Dedekind Zeta Zeroes and Faster Complex Dimension Computation*

J. Maurice Rojas[†]
Texas A&M University
College Station, Texas
rojas@math.tamu.edu

Yuyu Zhu[‡]
Texas A&M University
College Station, Texas
zhuyuyu@math.tamu.edu

ABSTRACT

Thanks to earlier work of Koiran, it is known that the truth of the Generalized Riemann Hypothesis (GRH) implies that the dimension of algebraic sets over the complex numbers can be determined within the polynomial-hierarchy. The truth of GRH thus provides a direct connection between a concrete algebraic geometry problem and the **P** vs. **NP** Problem, in a radically different direction from the geometric complexity theory approach to **VP** vs. **VNP**. We explore more plausible hypotheses yielding the same speed-up. One minimalist hypothesis we derive involves improving the error term (as a function of the degree, coefficient height, and x) on the fraction of primes $p \leq x$ for which a polynomial has roots mod p. A second minimalist hypothesis involves sharpening current zero-free regions for Dedekind zeta functions. Both our hypotheses allow failures of GRH but still enable complex dimension computation in the polynomial hierarchy.

CCS CONCEPTS

• **CCS** → Theory of computation, Computational complexity and cryptography; Algebraic complexity theory;

KEYWORDS

polynomial hierarchy, Dedekind zeta, Riemann hypothesis, random primes, height bounds, rational univariate reduction, nullstellensatz, complex dimension

ACM Reference Format:
J. Maurice Rojas and Yuyu Zhu. 2018. Dedekind Zeta Zeroes and Faster Complex Dimension Computation. In *Proceedings of ACM International Symposium on Symbolic and Algebraic Computation (ISSAC'18).* ACM, New York, NY, USA, Article ?, 6 pages. https://doi.org/10.475/123_4

1 INTRODUCTION

The subtlety of computational complexity in algebraic geometry persists in some of its most basic problems. For instance, let $\mathtt{FEAS}_{\mathbb{C}}$ denote the problem of deciding whether an input polynomial system

$$F \in \bigcup_{k,n \in \mathbb{Z}} (\mathbb{Z}[x_1, \ldots, x_n])^k$$

has a complex root. While the implication $\mathtt{FEAS}_{\mathbb{C}} \in \mathbf{P} \Longrightarrow \mathbf{P} = \mathbf{NP}$ has long been known, the inverse implication $\mathtt{FEAS}_{\mathbb{C}} \notin \mathbf{P} \Longrightarrow \mathbf{P} \neq \mathbf{NP}$ remains unknown. Proving the implication $\mathtt{FEAS}_{\mathbb{C}} \notin \mathbf{P} \Longrightarrow \mathbf{P} \neq \mathbf{NP}$ would shed new light on the **P** vs. **NP** Problem, and may be easier than attempting to prove the complexity lower bound $\mathtt{FEAS}_{\mathbb{C}} \notin \mathbf{P}$ (whose truth is still unknown).

Detecting complex roots is the $D = 0$ case of the following more general problem:

$\mathtt{DIM}_{\mathbb{C}}$: Given $(D, F) \in \mathbb{N} \times \bigcup_{k,n \in \mathbb{Z}} (\mathbb{Z}[x_1, \ldots, x_n])^k$, decide whether the complex zero set of F has dimension at least D. ⋄

In particular, $\mathtt{FEAS}_{\mathbb{C}} \notin \mathbf{P} \Longrightarrow \mathtt{DIM}_{\mathbb{C}} \notin \mathbf{P}$. Recall the containment of complexity classes $\mathbf{P} \subseteq \mathbf{NP} \subseteq \mathbf{AM} \subseteq \mathbf{P}^{\mathbf{NP}^{\mathbf{NP}}} \subseteq \mathbf{PSPACE}$, and that the question $\mathbf{P} \overset{?}{=} \mathbf{PSPACE}$ remains open [Pap95, AB09]. That $\mathbf{P} = \mathbf{NP}$ implies the *collapse* $\mathbf{P} = \mathbf{NP} = \mathbf{coNP} = \mathbf{AM} = \mathbf{P}^{\mathbf{NP}^{\mathbf{NP}}}$ is a basic fact from complexity theory (see, e.g., [AB09, Thm. 5.4, pp. 97–98]. (We briefly review these complexity classes in the next section.) $\mathtt{DIM}_{\mathbb{C}}$ (and thus $\mathtt{FEAS}_{\mathbb{C}}$) has been known to lie in **PSPACE** at least since [GH93], and the underlying algorithms have important precursors in [CG84, Can88, Ren92].

But in 1996, Koiran [Koi96] proved that the truth of the Generalized Riemann Hypothesis (GRH) implies that $\mathtt{DIM}_{\mathbb{C}} \in \mathbf{AM}$. In particular, one obtains that the truth of GRH yields the implication $\mathtt{DIM}_{\mathbb{C}} \notin \mathbf{P} \Longrightarrow \mathbf{P} \neq \mathbf{NP}$. Thus, if one can prove that computing the dimension of complex algebraic sets is hard, one can solve the **P** vs. **NP** Problem. An interesting application of Koiran's result is that it is a key step in the proof that the truth of GRH implies that knottedness (of a curve defined by a knot diagram) can be decided in **NP** [Kup14].

