyhedra and genera [Kho78]. His result, given the hypotheses above, implies that Z_f has positive genus for a generic choice of the coefficients. (In fact, the only assumptions necessary for his result are the Newton polytope condition stated in Theorem 1 and the nonsingularity of Z_f.) The classification of algebraic surfaces [Bea96] then tells us that Z_f has positive genus $\Rightarrow Z_f$ is non-ruled.

As for the assertion on $\sum_f$, assume momentarily that Z_f is irreducible, nonsingular, and non-ruled. Then by Sard's theorem [Hir94], $Z_f \cap \{v = v_0\}$ is irreducible and nonsingular for all but finitely many $v_0 \in \mathbb{C}$. Thus, $\sum_f$ is finite when Z_f is irreducible, nonsingular, and non-ruled.

Since the intersection of any two open Zariski-dense sets is open and dense, we are done. ∎

LEMMA 3. *Following the notation above, the set of* $v_0 \in \mathbb{Z}$ *such that* $\forall x \, \exists y f(v_0, x, y) = 0$ *is contained in* $\sum_f \cap \mathbb{Z}$, *whether both quantifiers range over* $\mathbb{N}$ *or* $\mathbb{Z}$. *Furthermore,* $\sum_f \cap \mathbb{N}$ *finite* $\Rightarrow$ *the number of elements of* $\sum_f \cap \mathbb{Z}$, *and the size of each such element, is polynomial in the dense encoding.*

Proof. By Siegel's Theorem [Sil99], $\forall x \, \exists y f(v_0, x, y) = 0 \Rightarrow Z_f \cap \{v = v_0\}$ contains a curve of genus zero (whether the quantification is over $\mathbb{N}$ or $\mathbb{Z}$).

Now note that for all nonzero $v_0 \in \mathbb{C}$, the Newton polytope of f (as a polynomial in *two* variables) is a polygon containing an integral point in its interior. So, by

Khovanskii's Theorem [Kho78] once again, $Z_f \cap \{v = v_0\}$ irreducible and non-singular $\Rightarrow Z_f \cap \{v = v_0\}$ is a curve of positive genus.

Putting together our last two observations, the first part of our lemma follows immediately.

To prove the final assertion, note that the Jacobian criterion for singularity [Mum95] implies that $\sum_f$ is simply the set of v_0 such that (v_0, x, y) is a complex root of the system of equations $(f(v_0, x, y), \partial f(v_0, x, y)/\partial x, \partial f(v_0, x, y)/\partial y)$ has a solution $(x, y) \in \mathbb{C}^2$. Thus, $\sum_f \in \mathbb{N}$ finite $\Rightarrow \sum_f$ is a finite set, and by Theorem 5 we are done. ∎

Thanks to the following result, we can solve the prefix $\forall\,\exists$ within **coNP**.

TUNG'S THEOREM [Tun87]. *Deciding the quantifier prefix* $\forall\,\exists$ (*with all quantifiers ranging over* $\mathbb{N}$ *or* $\mathbb{Z}$) *is* **coNP**-*complete relative to the dense encoding.*

The algorithms for $\forall\,\exists$ alluded in Tung's Theorem are based on some very elegant algebraic facts due to Jones, Schinzel, and Tung. We illustrate one such fact for the case of $\forall\,\exists$ over $\mathbb{N}$.

THE JST THEOREM [Jon81, Sch82, Tun87]. *Given any* $f \in \mathbb{Z}[x, y]$, *we have that* $\forall x\, \exists y f(x, y) = 0$ *iff all three of the following conditions hold*:

1. *The polynomial* f *factors into the form* $f_0(x, y) \prod_{i=1}^{k} (y - f_i(x))$ *where* $f_0(x, y) \in \mathbb{Q}[x, y]$ *has* no *zeroes in the ring* $\mathbb{Q}[x]$, *and for all* i, $f_i \in \mathbb{Q}[x]$ *and the leading coefficient of* f_i *is positive.*

2. $\forall x \in \{1, ..., x_0\} \exists y \in \mathbb{N}$ *such that* $f(x, y) = 0$, *where* $x_0 = \max\{s_1, ..., s_k\}$, *and for all* i, s_i *is the sum of the squares of the coefficients of* f_i.

3. *Let* α *be the least positive integer such that* $\alpha f_1, ..., \alpha f_k \in \mathbb{Z}[x]$ *and set* $g_i := \alpha f_i$ *for all* i. *Then the* union *of the solutions of the following* k *congruences*

$$g_1(x) \equiv 0 \bmod \alpha$$

$$\vdots$$

$$g_k(x) \equiv 0 \bmod \alpha$$

is all *of* $\mathbb{Z}/\alpha\mathbb{Z}$.

The analogue of the JST Theorem over $\mathbb{Z}$ is essentially the same, save for the absence of condition (2), and the removal of the sign check in condition (1) [Tun87].

Proof of Theorem 1. Within this proof, we will always use the *dense* encoding.

