Dedekind Zeta Functions and the Complexity of Hilbert's Nullstellensatz

J. Maurice Rojas*

Abstract

Let **HN** denote the problem of determining whether a system of multivariate polynomials with integer coefficients has a complex root. It has long been known that $\mathbf{HN} \in \mathbf{P} \Longrightarrow \mathbf{P} = \mathbf{NP}$ and, thanks to recent work of Pascal Koiran, it is now known that the truth of the **Generalized Riemann Hypothesis (GRH)** yields the inverse implication $\mathbf{HN} \notin \mathbf{P} \Longrightarrow \mathbf{P} \neq \mathbf{NP}$. We show that the assumption of GRH in the latter implication can be replaced by any one of three weaker hypotheses from analytic number theory. In particular, all our hypotheses still hold even under certain failures of GRH (including the presence of Siegel-Landau zeroes). We thus obtain a new application of Dedekind zero estimates to computational algebraic geometry. Along the way, we also derive a new and sharper explicit estimate on rational univariate reduction and employ some new (unpublished) analytic estimates of Silberman, both of which may be of independent interest. Our results also extend easily to the harder problem of determining the dimension of a complex algebraic set.

1 Introduction and Main Results

Deciding whether a system of multivariate polynomial equations has a solution is arguably the most fundamental problem of algebraic complexity. Over the ring $\mathbb{Z}/2\mathbb{Z}$ this problem defines the famous complexity class **NP** and is the subject of much interest in proof systems theory (see, e.g., [BIKPP96]). Over the complex numbers this problem is a cornerstone of computational algebraic geometry and is the defining problem of the complexity class $\mathbf{NP}_{\mathbb{C}}$ of the recent BSS computational model over $\mathbb{C}$ [BCSS98]. Let **HN** denote the problem of determining whether a multivariate system of polynomials with **integer** coefficients has a **complex** root. It has been known at least since the 1980's that $\mathbf{HN} \in \mathbf{PSPACE}$ (see, e.g., [CG84, Can88, Roj00]), and that the special case of two univariate polynomials is already **NP**-hard [Pla84].

Remark 1 *Recall the following containments of complexity classes:*

$$\begin{tikzcd}[column sep=small]
& \mathbf{RP} \arrow[rr, phantom, "\subseteq"] \arrow[dr, phantom, sloped, "\subseteq"] & & \mathbf{NP} \arrow[rr, phantom, "\subseteq"] \arrow[dr, phantom, sloped, "\subseteq"] & & \mathbf{NP}^{\mathbf{NP}} \arrow[dr, phantom, sloped, "\subseteq"] & \\
\mathbf{P} \arrow[ur, phantom, sloped, "\subseteq"] \arrow[dr, phantom, sloped, "\subseteq"] & & \mathbf{BPP} \arrow[rr, phantom, "\subseteq"] & & \mathbf{AM} \arrow[dr, phantom, sloped, "\subseteq"] & & \mathbf{P}^{\mathbf{NP}^{\mathbf{NP}}} \subseteq \cdots \subseteq \mathbf{PSPACE} \subseteq \mathbf{EXPTIME} \\
& \mathbf{coRP} \arrow[rr, phantom, "\subseteq"] \arrow[ur, phantom, sloped, "\subseteq"] & & \mathbf{coNP} \arrow[rr, phantom, "\subseteq"] & & \mathbf{coNP}^{\mathbf{NP}} \arrow[ur, phantom, sloped, "\subseteq"] &
\end{tikzcd}$$

and that the properness of **every** *inclusion above is a major open problem. In particular, even the inclusion* $\mathbf{P} \subseteq \mathbf{PSPACE}$ *is not known to be proper [Zac86, BM88,*

*Department of Mathematics, Texas A&M University, TAMU 3368, College Station, Texas 77843-3368, USA. e-mail: `rojas@math.tamu.edu` , web page: `http://www.math.tamu.edu/~rojas` .
This research was partially supported by NSF grant DMS-0211458 and a grant from the Texas A&M College of Science.

BF91, Pap95]. The definitions of the aforementioned complexity classes are reviewed briefly in Section 2.2 below. $\diamond$

Let **DIM** denote the problem of deciding whether, for an input $d \in \mathbb{N} \cup \{0\}$ and $f_1, \ldots, f_k \in \mathbb{Z}[x_1, \ldots, x_n]$, the complex zero set of $F := (f_1, \ldots, f_k)$ has dimension d or greater. (So **HN** is merely the special case $d = 0$ of **DIM**.) Here we use analytic number theory to get a surprisingly simple and fast algorithm for **DIM** completely different from the usual Gröbner basis [CGH89], resultant [EM99, HW00], or homotopy methods [SVW01, Lec03] of computational algebraic geometry. Our main algorithms (cf. Section 3) yield, under a plausible number-theoretic hypothesis, the following characterization of the $\mathbf{P} \stackrel{?}{=} \mathbf{NP}$ problem:

$(\star)$ $$\mathbf{DIM} \notin \mathbf{P} \Longrightarrow \mathbf{P} \neq \mathbf{NP}.$$

The (slightly sharpened) inverse implication $\mathbf{HN} \in \mathbf{P} \Longrightarrow \mathbf{P} = \mathbf{NP}$ is well-known [GJ79, Pla84], but the implication $(\star)$ above was known previously only under the assumption of the **Generalized Riemann Hypothesis (GRH)** [Koi97]. Our number-theoretic hypotheses can continue to hold even if GRH fails in certain ways, and this (along with the definition of GRH) is detailed in Section 1.1 below.