Here, we prove that $\mathtt{DIM}_{\mathbb{C}} \in \mathbf{P}^{\mathbf{NP}^{\mathbf{NP}}}$ under either of two new hypotheses: See Theorem 1 below. Each of our hypotheses is implied by GRH, *but can still hold true under certain failures of GRH.*

Remark. *To the best of our knowledge, the only other work on improving Koiran's conditional speed-up has focussed on proving unconditional speed-ups (from* **PSPACE** *to* $\mathbf{P}^{\mathbf{NP}^{\mathbf{NP}}}$ *or* **NP***) for special families of polynomial systems. See, e.g., [Che07, Roj07]. For instance, thanks to the first paper, the special case of* $\mathtt{FEAS}_{\mathbb{C}}$ *involving inputs of the form* $(f, x_1^D - 1)$ *with* $(D, f) \in \mathbb{N} \times \mathbb{Z}[x_1]$ *is* **NP***-complete.* ⋄

To state our first and most plausible hypothesis, let $f \in \mathbb{Z}[x_1]$ be an irreducible polynomial of degree d with coefficients of absolute value at most 2^{σ} for some $\sigma \in \mathbb{N}$. Let $\pi_f(x)$ denote the number of primes p for which the mod p reduction of f has a root mod p and

*Copyright, 2018

[†]Partially supported by NSF grants DMS-1460766 and CCF-1409020.
[‡]Partially supported by NSF grants DMS-1460766 and CCF-1409020.

ISSAC'18, July 2018, New York, USA

ACM ISBN 123-4567-24-567/08/06…$?
https://doi.org/10.475/123_4

$p \leq x$. Note that $\pi_{x_1}(x)$ is thus simply the number of primes $p \leq x$, i.e., the well-known prime-counting function $\pi(x)$. In what follows, *all* O- and Ω- constants are absolute (i.e., they really are constants) and effectively computable.

Modular Root Hypothesis (MRH). *There is a constant* $C > 1$ *such that for any* f *as above we have*

$$\pi_f(x) \geq x\left(\frac{1}{d\log x} - \frac{1}{\exp\left(\frac{(\log x)^{1/C}}{(\log(d^2\sigma+d^3))^C}\right)}\right).$$

for $x = \Omega\left(\exp\left(4(\log(d^2\sigma + d^3))^{2+C^2}\right)\right)$.

That $\pi_f(x)$ is asymptotic to $\frac{x}{s_f \log x}$ for some positive integer $s_f \leq d$ goes back to classical work of Frobenius [Fro96] (see also [LS96] for an excellent historical discussion). More to the point, as we'll see in our proofs, the behavior of π_f is intimately related to the distribution of prime ideals in the ring $\mathcal{O}_K$ of algebraic integers in the number field $K := \mathbb{Q}[x_1]/\langle f\rangle$, and the error term is where all the difficulty enters: MRH is not currently known to be true. However, MRH can still hold even if GRH fails (see Theorem 1 below). In particular, while the truth of GRH implies that the 1/exponential term in our lower bound above can be decreased to $O\left(\frac{d\log(\Delta x)}{\sqrt{x}}\right)$ in absolute value, we will see later that our looser bound still suffices for our algorithmic purposes. (Note that $\frac{1}{\sqrt{x}} = o\left(\frac{1}{\exp((\log x)^{1/C})}\right)$ for any $C > 1$.)

Our second hypothesis is a statement intermediate between MRH and GRH in plausibility. Recall that the *Dedekind zeta function*, $\zeta_K(s)$, is the analytic continuation (to $\mathbb{C} \setminus \{1\}$) of the function $\sum\limits_{\mathfrak{a}} \frac{1}{(N\mathfrak{a})^s}$, where the summation is taken over all integral ideals $\mathfrak{a}$ of $\mathcal{O}_K$ and $N\mathfrak{a}$ is the norm of $\mathfrak{a}$ [IK04]. (So $\zeta_{\mathbb{Q}}(s)$ is the classical *Riemann zeta function* $\zeta(s)$, defined from the sum $\sum\limits_{n=1}^{\infty} \frac{1}{n^s}$.) We call a root $\rho = \beta + \gamma\sqrt{-1}$ (with $\beta, \gamma \in \mathbb{R}$) of ζ_K a **non-trivial zero** if and only if $0 < \beta < 1$. GRH is then following statement:

> (GRH) All the non-trivial zeroes $\rho = \beta + \gamma\sqrt{-1}$ of ζ_K
> lie on the vertical line defined by $\beta = 1/2$. ⋄

Let Δ denote the absolute value of the discriminant of K. Our second hypothesis allows *infinitely many* zeroes off the line $\beta = \frac{1}{2}$, provided they don't approach the boundary of the critical region too quickly (as a function of (d, Δ)). We review the number theory we need in the next section.