Assume $\sum_f \cap \mathbb{N}$ is finite. *This* will be our genericity hypothesis and by Lemma 2, and our hypothesis on the Newton polytope of f, this condition indeed occurs generically. Further more, via [Can88, NR96], we can check whether $\sum_f$ is finite (and thus whether $\sum_f \cap \mathbb{N}$ or $E_f \in \mathbb{Z}$ is finite) within the class **NC**. It is then clear

from Lemma 3 that checking $\exists\,\forall\,\exists$ can now be reduced to checking an instance of $\forall\,\exists$ for every $v_0 \in \sum_f \cap \mathbb{N}$ (or $v_0 \in \sum_f \cap \mathbb{Z}$).

Our goal will then be to simply use **NP** certificates for finitely many false $\forall\,\exists$ sentences, or the emptiness of $\sum_f \cap \mathbb{N}$ (or $E_f \cap \mathbb{Z}$), as a single certificate of the falsity of $\exists\,\forall\,\exists$. The emptiness of $E_f \cap \mathbb{N}$ (or $E_f \cap \mathbb{Z}$) can also be checked within the class **NC** [Can88]. So by Lemma 3, it suffices to assume $\sum_f \cap \mathbb{N}$ is nonempty and then check that the size of each resulting certificate is polynomial in the dense size of f. So let us review this now.

Fixing $v_0 \in \sum_f \cap \mathbb{Z}$, first note that the dense size of $f(v_0, x, y)$ is clearly polynomial in the dense size of $f(v, x, y)$, thanks to another application of Lemma 3. A certificate of $\forall x\,\exists y f(v_0, x, y) \neq 0$ (quantified over $\mathbb{N}$) can then be constructed via the JST Theorem as follows: First, factor f within **NC** (via, say, [BCGW92]). If f has no linear factor of the form $y - f_i(x)$, then we can correctly declare that the instance of $\forall x\,\exists y f(v_0, x, y) \neq 0$ is true. Otherwise, we attempt to give an $x' \in \{1, ..., x_0\}$ such that $f(x', y)$ has no positive integral root. Should such an x' exist, Lemma 1 tells us that its size will be polynomial in size(f), so x' is an **NP** certificate. Otherwise, we give a pair (j, t) with $1 \leqslant j \leqslant k$ and $t \in \{0, ..., \alpha\}$ such that $g_j(t) \not\equiv 0 \bmod \alpha$. Exhibiting such a pair gives a negative solution of an instance of the *covering congruence* problem, which is known to lie in **NP** [Tun87].

So we have now proved our main theorem in the case of quantification over $\mathbb{N}$. The proof of the case where we quantify over $\mathbb{Z}$ is almost identical, simply using the aforementioned analogue of the JST Theorem over $\mathbb{Z}$ instead. ∎

Remark 6. Note that if $f \in \mathbb{Z}[v, y]$ then the zero set of f is a ruled surface in $\mathbb{C}^3$. From another point of view, the hypothesis of Theorem 1 is violated since this P has empty interior. Deciding $\exists\,\forall\,\exists$ for this case then reduces to deciding $\exists\,\exists$, which we've already observed is very hard. Nevertheless, Alan Baker has conjectured that the latter problem is decidable [Jon81, Sect. 5]. ∎

Remark 7. The complexity of deciding whether a given surface is ruled is an open problem. (Although one can check a slightly weaker condition $(\#\sum_f < \infty)$ within **NC**, as noted in our last proof.) It is also interesting to note that finding explicit parametrizations of *rational* surfaces (a special class of ruled surfaces) appears to be decidable. Evidence is provided by an algorithm of Josef Schicho which, while still lacking a termination proof, seems to work well in practice [Sch98].

4. PRIME DISTRIBUTION: PROVING THEOREM 2

The proofs of assertions (1) and (2) will implicitly rely on another quantitative result on factoring polynomials, which easily follows from Hadamard's inequality [Mig92].

DEFINITION 2. Given any univariate polynomial $g(t) = \alpha_0 + \alpha_1 t + \cdots + \alpha_d t^d \in \mathbb{Z}[t]$ with all $|\alpha_i|$ bounded above by some integer c, define the *discriminant of* $\boldsymbol{g}$, $\boldsymbol{\Delta_g}$, to be $((-1)^{d(d-1)/2)/\alpha^d}$ times the following $(2d-1) \times (2d-1)$ determinant,

$$\det \begin{bmatrix} \alpha_0 & \cdots & \alpha_d & 0 & \cdots & 0 & 0 \\ 0 & \alpha_0 & \cdots & \alpha_d & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & \alpha_0 & \cdots & \alpha_d & 0 \\ 0 & 0 & \cdots & 0 & \alpha_0 & \cdots & \alpha_d \\ \alpha_1 & \cdots & d\alpha_d & 0 & \cdots & 0 & 0 \\ 0 & \alpha_1 & \cdots & d\alpha_d & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & \alpha_1 & \cdots & d\alpha_d & 0 \\ 0 & 0 & \cdots & 0 & \alpha_1 & \cdots & d\alpha_d \end{bmatrix},$$

where the first $d-1$ (resp. last d) rows correspond to the coefficients of g (resp. the derivative of g).