Our approach begins by naturally associating a finite algebraic extension K of $\mathbb{Q}$ to any polynomial system F. Then, if the prime ideals in the ring of integers $\mathcal{O}_K$ of K are sufficiently well behaved, we can use a randomized sampling trick to relate the existence of complex roots of F to the existence of roots of "many" mod p reductions of F. This leads to a fast algorithm for **HN** and we can then solve **DIM** by adding more and more random linear equations to F (cf. Remark 2 of Section 3.2), eventually deciding no more than n instances of **HN**. Our hypotheses — **DZH**, **GIPIT**, and **RIPIT** (defined fully in Section 1.1 below) — are three successively more plausible statements encoding the quantitative behavior we require from the prime ideals of $\mathcal{O}_K$. For instance, consider the following two statements:

> (G) As $t \longrightarrow \infty$, the number of primes in the closed interval $[1+t^3, (t+1)^3]$ is asymptotic to $\frac{3t^2}{\log t}$.
>
> (R) For all N sufficiently large, at least 1% of the $t \in \{1, \ldots, N\}$ are such that the closed interval $[1+t^3, (t+1)^3]$ contains at least $1 + \frac{(t+1)^{1.5}}{2}$ primes.

Statement (G), which has been known at least since work of Selberg in 1943 [Sel43, Pg. 161], clearly implies (R). GIPIT and RIPIT are then simply refined quantitative extensions of (G) and (R), respectively, to prime ideals in arbitrary $\mathcal{O}_K$.

Theorem 1 *The following implications hold:*

(1) RIPIT $\Longrightarrow \mathbf{DIM} \in \mathbf{P}^{\mathbf{NP}^{\mathbf{NP}}}$	*(3) GRH $\Longrightarrow$ DZH*
(2) GIPIT $\Longrightarrow \mathbf{DIM} \in \mathbf{AM}$	*(4) DZH $\Longrightarrow$ GIPIT*
	(5) GIPIT $\Longrightarrow$ RIPIT

In particular, the truth of RIPIT yields the implication $\mathbf{DIM} \notin \mathbf{P} \Longrightarrow \mathbf{P} \neq \mathbf{NP}$*; and DZH can hold even under certain failures of GRH (cf. Theorem 4 of Section 1.1 below).*

The algorithms underlying Theorem 1 are detailed in Section 3 and are based on the following quantitative result relating prime distributions and solvability over the complex numbers and finite fields.

Definition 1 *For any* $f_1,\ldots,f_k \in \mathbb{Z}[x_1,\ldots,x_n]$*, let* $F := (f_1,\ldots,f_k)$ *and define* $\sigma(F)$*, the* **sparse size** *(or* **bit-size***)* **of** F*, 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*.* $\diamond$

Theorem 2 *For any* F *as defined above, there are positive integers* a_F*,* t_F*,* C_F*,* t'_F*, and* C'_F *such that the following assertions hold:*

1. *F has no complex root $\Longrightarrow$ the mod p reduction of F has a root in $(\mathbb{Z}/p\mathbb{Z})^n$ for at most a_F primes p. In particular,* $\log a_F = O(\sigma(F)^2)$*.*
2. *F has at least one complex root $\Longrightarrow$ for all integers $t \geq t_F$, there is a prime $p \in \{1+t^{C_F},\ldots,(t+1)^{C_F}\}$ such that the mod p reduction of F has a root in $(\mathbb{Z}/p\mathbb{Z})^n$.*
3. $C_F \leq 2^{1.45\sigma(F)^2}$ *unconditionally.*
4. *GIPIT* $\Longrightarrow$ C_F *and* $\log t_F$ *are in* $O(\sigma(F)^c)$ *for some absolute constant* $c>0$*.*
5. *GRH* $\Longrightarrow$ *we can take* $C_F = 2+\varepsilon$ *for any* $\varepsilon > 0$*, and* $\log t_F = O(\sigma(F)^2)$*.*
6. *There is an absolute constant $\delta > 0$ such that the following stochastic variation on Assertion (2) holds:*
   F has at least one complex root $\Longrightarrow$ for all integers $N \geq t \geq t'_F$, a fraction of at least δ of the closed intervals $\left[1+t^{C'_F},(t+1)^{C'_F}\right] \subset \left[1+(t'_F)^{C'_F},(N+1)^{C'_F}\right]$ contain a prime p such that the mod p reduction of F has a root in $(\mathbb{Z}/p\mathbb{Z})^n$.
   In particular, RIPIT $\Longrightarrow$ C'_F and $\log t'_F$ are in $O(\sigma(F)^{c'})$ for some absolute constant $c' > 0$.

Note: *Throughout this paper, all O-constants and Ω-constants (with the exception of δ, c, and c'), are absolute and effectively computable.* $\diamond$

Assertions (2)–(6) appear to be new. Assertion (1) was observed earlier by Pascal Koiran [Koi96, Thm. 5] (following easily from earlier work of János Kollár [Kol88]) and improved upper bounds on a_F were given in [Roj00, Sec. 6.1.6, Rem. 12]. A weaker version of Assertion (5) (with $C_F = 3$) was derived with explicit upper bounds for t_F and C_F in [Roj00, Sec. 6.1.6, Rem. 13], and the bound $C_F < \infty$ was alluded to at the end of Section 2 in [Koi96]. In particular, the current best **unconditional** results from number theory (e.g., those of [H-B77, BO01]) appear to leave t_F and t'_F completely unknown, and C_F and C'_F too large to be algorithmically useful.

One may then wonder if one could dispense with the randomization implicit in Assertions (1) and (2) above and instead simply check the solvability of F over $\mathbb{Z}/p\mathbb{Z}$ for a number of primes polynomial in $\sigma(F)$, thus obtaining an algorithm in $\mathbf{P}^{\mathbf{NP}}$ for **HN**. Unfortunately, the following family of examples shows that such a simplification is not possible.

Example 1 *[Koi96, Thm. 10] For $n \geq 1$, let P_n be the product of the first n prime numbers and consider $F := (x^{P_n} - 1, x - P_n)$. Then F clearly has no roots in $\mathbb{C}$ and $\sigma(F) = O(n \log n)$. (The latter fact follows easily from the Prime Number Theorem, stated in Section 1.1 below.) However, the number of primes p for which the mod p reduction of F has a root is at least 2^n, which is clearly exponential in $\sigma(F)$. This abundance of primes follows from the fact (observed by Noam Elkies around 1996) that the number of prime factors of $P_n^{P_n} - 1$ is at least 2^n [Koi96, Lem. 4].* $\diamond$

We also point out that while the possibility that $\mathbf{HN} \in \mathbf{P}^{\mathbf{NP}}$ still remains, Pascal Koiran has observed earlier that the possibility that $\mathbf{HN} \in \mathbf{NP}$ is rather unlikely [Koi96, Sec. 6].