Minimalist Dedekind Zero Hypothesis (MDZH). *There is a constant* $C > 4$ *such that for any number field* K*, the Dedekind zeta function* $\zeta_K(s)$ *has* no *zeroes* $\rho = \beta + \gamma\sqrt{-1}$ *in the region*

$$|\gamma| \geq (1 + 4\log\Delta)^{-1}$$
$$\beta \geq 1 - (\log(d\log(3\Delta))^C \log(|\gamma| + 2))^{-1}$$

and no *real zeroes in the open interval* $\left(1 - \log(d\log(3\Delta))^{-C}, 1\right)$.

The main motivation for our two preceding hypotheses is the following chain of implications, which form our main result.

Theorem 1. *The following three implications hold:*
(1) GRH$\Longrightarrow$*MDZH , (2) MDZH*$\Longrightarrow$*MRH , (3) MRH*$\Longrightarrow \mathtt{DIM}_{\mathbb{C}} \in \mathbf{P}^{\mathbf{NP}^{\mathbf{NP}}}$.

We prove Theorem 1 in Section 3. We briefly review some complexity theoretic notation in Section 2.1, and in Section 2.2 we review some algebraic tools we need to relate polynomial systems to number fields. It is important to recall that, like Koiran's original approach in [Koi96], our algorithm is completely distinct from numerical continuation, or the usual computational algebra techniques like Gröbner bases, resultants, or non-Archimedean Newton Iteration. In particular, we use random sampling to study the density of primes p for which the mod p reduction of a polynomial system has roots over the finite field $\mathbb{F}_p$.

2 TECHNICAL BACKGROUND

Our approach begins by naturally associating a number field K to a polynomial system $F = (f_1, \ldots, f_k) \in \mathbb{Z}[x_1, \ldots, x_n]$. Then, the distribution of prime ideals of $\mathcal{O}_K$ forces the existence of complex roots for F to imply (unconditionally) the existence of roots over $\mathbb{F}_p$ for a *positive density* of mod p reductions of F. Conversely, if F has no complex roots, then there are (unconditionally) only finitely many primes p such that the mod p reduction of F has a root over $\mathbb{F}_p$. These observations, along with a clever random-sampling trick that formed the first algorithm for computing complex dimension in the polynomial-hierarchy (assuming GRH), go back to Koiran [Koi96]. Our key contribution is thus isolating the minimal number-theoretic hypotheses ("strictly" more plausible than GRH) sufficient to make a positive density of primes observable via efficient random sampling.

2.1 Some Complexity Theory

Our underlying computational model will be the classical Turing machine, which, informally, can be assumed to be anyone's laptop computer, augmented with infinite memory and a flawless operating system. Our notion of input size is the following:

Definition 1. *The* ***bit-size*** *(or* ***sparse size****) of a polynomial system* $F := (f_1, \cdots, f_k) \in \mathbb{Z}[x_1, \ldots, x_n]$*, is defined to be the total number of bits in the binary expansions of all the coefficients and exponents of the monomial term expansions of all the* f_i.

Recall that an **oracle in A** is a special machine that runs, in unit time, an algorithm with complexity in A. Our complexity classes can then be summarized as follows (and found properly defined in [Pap95, AB09]).

P The family of decision problems which can be done within time polynomial in the input size.

NP The family of decision problems where a "yes" answer can be **certified** within time polynomial in the input size.

#P The family of enumerative problems $\mathcal{P}$ admitting an **NP** problem Q such that the answer to every instance of $\mathcal{P}$ is exactly the number of "yes" instances of Q.

$\mathbf{NP}^{\mathbf{NP}}$ The family of decision problems polynomial-time equivalent to deciding quantified Boolean sentences of the form $\exists x_1 \cdots \exists x_\ell \forall y_1 \cdots \forall y_m \; B(x_1, \ldots, x_\ell, y_1, \ldots, y_m)$.

$\mathbf{P}^{\mathbf{NP}^{\mathbf{NP}}}$ The family of decision problems solvable within time polynomial in the input size, with as many calls to an $\mathbf{NP}^{\mathbf{NP}}$-oracle as allowed by the time bound.

PSPACE The family of decision problems solvable within time polynomial in the input size, provided a number of processors exponential in the input size is allowed.

Finally, let us recall the following important approximation result of Stockmeyer.

Theorem 2 ([Sto85]). *Any enumerative problem $\mathcal{E}$ in #**P** admits an algorithm in $\mathbf{P}^{\mathbf{NP}^{\mathbf{NP}}}$ which decides if the output of an instance of $\mathcal{E}$ exceeds an input $M \in \mathbb{N}$ by a factor of 2.*

One can thus, in the preceding decisional sense, do constant-factor approximation of functions in #**P** within the polynomial-hierarchy.

2.2 Rational Univariate Reduction and an Arithmetic Nullstellensatz

In this section, we develop tools that will reduce the feasibility of polynomial systems to algebra involving "large" univariate polynomials. The resulting quantitative bounds are essential in constructing our algorithm.

Our first lemma is a slight refinement of earlier work on rational univariate reduction (see, e.g., [Can88, Roj00, Mai00]), so we leave its proof for the full version of this paper.