LEMMA 4. *Following the preceding notation,* $\log |\Delta_{\bar{g}}| \leqslant \bar{d}(d \log 2 + \log(\bar{d}+1) + \max_{\alpha_i \neq 0} \log |\alpha_i|)$, *where* $\bar{g}$ *is the square-free part of* g *and* $\bar{d}$ *is the degree of* $\bar{g}$.

The last and most intricate result we will need is the following refined effective version of the primitive element theorem.

THEOREM 7 [Roj00c, Theorem 7]. *Following the notation of Theorem* 5, *one can pick* h_F (*still satisfying the conclusion of Theorem* 5), *so that there exist* $a_1, ..., a_n \in \mathbb{N}$ *and* $h_1, ..., h_n \in \mathbb{Z}[t]$ *with the following properties*:

1. *The degrees of* $h_1, ..., h_n$ *are all bounded above by* V_F.
2. *For any root* $(\zeta_1, ..., \zeta_n) \in Z'_F$ *of* F, *there is a root* θ *of* h_F *such that* $\frac{h_i(\theta)}{a_i} = \zeta_i$ *for all* i.
3. *For all* i, *both* $\log a_i$ *and* $\sigma(h_i)$ *are bounded above by* $\mathcal{O}(e^n/\sqrt{n}\, V_F^3(\sigma(F) + m(n \log d + \log m)))$.

Remark 8. Earlier quantitative results of this type, e.g., those applied in [Koi96], had looser bounds which were polynomial in $d^{n^{\mathcal{O}(1)}}$.

4.1. Proving Assertion (2) *of Theorem* 2

First let us recall the following refined version of an important result due to Weinberger.

THEOREM 8. *Following the notation of Section* 1.2, *Theorem* 6, *and Lemma* 4, *suppose further that* g *has no factors of multiplicity* >1. *Then the truth of GRH implies that*

$$\left| \frac{N_g(x)}{\pi(x)} - r_g \right| < \frac{2\sqrt{x} \log(|\Delta_g|\, x^d) + d \log |\Delta_g|}{\mathrm{Li}(x)}, \qquad \textit{for all} \quad x > 2.$$

The original version from [Wei84] had an unspecified constant in place of the 2. The version above follows immediately from Weinberger's original proof,

simply using a stronger version of effective Chebotarev than he used; i.e., one replaces Theorem 1.1 of [LO77] with a result of Oesterlé [Oes79] (see also Theorem 8.8.22 of [BS96]).

The second (harder) bound of assertion (2) of Theorem 2 is then just a simple corollary of Theorems 5 and 8. The first bound then becomes an even simpler corollary of the second bound.

Proof of Assertion (2). By Theorems 5 and 7, it immediately follows that $r_F = r_g$, where g is the square-free part of h_F. It also follows easily that the mod p reduction of F has a root in $\mathbb{Z}/p\mathbb{Z} \Rightarrow$ the mod p reduction of g has a root in $\mathbb{Z}/p\mathbb{Z}$. Furthermore, Theorem 7 tells us that a sufficient condition for the converse assertion is that p not divide any of the a_i (the denominators in our rational univariate representation of Z_F). We thus obtain $|N_F(x) - N_g(x)| \leqslant V_F \sum_{i=1}^n (\log a_i + 1)$, for all $x > 0$.

Assume henceforth that $x > 2$. We then have

$$\left|\frac{N_F(x)}{\pi(x)} - r_F\right| \leqslant \left|\frac{N_g(x)}{\pi(x)} - r_g\right| + \frac{V_F(\sum_{i=1}^n \log a_i + n)}{\pi(x)}.$$

Combining Theorem 8 and Oesterlé's conditional bound on $|\pi(x) - \mathrm{Li}(x)|$, we thus obtain that the truth of GRH implies

$$\left|\frac{N_F(x)}{\pi(x)} - r_F\right| < \frac{2\sqrt{x}\log(|\Delta_g| x^{V_F}) + V_F \log|\Delta_g|}{\mathrm{Li}(x)} + \left(1 + \frac{\sqrt{x}\log x}{\mathrm{Li}(x)}\right)\frac{V_F(\sum_{i=1}^n \log a_i + n)}{\mathrm{Li}(x)}.$$

By Theorem 6, and the fact that $[(\log^3 x)(1 + 6/\log x)/\sqrt{x}(\log x + 1) - (2/\log 2)\log^2 x] < 1$ for all $x > 33766$, we then obtain

$$\left|\frac{N_F(x)}{\pi(x)} - r_F\right| < \frac{2\sqrt{x}\log(|\Delta_g| x^{V_F}) + V_F \log|\Delta_g| + 2V_F(\sum_{i=1}^n \log a_i + n)}{\mathrm{Li}(x)},$$

for all $x > 33766$. The second bound from assertion (2) then follows immediately from Lemma 4, Theorem 5, and the fact that $\frac{\mathrm{Li}(x)}{(x/\log x)} < (1 + 4/\log x)^2$ (applying Theorem 6 one last time).