The final new result we state is an effective version of rational univariate reduction (a.k.a. the effective primitive element theorem). Our result, while stronger than necessary for its application in proving Assertions (2)–(5) of Theorem 2, is of independent interest because it sharpens many earlier bounds by an exponential factor (e.g., [Roj00, Thms. 5 and 7] and [Can87, FGM90]) and removes the various hypotheses present in other polytopal bounds like [Mai00, Cor. 8.2.3].

Theorem 3 *Let $f_1, \ldots, f_k \in \mathbb{Z}[x_1, \ldots, x_n]$, $F := (f_1, \ldots, f_k)$, $D := \max_i \deg f_i$, and let V_F denote the volume of the convex hull of[1] the union of $\{\mathbf{O}, e_1, \ldots, e_n\}$ (the origin and the standard basis vectors of $\mathbb{R}^n$) and the set of all exponent vectors of the monomial term expansion of F. Finally, let Z_F denote the zero set of F in $\mathbb{C}^n$. Then there are univariate polynomials $h_1, \ldots, h_n, \hat{h}_F \in \mathbb{Z}[t]$ and positive integers $r_1, \ldots, r_n$ with the following properties:*

1. *The number of irreducible components of Z_F is bounded above by $\deg \hat{h}_F$; and $\deg h_1, \ldots, \deg h_n \leq \deg \hat{h}_F \leq V_F$.*
2. *For any root θ of $\hat{h}_F$ we have $F\left(\frac{h_1(\theta)}{r_1}, \ldots, \frac{h_n(\theta)}{r_n}\right) = \mathbf{O}$ and every irreducible component of Z_F contains at least one point that can be expressed in this way.*
3. *$\sigma(r_1), \sigma(h_1) \ldots, \sigma(r_n), \sigma(h_n) = O(V_F^5 \sigma(\hat{h}_F))$ and $\sigma(\hat{h}_F) = O(V_F[\sigma(F) + n \log D])$.*

Note: *Throughout this paper, n-dimensional volume $\mathrm{Vol}(\cdot)$ is normalized so that the n-dimensional unit cube has volume $n!$.* $\diamond$

Note that $V_F \leq D^n$ since the underlying polytope lies in a suitable scaled standard n-simplex. In particular, we improve all earlier bounds which were multiples of $D^{O(n)}$ (e.g., those based on Bézout's Theorem or its multihomogeneous/multigraded versions), and our bounds are frequently much sharper in practice. Theorem 3 is proved in Section 4.1.

1.1 Zeta Functions and Related Hypotheses

Primordial versions of the connection between analysis and number theory are not hard to derive from scratch and have been known since the 19th century. For example,

[1] i.e., smallest convex set containing...

letting $\zeta(s) := \sum_{n=1}^{\infty} \frac{1}{n^s}$ denote the usual **Riemann zeta function** (for any real number $s>1$), one can easily derive with a bit of calculus [TF00, pp. 30–32] that

$$\zeta(s)=\prod_{p \text{ prime}} \frac{1}{1-\frac{1}{p^s}} \text{ and thus } -\frac{\zeta'(s)}{\zeta(s)}=\sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s},$$

where Λ is the classical Mangoldt function which sends n to $\log p$ or 0, according as $n = p^m$ for some prime p (and some positive integer m) or not. For a deeper connection, recall that $\pi(x)$ denotes the number of primes (in $\mathbb{N}$) $\leq x$ and that the **Prime Number Theorem (PNT)** is the asymptotic formula $\pi(x) \sim \frac{x}{\log x}$ for $x \longrightarrow \infty$. Remarkably then, the first proofs of PNT, by Hadamard and de la Vallée-Poussin (independently, in 1896), were based essentially on the fact that $\zeta(\beta+i\gamma)$ has **no** zeroes on the vertical line $\beta=1$.[2]

More precisely, writing $\rho=\beta+i\gamma$ for real β and γ, recall that ζ admits an analytic continuation to the complex plane sans the point 1 [TF00, Sec. 2].[3] In particular, the only zeroes of ζ outside the **critical strip** $\{\rho=\beta+i\gamma \mid 0<\beta<1\}$ are the so-called **trivial** zeroes $\{-2,-4,-6,\ldots,\}$. Furthermore the zeroes of ζ in the critical strip are symmetric about the **critical line** $\beta=\frac{1}{2}$ and the real axis. The **Riemann Hypothesis (RH)** (from 1859) is then following assertion:

> **(RH)** All non-trivial zeroes $\rho=\beta+i\gamma$ of ζ lie on the critical line $\beta=\frac{1}{2}$.

Among a myriad of hitherto unprovably sharp statements in algorithmic number theory, it is known that RH is true $\iff$ $\left|\pi(x)-\int_2^x \frac{dt}{\log t}\right| = O(\sqrt{x}\log x)$ [TF00]. In particular, RH is widely agreed to be the most important problem in modern mathematics. Since May 24, 2000, RH even enjoys a bounty of one million US dollars thanks to the Clay Mathematics Foundation.

Through the last estimate on $\pi(x)$, RH also easily implies the following **short interval estimate**: $\pi\left(x+\sqrt{x}\log^2 x\right) - \pi(x) \geq 0.999\sqrt{x}\log x$, for all x sufficiently large. However, one can prove lower bounds nearly as good **without RH**. For example, it is known unconditionally that

$$(\star\star) \qquad \pi(x+x^{0.535}) - \pi(x) \geq \frac{x^{0.535}}{20\log x}$$

for all x sufficiently large [BH96]. Starting with [Hoh30], all results of this flavor (with the possible exception of some papers based on the sieve-method introduced in [IJ79]) were derived essentially by using refined estimates on the distribution of ζ zeroes to control quantities such as[4]

$$S(X,T) := \sum_{\substack{\zeta(\rho)=0\ ,\ \rho=\beta+i\gamma \\ 0<\beta<1\ ,\ |\gamma|<T}} \frac{X^\rho}{\rho} \qquad \text{or} \qquad S'(X,T) := \sum_{\substack{\zeta(\rho)=0\ ,\ \rho=\beta+i\gamma \\ 0<\beta<1\ ,\ |\gamma|<T}} X^{\beta-1}.$$

At this point, it is worth noting that randomization can take us much farther: Whereas the above results assert short intervals where one can **always** find primes,

[2] Shikau Ikehara later showed in 1931 that PNT is in fact **equivalent** to the fact that ζ has no zeroes on the vertical line $\beta=1$ (the proof is reproduced in [DMcK72]).