Lemma 1. *Let F be our polynomial system and Z_F denote the zero set of F in $\mathbb{C}^n$. Then there are univariate polynomials $u_1, \cdots, u_n, U_F \in \mathbb{Z}[t]$ and positive integers $r_1, \cdots, r_n$ such that*

1. *The number of irreducible components of Z_F is bounded above by $\deg U_F$, and $\deg(u_i) \leq \deg(U_F) \leq D^n$ for all $1 \leq i \leq n$.*
2. *For any root θ of U_F, we have $F\left(\frac{u_1(\theta)}{r_1}, \cdots, \frac{u_n(\theta)}{r_n}\right) = 0$, and every irreducible component of Z_F contains at least one point that can be expressed in this way.*
3. *The coefficients of U_F have absolute value no greater than $2^{O(D^n[\sigma(F)+n\log D])}$.* □

If F has finitely many roots then $(U_F, u_1, r_1, \ldots, u_n, r_n)$ will capture all the roots of F in the sense above. Let f be the square-free part of U_F. Note that if $p \nmid \mathrm{lcm}(r_1, \cdots, r_n)$ and $f \bmod p$ has a root, then $F \bmod p$ also has a root.

Now consider the following recently refined effective arithmetic version of Hilbert's Nullstellensatz. Recall that the **height** of a polynomial f, denoted by $h(f)$, is defined as the logarithm of the maximum of the absolute value of its coefficients.

Proposition 1 ([DKS13]). *Let $D = \max_i \deg(f_i)$, and $h = \max_i h(f_i)$. Then the polynomial system F has no roots in $\mathbb{C}^n$ if and only if there exist polynomials $g_1, \cdots, g_k \in \mathbb{Z}[x_1, \cdots, x_n]$ and a positive integer α satisfying the Bezóut identity $f_1 g_1 + \cdots + f_k g_k = \alpha$, and*

1. $\deg(g_i) \leq 4nD^n$,
2. $h(\alpha), h(g_i) \leq 4n(n+1)D^n(h + \log k + (n+7)\log(n+1)D)$.

If the mod p reduction of F has a root over $\mathbb{F}_p$, then p divides α. There are at most $1 + \log\alpha$ many prime factors of an integer α, hence

Theorem 3. *If F has no complex root then the mod p reduction of F has a root over $\mathbb{F}_p$ for no more than A_F primes p, where*

$$A_F = 4n(n+1)D^n(h + \log k + (n+7)\log(n+1)D). \quad \square$$

If we can somehow certify that the mod p reduction of F has roots over $\mathbb{F}_p$ for at least $A_F + 1$ many primes p, then we can certify that F has complex roots.

Example. *The following system F of two univariate polynomials:*

$$f_1 = x^{120017} + 4x^{110001} + 19x^{110000} - 3x^{101208} + x^{100000} - 47x^{25018} + 37x^{20017}$$
$$- 188x^{15002} - 893x^{15001} + 148x^{10001} + 703x^{10000} + 141x^{6209} - 47x^{5001} - 111x^{1208} + 37$$
$$f_2 = 19x^{210017} + 76x^{200001} + 361x^{200000} - 57x^{191208} + 19x^{190000} + 2x^{30016} - 7x^{20017}$$
$$+ 8x^{20000} + 38x^{19999} - 6x^{11207} - 28x^{10001} - 133x^{1000} + 2x^{9999} + 21x^{1208} - 7,$$

has a complex root. It is easy to compute that $A_F \approx 1.9567 \times 10^{12}$. However, as it is a small system, we can get a better bound on the Bezóut constant α by computing the determinant of the corresponding Sylvester matrix. Moreover, we can use a finer result due to Robin ([Rob83]) on $\omega(\alpha)$ (the number of prime factors of α).

$$\omega(\alpha) < \frac{\log\alpha}{\log\log\alpha} + \frac{\log\alpha}{(\log\log\alpha)^2} + 2.89726\frac{\log\alpha}{(\log\log\alpha)^3},$$

for $\alpha \geq 3$. Therefore, to determine if F has a $\mathbb{C}$ root, it suffices to check if the number of primes p such that the mod p reduction of F has a root in $\mathbb{F}_p$ is more than 163, 317. In fact, such p comprise roughly 2/3 of the first 163, 317 primes. ⋄

2.3 Prime Ideals

In what follows, p always denotes a prime in $\mathbb{N}$, and $\mathfrak{p}$ a prime ideal in the number ring O_K.

For any number field K, let $\pi_K(x)$ denote the number of $\mathfrak{p}$ satisfying $N\mathfrak{p} \leq x$. Recall that the ideal norm is defined to be $N\mathfrak{a} := |O_K/\mathfrak{a}|$. The classical Prime Ideal Theorem [IK04] states that for any number field K, $\pi_K(x)$ is asymptotic to $\frac{x}{\log x}$.