The first bound of assertion (2) follows immediately from the second bound via a simple application of the triangle inequality and the inequality $N_F(x) \leqslant V_F \pi_F(x)$. ∎

Remark 9. Carrying out the last step in detail (and observing that $(1 + 4/\log x)^2 < 2$ for all $x > 33766$) it is clear that the asymptotic bound on $b(F, x)$ can be replaced by the following explicit quantity:

$$\frac{4V_F \log^2 x + \left(4\log|\Delta_g| + \left(\frac{2V_F(2n(\log a + 1) + \log|\Delta_g|)}{\sqrt{x}}\right)\log x\right)}{\sqrt{x}},$$

where $0 \leqslant \log |\Delta_g| \leqslant V_F(V_F \log 2 + \log(V_F+1) + \sigma(h_F))$,

$$0 \leqslant \log a \leqslant V_F\{(V_F-1)[\log(V_F(V_F+1)^4\, 64^{V_F}) + 2\sigma(h_F)] + \sigma(h_F)\} + \sigma(h_F) + \log V_F,$$

$$0 \leqslant \sigma(h_F) \leqslant \log\left[\frac{e^{13/6}}{\pi}\sqrt{m_F+1}\cdot 2^{V_F} 4^{m_F} n^{V_F/2}\left(\binom{V_F}{2}+1\right)^{nV_F} \times (\sqrt{\mu}(m(mV_F+1)^{m-1}\, c+1)^{m_F}\right].$$

$V_F \leqslant m_F \leqslant e^{1/8}\, e^n/\sqrt{n+1}\; V_F$, and μ is the maximal number of monomial terms in any f_i. The explicit bounds for $\log a$ and $\sigma(h_F)$ are quoted from [Roj00c, Remarks 7 and 8].

4.2. *Proving Assertion* (1) *of Theorem* 2

Here we will need the following result dealing with the density of primes for which F has a root mod p. This theorem may be of independent interest to computational number theorists.

THEOREM 9. *Following the notation of Theorem* 2, *let* j_F *be the fraction of elements of* $\mathrm{Gal}(K/\mathbb{Q})$ *which fix at least one root of* F. *Then the truth of GRH implies that*

$$\left|\frac{\pi_F(x)}{\pi(x)} - j_F\right| < \frac{j_F(V_F!+1)\log^2 x + 2\left(j_F V_F! \log|\Delta_g| + \dfrac{\sigma(h_F)+1}{\sqrt{x}}\right)\log x}{\sqrt{x}}$$

for all $x > 33766$, *where* h_F *is the polynomial from Theorem* 5 *and* g *is the square-free part of* h_F.

Proof. Let j_g be the fraction of elements of the Galois group of g (over $\mathbb{Q}$) which fix at least one root of g. By essentially the same argument as the beginning of the proof of assertion (1), we obtain $j_F = j_g$. Similarly, we also obtain $|\pi_F(x) - \pi_g(x)| \leqslant \sigma(h_F) + 1$ for all $x > 2$.

Note that j_g is also the fraction of elements of the Galois group which give permutations (of the roots of g) possessing a fixed point. Oesterlé's (conditional) version of effective Chebotarev [Oes79, BS96] then tells use[9] that the truth of GRH implies

$$|\pi_g(x) - j_g\,\mathrm{Li}(x)| \leqslant j_g\sqrt{x}(2\log|\Delta| + \mathfrak{d}\log x),$$

where Δ is the discriminant of K, K is the splitting field of g, and $\mathfrak{d}$ is the field extension degree $|K/\mathbb{Q}|$. Since the degree of g is $\leqslant V_F$, basic Galois theory tells us that $\mathfrak{d} \leqslant V_F!$.

[9] His result is actually stated in terms of conjugacy classes, but since the number of fixed points of a Galois group element is stable under conjugacy, we can simply sum over conjugacy classes.

By Oesterlé's conditional bound on $|\pi(x) - \mathrm{Li}(x)|$ we then obtain

$$|\pi_g(x) - j_g \pi(x)| \leqslant j_g \sqrt{x}\,(2 \log |\Delta| + (\mathfrak{d}+1) \log x).$$

Following essentially the same reasoning as the proof of assertion (2) we then obtain

$$\left|\frac{\pi_F(x)}{\pi(x)} - j_F\right| < \frac{j_g(\mathfrak{d}+1)\log^2 x + 2\left(j_g \log|\Delta| + \dfrac{\sigma(h_F)+1}{\sqrt{x}}\right)\log x}{\sqrt{x}},$$

for all $x > 33766$. Using the fact that $|\Delta| \leqslant |\Delta_g|^{\mathfrak{d}}$ [BS96, p. 259], and applying Lemma 4, we are done. ∎

Of course, we must now estimate the quantity j_F. Fortunately, a good upper bound has already been derived by Peter J. Cameron and Arjeh M. Cohen, in answer to a 1991 question of Hendrik W. Lenstra.

THEOREM 10. *Suppose G is any group acting transitively and faithfully on a set of N elements and j_G is the fraction of elements of G with at least one fixed-point. Then $j_G \leqslant 1 - \frac{1}{N}$.*

The proof occupies the second page of [CC92] and requires only some basic group representation theory.[10] The upper bound is tight, but completely classifying the next lower values of j_G currently requires the classification of finite simple groups [GW97]. The latter classification will *not* be necessary for our results.