[3] We'll abuse notation henceforth by letting ζ denote the analytic continuation of ζ to $\mathbb{C}\setminus\{1\}$.

[4] Both sums count zeroes with multiplicities.

one can use even smaller intervals if one merely wishes guarantee the existence of primes **most** of the time. In particular, Selberg showed in 1943 [Sel43, Thm. 4, Pg. 173][5] that

> As $N \longrightarrow \infty$, the fraction of closed intervals $[t, t+t^{0.247}] \subset [1, N]$ containing, say, at least $0.999\frac{t^{0.247}}{\log t}$ primes tends to 1.

Let us now consider general number fields. GRH can be defined as follows: For any finite algebraic extension K of $\mathbb{Q}$, define the **Dedekind zeta function** via the formula $\zeta_K(s) := \sum_{\mathfrak{a}} \frac{1}{(\mathcal{N}\mathfrak{a})^s}$, where $\mathfrak{a}$ ranges over all nonzero ideals of $\mathcal{O}_K$, $\mathcal{N}$ denotes the norm function, and $s > 1$ [BS96]. (So $\zeta_{\mathbb{Q}} = \zeta$.) Then, like ζ, the function ζ_K also admits an analytic continuation to $\mathbb{C}\setminus\{1\}$ (which we'll also call ζ_K) [LO77], has trivial zeroes $\{-2, -4, -6, \ldots,\}$, and all other zeroes of ζ_K lie in the critical strip. (The zeroes of ζ_K in the critical strip are also symmetric about the critical line and the real axis.) GRH is then the following statement:[6]

> **(GRH)** For all finite algebraic extensions K of $\mathbb{Q}$, all the non-trivial zeroes $\rho = \beta + i\gamma$ of ζ_K lie on the critical line $\beta = \frac{1}{2}$.

In particular, letting $\pi_K(x)$ denote the number of **prime** ideals $\mathfrak{p}$ of $\mathcal{O}_K$ satisfying $\mathcal{N}\mathfrak{p} \leq x$, it is known that GRH is true $\Longleftrightarrow \left|\pi_K(x) - \int_2^x \frac{dt}{\log t}\right| = O\left(\sqrt{x}(n_K \log x + \log d_K)\right)$, where n_K and d_K respectively denote the field extension degree $[K : \mathbb{Q}]$ and the absolute value of the discriminant of K over $\mathbb{Q}$ (see, e.g., [LO77, Thm. 1.1] and [BS96]). Also, in addition to numerous other important consequences in number theory and complexity theory, the truth of GRH implies sub-exponential speed-ups for detecting rational points on certain algebraic sets [Roj01].

Paralleling the special case $K = \mathbb{Q}$, GRH (through our preceding estimate on π_K) also easily implies that $\pi_K\left(x + \sqrt{x}\log^2 x\right) - \pi_K(x) \geq 0.999\sqrt{x}\log x$, for all x sufficiently large in a manner depending on K. However, deriving estimates this strong without GRH introduces some difficulties: While it is known that one can always find positive constants A_K, C_K, and t_K (with, say, $C_K = \max\left\{0.626, 1 - \frac{0.99}{n_K}\right\}$) such that

$$\pi_K\left(x + x^{C_K}\right) - \pi_K(x) \geq A_K \frac{x^{C_K}}{\log x} \text{ for all } x \geq t_K \tag{1}$$

(see, e.g., [H-B77, Thm. 4] or [Sok68, Mit68, BO01]), there are no known estimates for A_K or t_K. In any event, in close analogy to the case of the ordinary prime counting function, bounds of this type can be derived by finding good upper bounds on sums[7] like

$$S_K(X,T) := \sum_{\substack{\zeta_K(\rho)=0\ ,\ \rho=\beta+i\gamma \\ 0<\beta<1\ ,\ |\gamma|<T}} \frac{X^\rho}{\rho} \qquad \text{or} \qquad S'_K(X,T) := \sum_{\substack{\zeta_K(\rho)=0\ ,\ \rho=\beta+i\gamma \\ 0<\beta<1\ ,\ |\gamma|<T}} X^{\beta-1}.$$

[5] Selberg actually proved a statement allowing slightly shorter intervals.

[6] Some authors define GRH to be a weaker hypothesis involving certain Dirichlet L-functions. The latter hypothesis is called ERH by some authors (e.g., [BS96]).

[7] ...counting the multiplicities of the zeroes.

We are thus naturally led to DZH, GIPIT, and RIPIT. These alternatives to GRH respectively deal with upper bounds on $S'_K(x,T)$, absolute lower bounds on $\pi_K(x+y)-\pi_K(x)$, and stochastic lower bounds on $\pi_K(x+y)-\pi_K(x)$. In what follows, the function $\boxed{M_K(c):=\log^{c/2}(3+3n_K\log d_K)}$ is quite important.