Let $\pi_F(x)$ be the number of primes p such that the mod p reduction of F has a root over $\mathbb{F}_p$ and $p \leq x$. (So our earlier π_f was the univariate version of π_F.) The main idea behind proving that GRH implies MDZH is an approximation, with an explicit error term, of the weighted prime-power-counting function $\psi_K(x)$ associated to $\pi_K(x)$, defined by

$$\psi_K(x) = \sum_{\mathfrak{p}} \log N\mathfrak{p}.$$

Here the sum is taken over the unramified primes such that $N\mathfrak{p}^m \leq x$ for some m. To start, we first quote the following important lemmas:

Lemma 2 ([LO77], Lemma 7.1). *Let $\rho = \beta + \gamma\sqrt{-1}$ denote a non-trivial zero of ζ_K (so $0 < \beta < 1$). For $x \geq 2$, and $T \geq 2$, define*

$$S(x,T) = \sum_{|\gamma|<T} \frac{x^\rho}{\rho} - \sum_{|\rho|<\frac{1}{2}} \frac{1}{\rho}.$$

Then

$$\psi_K(x) - x + S(x,T) \ll \frac{x\log x + T}{T}\log\Delta + d\log x + \frac{dx\log x\log T}{T}$$
$$+ \log x\log\Delta + dxT^{-1}(\log x)^2.$$

Lemma 3 ([LO77] in the proof of Thm 9.2). *Using the notation above,*

1. *ζ_K has at most one non-trivial zero ρ in the region*

$$|\gamma| \leq (4\log\Delta)^{-1}$$
$$\beta \geq 1 - (4\log\Delta)^{-1}.$$

This zero, if it exists, has to be real and simple. If it exists and we call it β_0 then it must satisfy

$$\frac{x^{1-\beta_0}}{1-\beta_0} + \frac{1}{1-\beta_0} = x^{\sigma}\log x \le x^{1/2}\log x$$

for some $0 \le \sigma \le 1-\beta_0$.

(2) *For $\rho \neq \beta_0$, we have*

$$\sum_{\substack{\rho\neq 1-\beta_0\\ |\rho|<\frac{1}{2}}} \left(\frac{x^{\rho}}{\rho} - \frac{1}{\rho}\right) \ll x^{1/2} \sum_{\substack{\rho\neq 1-\beta_0\\ |\rho|<\frac{1}{2}}} \left|\frac{1}{\rho}\right| \ll x^{1/2}(\log\Delta)^2$$

(3) *If we have further that $T \ge 2$ then*

$$\sum_{\substack{|\rho|\ge\frac{1}{2}\\ |\gamma|<T}} \left|\frac{1}{\rho}\right| \ll \log T\log(\Delta T^{d})$$

Remark. *An earlier unconditional zero-free region is the following ([LO77]):*

$$|\gamma| \ge (1+4\log\Delta)^{-1}$$
$$\beta \ge 1-\varepsilon(\log\Delta+\log(|\gamma|+2))^{-1},$$

for some constant $\varepsilon > 0$. It is easily checked that for any fixed C (and any sufficiently large d and Δ) the preceding region is strictly contained in the zero-free region of MDZH. Unfortunately, the unconditional region of [LO77], and even the best current unconditional refinements, are too small to guarantee that our upcoming algorithm is in the polynomial-hierarchy. ⋄

Remark. *We call the β_0 from Lemma 2 a* ***Siegel-Landau zero****. Observe that β_0 is a potential counterexample to GRH since it is known that*

$$\beta_0 \ge 1-(4\log\Delta)^{-1},$$

and the right-hand side is at least $3/4$ for suffcently large Δ, thus contradicting GRH. By using Lemma 3 in the following discussion, we take into account the possibility of a Siegel-Landau zero. ⋄

Proposition 2. *Assuming MDZH with constant C, there is an effectively computable positive function $c_2(C)$ such that if*

$$x \ge \exp\left(4(\log\log(3\Delta))^2\log(d\log(3\Delta))^{C^2}\right)$$

then

$$\psi_K(x) = x - \frac{x^{\beta_0}}{\beta_0} + R(x)$$

where

$$|R(x)| \le x\exp\left(-c_2(C)\frac{(\log x)^{1/C}}{(\log(d\log(3\Delta)))^{C}}\right)$$

and the term $\frac{x^{\beta_0}}{\beta_0}$ only occurs if $\zeta_K(s)$ has a Siegel-Landau zero β_0.

Proof. By simply applying the Lemma 3, we have

$$S(x,T) - \frac{x^{\beta_0}}{\beta_0} \le \frac{x^{1-\beta_0}}{1-\beta_0} + \frac{1}{1-\beta_0} + \sum_{\substack{\rho\neq 1-\beta_0\\ |\rho|<\frac{1}{2}}}\left(\frac{x^{\rho}}{\rho}-\frac{1}{\rho}\right) + \sum_{\substack{|\rho|\ge\frac{1}{2}\\ |\gamma|<T}}\frac{x^{\rho}}{\rho}$$
$$\ll x^{1/2}\log x + x^{1/2}(\log\Delta)^2 + \sum_{\substack{|\rho|\ge\frac{1}{2}\\ |\gamma|<T}}\frac{x^{\rho}}{\rho}$$
$$\ll x^{1/2}\log x + x^{1/2}(\log\Delta)^2 + \log T\log(\Delta T^{d}) \max_{\substack{|\rho|\ge\frac{1}{2}\\ |\gamma|<T}} |x^{\rho}|.$$