Proof of Assertion (1). First note that by assumption, $V_F \geqslant \# Z_F \geqslant 2$. Furthermore, by Theorems 5 and 10, $j_F \leqslant 1 - \frac{1}{V_F}$. So by Theorem 9 we are done. ∎

Remark 10. From our proofs above we easily see that the asymptotic bound from assertion (1) can be replaced by the explicit quantity

$$\left(1 - \frac{1}{V_F}\right)\left(1 + \frac{(V_F! + 1)\log^2 x + 2\left(V! \log|\Delta_g| + \dfrac{V_F}{V_{F-1}} \cdot \dfrac{\sigma(h_F)+1}{\sqrt{x}}\right)\log x}{\sqrt{x}}\right),$$

where $\sigma(h_F)$ and $\log|\Delta_g|$ are bounded as in Remark 9.

5. THE PROOF OF THEOREM 3

Our algorithm essentially boils down to checking whether $r_F \geqslant 2$ or $r_F = 1$, following the notation of Theorem 2. Via our initial assumptions on F, we will see that this is the same as checking whether F as a rational root or not.

[10] Their paper actually dealt with finding a *lower* bound for the quantity $1 - j_G$.

More precisely, our algorithm proceeds as follows: First check whether Z_F is empty. If so, then we immediately know that $Z_F \cap \mathbb{Q}^n$ is empty and we are done. Otherwise, approximate $N_F(M)$ and $\pi(M)$ within a factor of $\frac{9}{8}$, where M is an integer sufficiently larger than 33,766 so that $b(F, M) < \frac{1}{10}$. Respectively calling these approximations $\bar{N}$ and $\bar{\pi}$, we then do the following: If $\bar{N} \leqslant (\frac{9}{8})^2 \bar{\pi}$, declare $Z_F \cap \mathbb{Q}^n$ empty. Otherwise, declare $Z_F \cap \mathbb{Q}^n$, nonempty.

That our algorithm works is easily checked. First note that $\bar{N} \leqslant (\frac{9}{8})^2 \bar{\pi} \Leftrightarrow \frac{N_F(M)}{\pi(M)} \leqslant (\frac{9}{8})^4$. So by Theorem 2, our assumption on $b(F, M)$ implies that the last inequality occurs iff $r_F = 1$. (Note that we need GRH at this point.) Letting g be the square-free part of the polynomial h_F from Theorem 5, it is easily checked that $r_F = r_g$. So by [Jac85, Theorem 4.14], we have that $\mathrm{Gal}(K/\mathbb{Q})$ acts transitively on Z_F iff g is irreducible over $\mathbb{Q}$ (or equivalently, $r_F = r_g = 1$). So by our initial assumptions on F, $r_F = 1$ iff F has no rational roots. Thus, we now need only check the complexity of our algorithm.

That the emptiness and finiteness of Z_F can be checked within **PSPACE** unconditionally goes back to [Can88]. That the truth of GRH implies both bounds can be lowered to **AM** is proved respectively in [Koi96] and [Koi97]. So now we need only check the complexity of computing M, $\bar{N}$, and $\bar{\pi}$.

It follows immediately from [Pra75] that $N_F(x)$ and $\pi(x)$ can be computed within $\#\mathbf{P}$. Also, via [GK94], V_F can be computed within $\#\mathbf{P}$ as well. Furthermore, via Theorems 2 and 5 (and the fact that $0 \leqslant \log V_F \leqslant n \log d$), the number of bits of M is polynomial in the size of F. So by [Sto85], M, $\bar{N}$, and $\bar{\pi}$ can be computed within $\mathbf{P}^{\mathbf{NP}^{\mathbf{NP}}}$. Therefore, our algorithm runs within $\mathbf{P}^{\mathbf{NP}^{\mathbf{NP}}}$, assuming GRH.

Remark 11. It is an open problem whether Theorem 3 continues to hold under the weaker condition that the *real* dimension of Z_F is at most zero.

6. THE PROOF OF THEOREM 4

If $m > n$ then we have already observed that F generically has no roots, so there is nothing to prove. On the other hand, if $m < n$ and Z_F is a finite set, then Z_F must be empty. So again there is nothing to prove. We can therefore assume that $m = n$. Since the $n = 1$ case was already solved by Gallagher [Gal73], we may further assume that $n > 1$. (In fact, Gallagher proved that when $n = 1$, one can make the stronger assertion that the Galois group of f_1 is the full symmetric group for asymptotically the same fraction of f_1.)

Now consider the toric resultant, $\mathscr{R}$, of $f_1, ..., f_n$ and $u_0 + u_1 x_1 + \cdots + u_n x_n$. (The classical resultant of Macaulay would-suffice to prove a version of our theorem here, but only for a highly limited family of monomial term structures.) Then, for indeterminate coefficients, $\mathscr{R}$ is an irreducible polynomial over $\mathbb{Z}$ adjoin $u_0, ..., u_n$ and the coefficients of F. More importantly, if the coefficients of F are *constants*, $\mathscr{R}$ is divisible by $u_0 - (\zeta_1 u_1 + \cdots + \zeta_n u_n)$, for any root $(\zeta_1, \cdots, \zeta_n) \in \mathbb{C}^n$ of F.