Dedekind Zero Hypothesis (DZH)[8] *There is an absolute constant $c>0$ such that for all finite algebraic extensions K of $\mathbb{Q}$*

$$S'_K(x,T)\leq\frac{T\log T}{x^{1/M_K(c)}} \quad \text{for all } x,T\geq 2^{M_K(c)}. \ \diamond$$

Good Short Interval Prime Ideal Theorem (GIPIT) *There is an absolute constant $c>0$ such that for all finite algebraic extensions K of $\mathbb{Q}$*

$$\pi_K\left((x+1)^{M_K(c)}\right)-\pi_K\left(x^{M_K(c)}\right)\geq 1+\frac{n_K}{2}(x+1)^{M_K(c)/2},$$

for all $x\geq 2^{M_K(c)}$. $\diamond$

Randomized Short Interval Prime Ideal Theorem (RIPIT) *There are absolute constants $\delta,c>0$ such that, for all finite algebraic extensions K of $\mathbb{Q}$, and all integers $N\geq x\geq 2^{M_K(c)}$, a fraction of at least δ of the closed intervals*

$$\left[1+x^{M_K(c)},(x+1)^{M_K(c)}\right]\subset\left[1+2^{M_K^2(c)},(N+1)^{M_K(c)}\right]$$

contains the norms of at least $1+\frac{n_K}{2}(x+1)^{M_K(c)/2}$ prime ideals from $\mathcal{O}_K$. $\diamond$

Note that DZH, GIPIT, and RIPIT become harder to prove as we decrease the constant c. In particular, by our preceding discussion, the truth of GRH easily implies that DZH, GIPIT, and RIPIT are true, for **all** $c\geq 15$.

However, what is most interesting is the feasibility of our three hypotheses. Let us now make this precise by showing that the strongest of our hypotheses (DZH) can hold even in the presence of a bad failure of GRH. In particular, consider the following hypothesis:

Shrinking Zero-Free Strip Hypothesis (SZH) *There is an absolute constant c such that for all finite algebraic extensions K of $\mathbb{Q}$, the strip*

$$\left\{\rho=\beta+i\gamma \;\middle|\; 1-\frac{1}{M_K(c)}<\beta<1\right\}$$

contains **no** *zeroes of ζ_K.* $\diamond$

[8] An earlier version of DZH (from `http://xxx.arxiv.org/abs/math.NT/0301111v1`) was based on the related quantity $S_K(x,T)$. It is not hard to show that our new hypothesis is weaker.

Theorem 4 *We have the two implications GRH$\Longrightarrow$SZH and SZH$\Longrightarrow$DZH.*[9] *In particular, unlike GRH, an infinite sequence of the form*

$$\left(\rho_1, \rho_2, \rho_3, \ldots \;\middle|\; \frac{1}{2} < \rho_j < 1 - \frac{1}{M_{K_j}(c)} \;,\; \zeta_{K_j}(\rho_j) = 0 \textit{ for all } j\right),$$

with $n_{K_j} \longrightarrow \infty$ as $j \longrightarrow \infty$, need not affect the truth of SZH or DZH.

We prove Theorem 4 in Section 3.1, just before proving Theorem 1.

2 Background and Related Work

2.1 Nullstellensatze and Number Theory

Let us first consider the following recent refined effective arithmetic version of Hilbert's Nullstellensatz. The version below follows important seminal work by many other authors (e.g., [Her26, Bro87, CGH88, Kol88, Phi90, BY91, KP94, Som99, CE00] to name just a few) and is the best current version incorporating Newton polytopes as well.

Theorem 5 *[Som02, Thm. 4.1] Let $f_1, \ldots, f_k \in \mathbb{Z}[x_1, \ldots, x_n]$, $F := (f_1, \ldots, f_k)$, $D := \max_i \deg f_i$, and let V_F denote the volume of the convex hull of the union of $\{\mathbf{O}, e_1, \ldots, e_n\}$ (the origin and the standard basis vectors of $\mathbb{R}^n$) and the set of all exponent vectors of the monomial term expansions of all the f_i. Then F has* **no** *roots in $\mathbb{C}^n \Longleftrightarrow$ there exist polynomials $g_1, \ldots, g_k \in \mathbb{Z}[x_1, \ldots, x_n]$ and a positive integer α with $f_1 g_1 + \cdots + f_k g_k = \alpha$ identically and*

1. $\deg g_i \leq 2n^2 D V_F$
2. $\log(\alpha) \leq 2(n+1)^3 D V_F(\sigma(F) + \log k + 14(n+1) D \log(D+1))$ ■

Since, as we've observed before, $V_F \leq D^n$ always and usually with room to spare, the result above is a tremendous improvement over earlier bounds which were multiples of $D^{O(n)}$. Note also that by expanding the above polynomial linear combination as a matrix vector product, we immediately obtain that **HN** can be decided by solving a linear system with $O(k(2n^2 D V_F)^n)$ variables and equations over the rationals (with total bit-size $O(k(2n^2 D V_F)^n \sigma(F))$), thus easily yielding **HN** $\in$ **EXPTIME**. That **HN** $\in$ **PSPACE** then follows immediately from the fact that linear algebra can be efficiently parallelized [Csa76].

Let us now turn to some quantitative estimates that we'll need. For technical reasons, it will be more convenient to work with a weighted variant of π_K instead of π_K itself. So let us define $\psi_K(x) := \sum \log \mathcal{N}\mathfrak{p}$ — the natural generalization of the

[9] During a conversation at IAS around February 2003, Enrico Bombieri informed the author that an older version of DZH (based on $S_K(X,T)$ instead) implies the existence of zero-free strips for ζ_K. However, the author does not know (as of early 2004) whether the the present version of DZH implies SZH.

summatory of the Mangoldt Λ function to prime ideals in algebraic number rings — where the sum ranges over all integral ideals of the form $\mathfrak{p}=\mathfrak{q}^m$ with $m\in\mathbb{N}$, $\mathfrak{q}$ an unramified prime ideal of $\mathcal{O}_K$, and $N\mathfrak{q}^m\leq x$. The results from analytic number theory we'll need can then be summarized as follows.