On the other hand, let $\rho = \beta + i\gamma$ be a non-trivial zero of $\zeta_K(s)$ with $|\gamma| \le T$, and ρ is not a Siegel-Landau zero. As MDZH assumes a zero-free region dependent on a given constant C,

$$|x^{\rho}| = x^{\beta} \le x\exp\left(-c_3\frac{\log x}{\log\log(3\Delta)+(\log(d\log(3\Delta)))^{2C}\log T}\right)$$

for some constant c_3. Now take

$$T = \exp\left((\log(d\log(3\Delta)))^{-C}(\log x)^{1-1/C} - \log\log(3\Delta)\right).$$

The estimate of the theorem then follows from the above computation, and Lemma 2. □

3 THE PROOF OF THEOREM 1

Since GRH trivially implies MDZH, Assertion (1) tautologically true. So we now proceed with proving Assertions (2) and (3).

3.1 The Proof of Assertion (2): MDZH $\Longrightarrow$ MRH

Define $\theta_K(x) = \sum\log N\mathfrak{p}$ where the summation is over all the unramified prime $\mathfrak{p}$ such that $N\mathfrak{p} \le x$. There are at most d ideals $\mathfrak{p}^m$ of a given norm in K, hence

$$0 \le \psi_K(x) - \theta_K(x) = \sum_{N\mathfrak{p}^m\le x,\, m\ge 2}\log N\mathfrak{p}$$
$$\le \sum_{m=2}^{\log_2 x} dx^{1/m}\log x \le 3d\sqrt{x}\log x.$$

The error term $R(x)$ still dominates this discrepancy, so the estimates in Proposition 2 still holds when $\psi_K(x)$ is replaced by $\theta_K(x)$. By a standard partial summation trick we have:

$$\left|\pi_K(x) - \frac{x}{\log x}\right| \le \frac{x^{\beta_0}}{\beta_0\log x} + O\left(x\exp(-\frac{(\log x)^{1/C}}{(\log(d\log(3\Delta)))^{C}})\right),$$

for

$$x \ge \exp\left(4(\log\log(3\Delta))^2\log(d\log(3\Delta))^{C^2}\right).$$

By the last assertion of MDZH, the error arising from the possible existence of the Siegel-Landau zero β_0 is dominated by $R(x)$ for x in the range of x we are using. Therefore,

$$\pi_K(x) \ge x\left(\frac{1}{\log x} - O\left(\exp\left(-\frac{(\log x)^{1/C}}{(\log(d\log(3\Delta)))^{C}}\right)\right)\right).$$

Let $W(p)$ be the number of linear factors of f mod p. The key fact we observe now is that if $p \nmid \Delta$ then $W(p)$ equals the number of prime ideals $\mathfrak{p}$ of K of degree 1 that lie over p. Thus, $\sum_{p\le x} W(p)$ counts the number of $\mathfrak{p}$ of degree 1 with norm up to x. As the prime ideals of degree greater than 1 must lie over a prime number $p \leq x^{1/2}$, and there are no more than d such p, we have

$$\pi_K(x) - \sum_{p \leq x} W(p) = O(dx^{1/2}).$$

Note that if p divides the discriminant of f, the correspondence between $\mathfrak{p}$ of degree 1, and the linear factors of f mod p will break. But there are no more than $\log \Delta$ such p. However, the error term coming from $R(x)$ still dominates. Therefore, $\sum_{p \leq x} W(p)$ satisfies the same estimate as $\pi_K(x)$.

Let $r(p) = 1$ if f has a root in $\mathbb{F}_p$ and 0 otherwise. As f is irreducible of degree d, so f mod p is non-trivial. Then

$$\pi_f(x) = \sum_{p \leq x} r(p) \geq \sum_{p \leq x} W(p)/d,$$

and MRH thus follows upon recalling that $\log \Delta = O(d^2\sigma + d^3)$ [Roj01]. □

Remark. *We will deal later with square-free polynomial that are possibly reducible. In this case, we write $f(x) = \prod f_i(x)$, with $f_i(x)$ irreducible, and apply the same argument to each summand of*

$$\mathbb{Q}[x]/\langle f(x)\rangle \cong \oplus \mathbb{Q}[x]/\langle f_i(x)\rangle.$$

Therefore, we can replace the "irreducible" assumption in MRH with "square-free". ⋄

3.2 The Proof of Assertion (3): MRH $\Longrightarrow$ $\mathtt{DIM}_{\mathbb{C}} \in \mathbf{P}^{\mathbf{NP}^{\mathbf{NP}}}$

Let $u_1, \cdots, u_n, U_F \in \mathbb{Z}[t]$ and $r_1, \cdots, r_n$ respectively be the polynomials and integers arising from a rational univariate reduction of F. Let $K = \mathbb{Q}[x]/\langle f\rangle$, where f is the square-free part of U_F. Then $d = \deg f \leq D^n$. Moreover, assuming the coefficients of U_F have absolute value no greater than $2^{\sigma(F)}$, we can effectively bound the discriminant of f: $\log \Delta = O((\deg U_F)^2\sigma(U_F) + (\deg U_F)^3)$ [Roj01]. Note that if $p \nmid \operatorname{lcm}(r_1, \cdots, r_n)$, then Assertion (2) of Lemma 1 continues to hold modulo p. That is, if in addition f has a root in $\mathbb{F}_p$, then F has a root over $\mathbb{F}_p$. Hence we have $\pi_F(x) \geq \pi_f(x)$.