If it happens that $\mathscr{R}$ is the constant 1, then it follows from the degree formula for the toric resultant [GKZ94] that Z_F is empty for a generic choice of the coefficients. So let us assume $\mathscr{R}$ is not identically 1 and let N denote the number of monomial terms of F.

By [Coh81] it then follows that a fraction of at most $\mathcal{O}(\log c/\sqrt{c})$ of the points

in $\mathbb{Q}^{N+n}$ with (multiplicative) height $\leqslant c$ result in choices of rational coefficients where $\mathscr{R}$ is a reducible polynomial over $\mathbb{Q}[u_0]$. By rescaling, this easily implies that at least a fraction of $1-\mathcal{O}(\log c/\sqrt{c})$ of the points in $\{-c, ..., c\}^{N+n}$ result in $\mathscr{R}$ being irreducible over $\mathbb{Q}[u_0]$.

To conclude, we observe (say from [Roj00c, Sect. 6]) that the polynomial h_F from Theorems 5 and 7 is nothing more than the resultant $\mathscr{R}$, for suitably chosen $u_1, ..., u_n$. In fact, the set of $u_1, ..., u_n$ of which h_F fails to have the properties specified in Theorems 5 and 7 is a collection of $\mathcal{O}(V_F^2)$ hyperplanes in $\mathbb{C}^n$ [Roj99b, Roj00c]. Thus by Schwartz' lemma, the fraction of polynomial systems F (with integer coefficients of absolute value $\leqslant c$) for which h_F is irreducible over $\mathbb{Q}$ is at least $1-\mathcal{O}(\log c/\sqrt{c})$. By [Jac85, Theorem 4.14], h_F is irreducible iff its Galois group acts transitively on its roots. So by Theorem 7, the fraction of polynomial systems F (with integer coefficients of absolute value $\leqslant c$) for which $\mathrm{Gal}(K/\mathbb{Q})$ acts transitively on Z_F is at least $1-\mathcal{O}(\log x/\sqrt{c})$.

That $\mathrm{Gal}(K/\mathbb{Q})$ acts transitively on Z_F can be checked within $\mathbf{P}^{\mathbf{NP}^{\mathbf{NP}}}$ (assuming GRH) is already clear from the proof of Theorem 3. To obtain the unconditional complexity bound, it clearly suffices to factor h_F within **EXPTIME** and see whether h_F is irreducible. Since Theorem 5 tells us that the dense size of h_F is exponential in size (F), we can conclude via an application of the polynomial time LLL factoring algorithm from [LLL82].

ACKNOWLEDGMENTS

The author thanks Felipe Cucker, Jan Denef, Michael Fried, Teresa Krick, Jeff Lagarias, Luis-Muigel Pardo-Vasallo, and Bjorn Poonen for some very useful discussions, in person and via e-mail. In particular, Jan Denef pointed out the excellent reference [FJ86], and Michael Fried helped confirm a group-theoretic hope of the author (Theorem 10). Special thanks go to Pascal Koiran for pointing out errors in earlier versions of Theorems 2 and 3. This paper is dedicated to Gretchen Davis, a remarkable educator who first inspired the author's interest in mathematics.

Note added in proof. The explicit estimates in Remarks 9 and 10 of Section 4 have recently been improved. The interested reader can see the Math ArXiV preprint math.NT/0005029 at http://xxx.arXiv.org for further details.

REFERENCES

[AM75] L. Adleman and K. Manders, NP-complete decision problems for quadratic polynomials, *in* "Eighth annual ACM Symposium on theory of Computing" (P. A. Hershey, Ed.), pp. 23–29, Assoc. Comput. Mach., New York, 1976.

[Apo90] T. M. Apostol, "Introduction to Analytic Number Theory," Undergraduate Texts in Mathematics, Springer-Verlag, New York/Heidelberg, 1976.

[BF91] L. Babai and F. Fortnow, Arithmetization: A new method in structural complexity theory, *Comput. Complexity* **1**, No. 1 (1991), 41–66.

[BM88] L. Babai and S. Moran, Arthur–Merlin games: A randomized proof system and a hierarchy of complexity classes, *J. Comput. System Sci.* **36** (1988), 276–276.

[BS96] E. Bach and J. Shallit, "Algorithmic Number Theory," Vol. I, Efficient Algorithms, MIT Press, Cambridge, MA, 1996.

[BCGW92] C. Bajaj, J. F. Canny, T. Garrity, and J. Warren, Factoring rational polynomials over the complex numbers, *SIAM J. Comput.* **22**, No. 2 (1993), 318–331.

[Bea96] A. Beauville, "Complex Algebraic Surfaces," 2nd ed., London Mathematical Society Student Texts, Vol. 34, Cambridge Univ. Press, Cambridge, UK, 1996.

[Bre76] R. P. Brent, Fast multiple-precision evaluation of elementary functions, *J. Assoc. Comput. Mach.* **23**, No. 2 (1976), 242–251.

[Bür00] P. Bürgisser, Cook's versus Valiant's hypothesis, special issue in honor of Manuel Blum's 60th Birthday, *Theoret. Comput. Sci.* **235** (2000).

[CC92] P. J. Cameron and A. M. Cohen, On the number of fixed point free elements in a permutation group, A collection of contributions in honour of Jack van Lint, *Discrete Math.* **106/107** (1992), 135–138.