Theorem 6 (Unconditional (Weighted) Effective Prime Ideal Theorem) *For all $X,T\geq 2$, we have*

$$\left|\psi_K(X)-\left(X-\sum_{\substack{\zeta_K(\rho)=0\ ,\ \rho=\beta+i\gamma\\ 0<\beta<1\ ,\ |\gamma|<T}}\frac{X^\rho}{\rho}+\sum_{\zeta_K(\rho)=0\ ,\ |\rho|<\frac{1}{2}}\frac{1}{\rho}\right)\right|\leq O\left(\frac{X}{T}\left(n_K\log^2 X+\log d_K+n_K\log T\right)+(n_K+\log d_K)\log X\right).$$

In particular, for all $X\geq e^{10}\approx 22027$ and $T\geq e^5\approx 148.4$, we can replace the O-estimate above by

$$\frac{X}{T}\left\{5n_K\log^2 X+36.55n_K\log X+375.2n_K\log T+196.6\log d_K+351n_K\right\}+(2\log d_K+3.51n_K)\log X+25\log d_K+283.1n_K,$$

or

$$2^{M_K(49)}\left(\frac{X\log^2 X}{T}+\frac{X\log T}{T}+\log X\right).$$

Sketch of Proof: The first bound is nothing more than the special case of [LO77, Thm. 7.1] where, in the notation there, $K=L$ and the conjugacy class C of $\mathrm{Gal}(L/K)$ is just the identity element e. (The sums over zeroes of ζ_K also simplify since there is just one underlying character of $H=\langle e\rangle$ and it is the trivial character.) The second bound is a variation of [Sil02, Thm. 9.1]. (The latter theorem gives a bound on $\psi_K(X)-X$ instead, and assumes the truth of GRH.) In particular, by modifying the proof to **avoid** the use of GRH, and employing [Sil02, Lem. 5.8], the second bound follows easily.

Assuming $x\geq e^{10}$ it is clear that $\log x\geq 10$. Using this, and the fact that $M_K(10)\geq 3+3n_K\log d_K\geq n_K+\log d_K$, the final bound follows routinely. ■

Subtracting the approximations for $\psi_K(X+Y)$ and $\psi_K(X)$ implied above, we then easily obtain the following corollary.

Corollary 1 (Unconditional (Weighted) Effective Short Interval Prime Ideal Theorem) *For all $X,Y,T\geq 2$, we have that $\psi_K(X+Y)-\psi_K(X)$ is bounded below by*

$$Y\left(1-\sum_{\substack{\zeta_K(\rho)=0\ ,\ \rho=\beta+i\gamma\\ 0<\beta<1\ ,\ |\gamma|<T}}X^{\beta-1}\right)-O\left(\frac{X+Y}{T}\left(n_K\log^2(X+Y)+\log d_K+n_K\log T\right)+(n_K+\log d_K)\log(X+Y)\right).$$

In particular, for all $X,Y\geq e^{10}\approx 22027$ and $T\geq e^5\approx 148.4$, we can replace the $O(\cdot)$ estimate by the following:

$$\frac{X+Y}{T}\left\{10n_K\log^2(X+Y)+73.1n_K\log(X+Y)+750.4n_K\log T+393.2\log d_K+702n_K\right\}+(4\log d_K+7.02n_K)\log(X+Y)+50\log d_K+566.2n_K,$$

or

$$2^{M_K(51)}\left(\frac{(X+Y)\log^2 X}{T}+\frac{(X+Y)\log T}{T}+\log(X+Y)\right).\ ■$$

The only non-trivial step in proving Corollary 1 is to observe that

$$\begin{aligned}\left|\frac{(X+Y)^\rho - X^\rho}{\rho}\right| &= \left|\int_X^{X+Y} t^{\rho-1}dt\right| \\ &\leq \int_X^{X+Y} |t^{\rho-1}|dt \\ &= \int_X^{X+Y} t^{\beta-1}dt \\ &\leq (X+Y-X)X^{\beta-1} = YX^{\beta-1}\end{aligned}$$

(since $\beta<1$ and $X,Y\geq 2$).

We will also need to know how many zeroes of ζ_K in the critical strip have bounded imaginary part.

Theorem 7 *For any finite algebraic extension K of $\mathbb{Q}$, the number of zeroes of ζ_K in the region $\{\rho=\beta+i\gamma \mid 0<\beta<1\ ,\ |\gamma|\leq T\}$ is asymptotic to $\frac{n_K}{\pi}T\log T$ as $T\longrightarrow\infty$. Moreover, the number of such zeroes is bounded above by*

$$T(5\log d_K + 45n_K) + 15n_K T\log(T+1) \quad \textit{for all } T\geq 0,$$

or

$$2^{M_K(44)}T\log T \quad \textit{for all } T\geq e.$$

Proof: The first assertion is classical (see, e.g., [Lan49]). The second assertion follows easily from [Sil02, Lemma 5.7] (which gives an explicit upper bound on the number of zeroes of ζ_K in the rectangle $\{\rho=\beta+i\gamma \mid 0<\beta<1\ ,\ |\gamma-T|\leq 1\}$) by summing over the even integers k with $|k|\leq T$. The final assertion follows routinely from the inequalities $M_K(10)\geq 3+3n_K\log d_K\geq n_K+\log d_K$ and $T^2\geq T+1$ (valid for $T\geq 2$). ■

Finally, the following basic result will help us relate $\log d_K$ and n_K to the bit-size of the minimal polynomial defining K. Recall that the square-free part of a univariate polynomial $f\in\mathbb{Z}[x_1]$ is $f/\gcd(f,f')$.

Proposition 1 *(See [Roj01, Lemmata 2.1 and 4.1]) Suppose $K=\mathbb{Q}[x_1]/\langle f\rangle$ where f is the square-free part of some polynomial $g\in\mathbb{Z}[x_1]\setminus\mathbb{Z}$, and let $d_f:=\deg f$ and $d_g:=\deg g$. Then $n_K\leq d_f$ and $\log d_K=O(d_g\sigma(g)+d_f^2)$. More precisely,*

$$\log d_K \leq (2d_g-1)(\sigma(g)+(d_g+\alpha)\log 2)+\left(d_g-\frac{1}{2}\right)\log(d_g+1)+\frac{d_g}{2}\log(d_g(2d_g+1)/6). \ ■$$

2.2 Complexity Theory

Let us now briefly and informally review the complexity classes mentioned earlier in the introduction. First, our underlying (deterministic) computational model will be the classical Turing machine, which for our purposes can be assumed to be anyone's favorite lap-top computer, augmented with infinite memory and a flawless operating system. In particular, bit operations (and time) can be identified with the number of clock-cycles used by the underlying microprocessor, and a **randomized** algorithm assumes further a source of randomness which gives one random bit per clock-cycle.