Recall from Theorem 3 that if F has no complex solutions, then the mod p reduction of F has a root over $\mathbb{F}_p$ for at most A_F many primes p. On the other hand, we have the following result:

Proposition 3. *If F has a complex root then there is a positive function $t(F)$ such that $\pi_F(x) \geq 7A_F$ for every $x \geq t(F)$. In particular, $\log t(F)$ is polynomial in the bit-size of F.*

Proof of Proposition 3: Recall from MRH that the asymptotic formula for $\pi_f(x)$, and thus $\pi_F(x)$, only holds for x sufficiently large. In particular, we need

$$x \geq \exp\left(4(\log\log(3\Delta))^2 \log(d\log(3\Delta))^{C^2}\right).$$

Let t_1 denote this lower bound and let $\sigma(F)$ denote the bit-size of F. It is easy to see that for $C \geq 2$,

$$\begin{aligned}\log t_1 &\leq O\left(\log(D^{3n}(\sigma(F) + n\log D))^{C^2}\right)\\ &= O\left((3\sigma(F)^2 + 2\log\sigma(F))^{C^2}\right) = O\left(\sigma(F)^{4C^2}\right),\end{aligned}$$

which is polynomial in $\sigma(F)$.

On the other hand, by applying the numerical bounds from Lemma 1, and MRH with constant C, we see that $\pi_F(x) \geq 7A_F$ if:

$$\begin{aligned}&x\left(\frac{1}{d\log x} - \exp\left(-\frac{(\log x)^{1/C}}{(\log(d\log(3\Delta)))^C}\right)\right)\\ &\quad\geq 28n(n+1)D^n(h + \log k + (n+7)\log(n+1)D).\end{aligned}$$

Necessarily,

$$\frac{1}{D^n}\frac{x}{\log x} \gg x\exp(-\frac{(\log x)^{1/C}}{(\log(D^n\log\Delta))^C})(n+k)^2D^{n+1}(\sigma(F) + n\log n)).$$

Now with $\log\Delta = O(\deg U_F\sigma(U_F) + d^2) = O(D^{2n}(\sigma(F) + n\log D))$, and $n\log D \leq (n + \log D)^2 \leq \sigma(F)^2$, we have

$$\begin{aligned}&\Leftarrow \frac{x}{\log x} \gg x\exp(-\frac{(\log x)^{1/C}}{(2\log(D^{3n}\sigma(F)^2)^C})(n+k)^2D^{2n+1}\sigma(F)^2,\\ &\Leftarrow \log x \gg \log\log x + \log x - \frac{(\log x)^{1/C}}{(2\log(D^{3n}\sigma(F)^2)^C} + 7\sigma(F)^2,\\ &\Leftarrow \frac{(\log x)^{1/C}}{(6\sigma(F))^{2C}} \gg \log\log x + 7\sigma(F)^2,\end{aligned}$$

which holds if $\log x \geq \log t_2 := O(\sigma(F)^{4C^2})$. The proposition follows by letting $t(F) := \max(t_1, t_2)$. □

Continuing our proof of Assertion (3) of Theorem 1, consider the following algorithm:

```
PHFEAS
Input   A $k \times n$ polynomial system $F$ with integer coefficients.
Output  A true declaration whether $F$ has a complex root.
Step 1  Compute $A_F$ and $t(F)$ from Theorem 3 and Proposition 3.
Step 2  Use Stockmeyer's algorithm as in Theorem 2, to approximate the number $M$ of primes $p \in \{1, \cdots, t(F)\}$,
        such that the mod $p$ reduction of $F$ has a root over $\mathbb{F}_p$.
Step 3  If $M > 3A_F$, then declare that $F$ has a complex root.
        Otherwise, declare that $F$ has no complex root.
```

Since $\mathtt{DIM}_{\mathbb{C}}$ can be reduced in **BPP** to $\mathtt{FEAS}_{\mathbb{C}}$, and **BPP** ⊆ **AM** [Pap95, AB09], it suffices to prove that algorithm PHFEAS is correct and runs in time $\mathbf{P}^{\mathbf{NP}^{\mathbf{NP}}}$.