[Can88] J. F. Canny, Some algebraic and geometric computations in PSPACE, *in* "Proc. 20th ACM Symp. Theory of Computing, Chicago (1988)," ACM Press.

[Coh81] S. D. Cohen, The distribution of Galois groups and Hilbert's irreducibility theorem, *Proc. London Math. Soc. (3)* **43**, No. 2 (1981), 227–250.

[FGM90] N. Fitchas, A. Galligo, and J. Morgenstern, Precise Sequential and parallel complexity bounds for quantifier elimination over algebraically closed fields, *J. Pure Appl. Algebra* **67** (1990), 1–14.

[FJ86] M. D. Fried and M. Jarden, "Field Arithmetic," Ergebnisse der Mathematik und ihrer Grenzgebiete (3), Springer-Verlag, Berlin/New York, 1986.

[Gal73] P. X. Gallagher, The large sieve and probabilistic Galois Theory, *in* "Analytic Number Theory," Proc. Sympos. Pure Math., Vol. XXIV, pp. 91–101, Amer. Math. Soc., Providence, RI, 1973.

[Gal80] P. X. Gallagher, Some consequences of the Riemann hypothesis, *Acta Arith.* **37** (1980), 339–343.

[GKZ94] I. M. Gel'fand, M. M. Kapranov, and A. V. Zelevinsky, "Discriminants, Resultants and Multidimensional Determinants," Birkhäuser, Boston, 1994.

[GK94] P. Gritzmann and V. Klee, On the complexity of some basic problems in computational convexity. II. Volume and mixed volumes, *in* "Polytopes: Abstract, Convex, and Computational (Scarborough, ON, 1993)," NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci., Vol. 440, pp. 373–466, Kluwer Academic, Dordrecht, 1994.

[GW97] R. Guralnick and D. Wang, Bounds for fixed point free elements in a transitive group and applications to curves over finite fields, *Israel J. Math.* **101** (1997), 255–287.

[HW79] G. H. Hardy and E. M. Wright, "An Introduction to the Theory of Numbers," 5th ed., Clarendon Oxford Univ. Press, New York, 1979.

[Har77] R. Hartshorne, "Algebraic Geometry," Graduate Texts in Mathematics, Vol. 52, Springer-Verlag, Berlin/New York.

[Hir94] M. Hirsch, "Differential Topology," corrected reprint of the 1976 original, Graduate Texts in Mathematics, Vol. 33, Springer-Verlag, New York, 1994.

[Jac85] N. Jacobson, "Basic Algebra I," 2nd ed., Freeman, New York, 1985.

[Jon81] J. P. Jones, Classification of quantifier prefixes over Diophantine equations, *Z. Math. Logik Grundlag. Math.* **27** (1981), 403–410.

[Jon82] J. P. Jones, Universal Diophantine equation, *J. Symbolic Logic* **47**, No. 3 (1982), 403–410.

[Kho78] A. G. Khovanskii, Newton polyhedra and the genus of complete intersections, *Funct. Anal.* **12**, No. 1 (1978), 51–61. [Translated from Russian]

[Knu98] D. Knuth, "The Art of Computer Programming. II Seminumerical Algorithms," 3rd ed., Addison–Wesley, Reading, MA, 1998.

[Koi96] P. Koiran, "Hilbert's Nullstellensatz Is in the Polynomial Hierarchy," DIMACS Technical Report 96–27, July 1996. (Note: This preprint considerably improves the published version which appeared in the *Journal of Complexity* in 1996.)

[Koi97] P. Koiran, Randomized and deterministic algorithms for the dimension of algebraic varieties, *in* "Proceedings of the 38th Annual IEEE Computer Society Conference on Foundations of Computer Science (FOCS), Oct. 20–22, 1997," ACM Press.

[KP96] T. Krick and L. M. Pardo, A computational method for Diophantine approximation, *in* "Algorithms in Algebraic Geometry and Applications (Santander, 1994)," Progr. Math., Vol. 143, pp. 193–253, Birkhäuser, Basel, 1996.

[KPS99] T. Krick, L. M. Pardo, and M. Sombra, Sharp arithmetic nullstellensatz, submitted for publication.

[Kus75] A. G. Kushnirenko, A Newton polytope and the number of solutions of a system of k equations in k unknowns, *Usp. Mat. Nauk*. **30**, No. 2 (1975), 266–267.

[LO77] J. Lagarias and A. Odlyzko, Effective versions of the Chebotarev density theorem, *in* "Algebraic Number Fields: L-functions and Galois Properties" (Proc. Sympos. Univ. Durham, Durham, 1975), pp. 409–464, Academic Press, London, 1977.

[LLL82] A. K. Lenstra, H. W. Lenstra, and L. Lovász, Factoring polynomials with rational coefficients, *Math. Ann.* **261**, No. 4 (1982), 515–534.

[Len98] H. W. Lenstra, Finding small degree factors of lacunary polynomials, *in* "Number Theory in Progress, Proceedings of a Meeting in Honor of the 70th Birthday of Andrej Schnizel," W. de Gruyter, to appear.