Input size, for an input such as F, is then simply $\sigma(F)$, and can also be interpreted (up to a constant multiple) as the amount of memory used by our idealized lap-top to store F.

Recall that an **oracle in $\boldsymbol{A}$** is a special machine which is allowed to run an algorithm with complexity in A in one unit of time. Recall also that an **enumerative** (resp. **decision**) problem is a problem where the answer to any instance is a positive integer (resp. either `Yes` or `No`). Our complexity classes can then be summarized as follows.

P The family of decision problems which can be done within time polynomial in the input size.[10]

RP The family of decision problems admitting a randomized polynomial-time algorithm for which a ``Yes'' answer is always correct but a ``No'' answer is wrong with probability $\frac{1}{2}$.

coRP The family of decision problems admitting a randomized polynomial-time algorithm for which a ``No'' answer is always correct but a ``Yes'' answer is wrong with probability $\frac{1}{2}$.

BPP The family of decision problems admitting randomized algorithms that terminate in polynomial-time to give an answer which is correct with probability at least[11] $\frac{2}{3}$.

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

coNP The family of decision problems where a ``No'' answer can be **certified** within time polynomial in the input size.

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

AM The family of decision problems solvable by a **BPP** algorithm which has been augmented with exactly **one** use of an oracle in **NP**.

$\mathbf{NP}^{\mathbf{NP}}$ The family of decision problems where a ``Yes'' answer can be certified by using an **NP**-oracle a number of times polynomial in the input size.

$\mathbf{coNP}^{\mathbf{NP}}$ The family of decision problems where a ``No'' answer can be certified by using an **NP**-oracle a number of times polynomial in the input size.

$\mathbf{P}^{\mathbf{NP}^{\mathbf{NP}}}$ 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.

[10] Note that the underlying polynomial depends only on the problem in question (e.g., matrix inversion, shortest path finding, primality detection) and not the particular instance of the problem.

[11] It is easily shown that we can replace $\frac{2}{3}$ by any constant strictly greater than $\frac{1}{2}$ and still obtain the same family of problems.

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.

EXPTIME The family of decision problems solvable within time exponential in the input size.

We note that **RP** algorithms and **BPP** algorithms are sometimes respectively referred to as **Monte-Carlo** and **Atlantic City** algorithms, i.e., Atlantic City cheats you more than Monte Carlo. Let us also recall the basic fact that $\mathbf{P}=\mathbf{NP} \Longrightarrow \mathbf{P}=\mathbf{P}^{\mathbf{NP}^{\mathbf{NP}}}$ [Pap95, Thm. 17.9]. So if $\mathbf{P}=\mathbf{NP}$, all but two of the complexity classes mentioned above collapse into **P**. Finally, let us recall the following important approximation result of Stockmeyer.

Theorem 8 *[Sto85] Any problem in* $\#\mathbf{P}$ *admits an algorithm in* $\mathbf{P}^{\mathbf{NP}^{\mathbf{NP}}}$ *which approximates the answer to any instance to within a factor of* 2. ■

Note in particular that the number of **bits** in the output of Stockmeyer's algorithm is always polynomial in the input size. So one remains in $\mathbf{P}^{\mathbf{NP}^{\mathbf{NP}}}$ simply by using polynomially many `''Yes''`/`''No''` answers to obtain the bits of the desired integer output.

3 Proving Theorem 4 and Reducing Theorem 1 to Theorem 2

Let us begin with a description of two important algorithms for solving **HN** that underlie Theorem 1. An algorithm similar to Algorithm `K` below was outlined on Page 6 of [Koi96], but **not** in the journal version of that paper, hence our naming.

ALGORITHM `K`

Input *A system F of k polynomials in n variables with integer coefficients*

Output *A declaration, correct with probability $\geq \frac{2}{3}$, of whether F has a complex root or not.*

Step 0 *Compute, via recursive squaring, the smallest powers of* 2 *(which we will name t, a, and C) which are respectively larger than the constants t_F, a_F, and C_F from Theorem 2.*

Step 1 *Pick a (uniformly distributed) random integer $x\in\{t+1,\ldots,t+3a\}$.*

Step 2 *Using an* **NP** *oracle just once, decide if there is a prime $p\in\{1+x^C,\ldots,(x+1)^C\}$ such that the mod p reduction of F has a root in $(\mathbb{Z}/p\mathbb{Z})^n$. If so, declare that F has a complex root. Otherwise, declare that F has no complex root.* ◇

ALGORITHM `R`

Input *A system F of k polynomials in n variables with integer coefficients*

Output *A true declaration of whether F has a complex root or not.*

Step 0 *Following the notation of Theorem 2, let $N' := \lceil 5/\delta \rceil$, and compute, via recursive squaring, the smallest powers of 2 (which we will name t', a', and C') which are respectively larger than t'_F, a_F, and C'_F.*

Step 1 *Using the algorithm from Theorem 8, approximate the number M' of intervals*
$$\left[1 + x^{C'}, (x+1)^{C'}\right] \subset \left[1 + (t')^{C'}, (N'a'+1)^{C'}\right]$$
containing a prime p such that the mod p reduction of F has a root in $(\mathbb{Z}/p\mathbb{Z})^n$.

Step 2 *If $M' \geq \frac{5}{2}a'$ then declare that F has a complex root. Otherwise, declare that F has no complex root.* $\diamond$

The last technical lemma we will need relates short interval bounds between π_K and ψ_K.