Toward this end, observe that if F has no complex root, then there are no more than A_F primes p such that the mod p reduction of F has a root over $\mathbb{F}_p$. By Proposition 3 and assuming MRH, if F has a complex root, then there are at least $7A_F$ primes $p \leq t(F)$ such that F mod p has a root. Such primes have bit-size no greater than $O(\log t(F))$. It is also easy to check that $\log A_F$ is also polynomial in $\sigma(F)$. Moreover, primality checking can be done in **P**, and the existence of roots of F over $\mathbb{F}_p$ can be done in **NP**. Hence the number of primes we are approximating is computable in **#P**. So the algorithm is correct and runs in time $\mathbf{P}^{\mathbf{NP}^{\mathbf{NP}}}$. □

REFERENCES

[AB09] Sanjeev Arora and Boaz Barak, *Computational complexity. A modern approach.* Cambridge University Press, Cambridge, 2009.

[BS96] Bach, Eric and Shallit, Jeff, *Algorithmic Number Theory, Vol. I: Efficient Algorithms,* MIT Press, Cambridge, MA, 1996.

[Can88] John F. Canny. Some algebraic and geometric computations in pspace. In *Proc.20th ACM Symp. Theory of Computing*, 1988.

[Che07] Qi Cheng, *"Derandomization of Sparse Cyclotomic Integer Zero Testing,"* Proceedings of FOCS 2007, IEEE Press, 2007, pp. 74–80.

[CG84] Chistov, Alexander L., and Grigoriev, Dima Yu, *"Complexity of Quantifier Elimination in the Theory of Algebraically Closed Fields,"* Lect. Notes Comp. Sci. 176, Springer-Verlag (1984).

[DKS13] Carlos D'Andrea, Teresa Krick, and Martin Sombra. Heights of Varieties in Multiprojective Spaces and Arithmetic Nullstellensatze. *Annales Scientifiques de l'ENS*, pages 549–627, 2013.

[Fro96] F. G. Frobenius, *Über Beziehungen zwischen den Primidealen eines algebraischen Körpers und den Substitutionen seiner Gruppe,* Sitzungsberichte der Königlich Preußischen Akademie der Wissenschaften zu Berlin (1896), pp. 689–703; Gesammelte Abhandlungen II, 719–733.

[GH93] Marc Giusti and Joos Heintz, *"La détermination des points isolés et de la dimension d'une variété algébrique peut se faire en temps polynomial,"* Computational algebraic geometry and commutative algebra (Cortona, 1991), pp. 216–256, Sympos. Math., XXXIV, Cambridge University Press, Cambridge, 1993.

[IK04] Henryk Iwaniece and Emmanuel Kowalski, *Analytic Number Theory,* Colloquium Publications, vol. 53, American Mathematical Society, 2004.

[Koi96] Pascal Koiran, Hilbert's Nullstellensatz is in the Polynomial Hierarchy. *DIMACS Technical Report 96-27*, 27, 1996.

[Kup14] Greg Kuperberg, *"Knottedness is in NP, modulo GRH,"* Adv. Math. 256 (2014), pp. 493–506.

[LO77] Jeff Lagarias and Andrew Odlyzko. Effective Versions of the Chebotarev Density Theorem. In *Algebraic Number Fields: L-functions and Galois Properties*. Proc. Sympos. Univ. Durham, Durham, 1977.

[LS96] P. Stevenhagen and H. W. Lenstra, Jr., *"Chebotarëv and his Density Theorem,"* The Mathematical Intelligencer, Vol. 18, No. 2, 1996, Springer-Verlag, New York.

[Mai00] Vincent Maillot, *"Géométrie D'Arakelov Des Variétés Toriques et Fibrés en Droites Intégrables,* Mém. Soc. Math. France (N.S.), No. 80 (2000).

[Pap95] Christos H. Papadimitriou, *Computational Complexity,* Addison-Wesley, 1995.

[Pla84] David A. Plaisted. New NP-Hard and NP-Complete Polynomial and Integer Divisibility Problems. *Theoret. Comput. Sci*, 31(1-2):125–138, 1984.

[Ren92] James Renegar, *"On the computational complexity and geometry of the first-order theory of the reals. I, II, III,"* J. Symbolic Comput. **13** (1992), no. 3, pp. 255–352.

[Rob83] Guy Robin. Estimation de la fonction de Tchebychef θ. In *Acta Arithmetica*, 1983.

[Roj00] J. Maurice Rojas, *"Algebraic Geometry Over Four Rings and the Frontier to Tractability,"* Contemporary Mathematics, vol. 270, pp. 275–321, AMS Press (2000).

[Roj01] J. Maurice Rojas. Computational Arithmetic Geometry I: Sentences Nearly in the Polynomial Hierarchy. *J. Comput. System Sci.*, 62(2):216–235, March 2001.

[Roj07] J. Maurice Rojas, *"Efficiently Detecting Subtori and Torsion Points,"* proceedings of MAGIC 2005 (Midwest Algebra, Geometry, and their Interactions Conference, Oct. 7-11, 2005, Notre Dame University, Indiana), edited by A. Corso, J. Migliore, and C. Polini), pp. 213–233, Contemporary Mathematics, vol. 448, AMS Press, 2007.

[Sta74] H.M. Stark. Some Effective Cases of the Brauer-Siegel theorem. *Inventiones math.*, 23:135–152, 1974.

[Sto85] Larry Stockmeyer. On approximation algorithms for #P. *SIAM Journal of Computing*, pages 849–861, 1985.