[Mai00] V. Maillot, Géométrie d'Arakelov des variétés toriques et fibrés en droites intégrables, *Mém. Soc. Math. France*, to appear.

[Mat70] Y. V. Matiyasevich, The diophantineness of enumerable sets, *Sov. Math. Dokl.* **11** (1970), 354–358.

[Mat93] Y. V. Matiyasevich, "Hilbert's Tenth Problem," MIT Press, Cambridge, MA, 1993.

[MR74] Y. V. Matiyasevich and J. Robinson, Two univeral 3-quantifier representations of recursively enumerable sets, *in* "Teoriya Algorifmov i Matematicheskaya Logika (Volume Dedicated to A. A. Markov)," pp. 112–123, Vychislitel'nyĭ Tsentr, Akademiya Nauk SSSR, Moscow. [In Russian]

[Mig92] M. Mignotte, "Mathematics for Computer Algebra," Translated from the French by Catherine Mignotte, Springer-Verlag, New York, 1992.

[Mil76] G. L. Miller, Riemann's hypothesis and tests for primality, *J. Comput. System Sci.* **13**, No. 3 (1976), 300–317.

[Mor97] J. E. Morais, "Resolucion Eficaz de Sistemas de Ecuaciones Polinomiales" [Efficient Solution of Systems of Polynomial Equations], Ph.D. thesis, Univ. Cantabria, Santander, 1997.

[Mum95] D. Mumford, "Algebraic Geometry I. Complex Projective Varieties," reprint of the 1976 edition, Classics in Mathematics, Springer-Verlag, Berlin, 1995.

[NR96] C. A. Neff and J. Reif, An efficient algorithm for the complex roots problem, *J. Complexity* **12**, No. 2 (1996), 81–115.

[Oes79] J. Oesterlé, Versions effectives du théorème de Chebotarev sous l'hypothèse de Riemann généralisée, *Astérisque* **61** (1979), 165–167.

[Pap95] C. H. Papadimitriou, "Computational Complexity," Addison–Wesley, Reading, MA, 1995.

[Pra75] V. R. Pratt, Every prime has a succinct certificate, *SIAM J. Comput.* **4** (1975), 327–340.

[Roj99a] J. M. Rojas, On the complexity of Diophantine geometry in low dimensions, *in* "Proceedings of the 31st Annual ACM Symposium on Theory of Computing (STOC '99, May 1–4, 1999, Atlanta, Georgia)," pp. 527–536, ACM Press, 1999.

[Roj99b] J. M. Rojas, Solving degenerate sparse polynomial systems faster, *J. Symbolic Comput.* **28**, No. 1/2 (1999), 155–186.

[Roj00a] J. M. Rojas, Uncomputably large integral points on algebraic plane curves? Special issue in honor of Manuel Blum's 60th Birthday, *Theoret. Comput. Sci.* **235**, (2000), 145–162.

[Roj00b] J. M. Rojas, Some speed-ups and speed limits for real algebraic geometry, FOCM 1999 special issue, *J. Complexity* **16**, No. 3 (2000), 552–571.

[Roj00c] J. M. Rojas, Algebraic geometry over four rings and the frontier to tractability, *in* "Contemporary Mathematics, Proceedings of a Conference on Hilbert's Tenth Problem and Related Subjects (University of Gent, November 1–5, 1999)" (Jan Denef, Leonard Lipschitz, Thanases Pheidas, and Jan Van Geel, Eds.), Vol. 270, pp. 275–324, AMS Press.

[Sch98] J. Schicho, Rational parametrization of surfaces, *J. Symbolic Comput.* **26**, No. 1 (1998), 1–29.

[Sch82] A. Schnizel, "Selected Topics on Polynomials," Univ. of Michigan Press, Ann Arbor, 1982.

[Sch80] J. Schwartz, Fast probabilistic algorithms for verification of polynomial identities, *J. Assoc. Comput. Mach.* **27** (1980), 701–717.

[Sil99] J. H. Silverman, On the distribution of integer points on curves of genus zero, Special issue in honor of Manuel Blum's 60th Birthday, *Theoret. Comput. Sci.* **2354**, No. 1 (2000), 163–170.

[Sto85] L. Stockmeyer, On approximation algorithms for $\#\mathbf{P}$, *SIAM J. Comput.* **14**, No. 4 (May 1985), 849–861.

[Stu98] B. Sturmfels, Introduction to resultants, *in* "Applications of Computational Algebraic Geometry (San Diego, CA, 1997)," Proc. Sympos. Appl. Math., Vol. 53, pp. 25–39, Amer. Math. Soc., Providence, RI, 1998.

[Tun87] S.-P. Tung, Computational complexities of Diophantine equations with parameters, *J. Algorithms* **8** (1987), 324–336.

[Wei84] P. Weinberger, Finding the number of factors of a polynomial, *J. Algorithms* **5** (1984), 180–186.

[Zac86] S. Zachos, Probabilistic quantifiers, adversaries, and complexity classes: An overview, *in* "Proc. 1st Structure in Complexity Theory Conference," Lecture Notes in Computer Science, Vol. 223, Springer-Verlag, Berlin/New York, 1986.