Lemma 1 *Suppose $f \in \mathbb{Z}[x_1] \setminus \mathbb{Z}$ is square-free and $K := \mathbb{Q}[x_1]/\langle f \rangle$. Then, assuming $x \geq 1 + \log d_K$ and $y \geq 0$,*
$$\psi_K(x+y) - \psi_K(x) \geq \left(1 + \frac{7n_K}{2}\sqrt{x+y}\right)\log(x+y) \Longrightarrow \pi_K(x+y) - \pi_K(x) \geq 1 + \frac{n_K}{2}\sqrt{x+y}.$$

Proof: Note that the right-hand bound can be enforced via a similar bound on yet another related weighted prime power counting function: First, define $\Theta_K(x) := \sum \log \mathcal{N}\mathfrak{p}$ where the sum ranges over all unramified prime ideals of $\mathcal{O}_K$ of norm $\leq x$. Since
$$\Theta_K(x+y) - \Theta_K(x) \leq (\pi_K(x+y) - \pi_K(x))\log(x+y),$$
the right-hand bound of our lemma is clearly implied by
$$\Theta_K(x+y) - \Theta_K(x) \geq \left(1 + \frac{n_K\sqrt{x+y}}{2}\right)\log(x+y).$$

Now, for $x \geq 3^6$, it is easily checked that $x^{1/3}\log_2 x \leq 2\sqrt{x}$. So for $x \geq 3^6$,
$$\begin{aligned}
0 \leq \psi_K(x) - \Theta_K(x) &= \sum_{\substack{(\mathfrak{q},m)\\ m\geq 2\\ \mathcal{N}\mathfrak{q}^m \leq x}} \log \mathcal{N}\mathfrak{q} \\
&\leq \sum_{m=2}^{\lfloor \log_2 x \rfloor} n_K x^{1/m} \log x \\
&\leq n_K(\log x) \sum_{m=2}^{\lfloor \log_2 x \rfloor} x^{1/m} \\
&\leq n_K(\log x)(\sqrt{x} + x^{1/3}\log_2 x) \\
&\leq n_K(\log x)(3\sqrt{x}) = 3n_K\sqrt{x}\log x.
\end{aligned}$$

So it suffices to enforce
$$\psi_K(x+y) - \psi_K(x) \geq \left(1 + \frac{7n_K\sqrt{x+y}}{2}\right)\log(x+y)$$
and we are done. ■

3.1 The Proof of Theorem 4

Assume SZH for a given parameter c. In particular, it is clear that once SZH holds for a given c, SZH continues to hold for all larger c as well. This immediately proves the very last statement of Theorem 4, and allows us to assume (to simplify matters later) that $c \geq 15$.

That GRH implies SZH is obvious from the definition, so we now need only prove that SZH implies DZH. Toward this end, note that for any $T \geq e \approx 2.718281828$ and $X > 1$,

$$\begin{aligned} S'(X,T) &= \sum_{\substack{\zeta(\rho)=0\ ,\ \rho=\beta+i\gamma \\ 0<\beta<1\ ,\ |\gamma|<T}} X^{\beta-1} \\ &\leq X^{-1/M_K(c)} 2^{M_K(44)} T \log T \end{aligned}$$

where the last inequality is an immediate consequence of SZH and Theorem 7. So to prove DZH for parameter c^*, it suffices to find a c^* such that

$$\frac{2^{M_K(44)} T \log T}{x^{1/M_K(c)}} \leq \frac{T \log T}{X^{1/M_K(c^*)}}, \text{ for all } X, T \geq 2^{M_K(c^*)}$$

The last inequality is clearly equivalent to

$$\frac{2^{M_K(44)}}{X^{1/M_K(c)}} \leq \frac{1}{X^{1/M_K(c^*)}}.$$

or

$$2^{M_K(44)} \leq X^{\frac{1}{M_K(c)} - \frac{1}{M_K(c^*)}}. \tag{2}$$

Now note that $M_K(c+15) = M_K(c) M_K(15) \geq 2M_K(c) \geq M_K(c) + 1$ (since $c \geq 15 \implies M_K(c) \geq 2$). So we then clearly have the following:

$$\begin{aligned} M_K(2c+15) &= M_K(c) M_K(c+15) \\ &\geq \frac{M_K(c) M_K(c+15)}{M_K(c+15) - M_K(c)} \\ &= \left(\frac{1}{M_K(c)} - \frac{1}{M_K(c+15)} \right)^{-1} \end{aligned}$$

So for $X > 1$, $X^{1/M_K(2c+15)} \leq X^{\frac{1}{M_K(c)} - \frac{1}{M_K(c+15)}}$, and thus $2^{M_K(44)} \leq X^{1/M_K(2c+15)}$ implies Inequality (2).

To conclude, we have seen that $T \geq e$ and $X \geq 2^{M_K(2c+15) M_K(44)} = 2^{M_K(2c+59)}$ imply that $S'(X,T) \leq \frac{T \log T}{X^{1/M_K(2c+15)}} \leq \frac{T \log T}{X^{1/M_K(2c+59)}}$, thus proving DZH for parameter $c^* = 2c + 59$. ■

3.2 The Proof of Theorem 1

Let us first address the easiest assertions: Assertion (3) follows trivially from Theorem 4, which we have just proved. Assertion (5) follows immediately from the definitions of GIPIT and RIPIT.

Let us now move to our algorithmic Assertions (1) and (2). Their proof will follow easily from a now standard reduction: **DIM** is polynomial-time many-one reducible to **HN** [Koi97, Thm. 5.8].

Remark 2 *The main trick underlying this reduction goes as follows: Let Z denote the complex zero set of an input F. Then there are now standard quantitative results (dating back to earlier work of Jacob T. Schwarz [Sch80] and modernized in [Koi97, Sec. 3] and [Roj00, Sec. 6]) that allow one to find, in* **BPP***, a subspace L (defined by a linear system of equations G with $\sigma(G)$ polynomial in $\sigma(F)$) such that* $\dim Z \geq d \Longrightarrow Z \cap L \neq \emptyset$ *with probability* $\geq 2/3$. *(The probability arises because the coefficients of G are random.)* $\diamond$

So to prove Assertions (1) and (2), it clearly suffices to prove (respectively):
($1'$) RIPIT$\Longrightarrow$ $\mathbf{HN} \in \mathbf{P}^{\mathbf{NP}^{\mathbf{NP}}}$.
($2'$) GIPIT$\Longrightarrow$ $\mathbf{HN} \in \mathbf{AM}$.
To do the latter, it in turn suffices to prove the following:
($1''$) RIPIT$\Longrightarrow$ Algorithm `R` is correct and runs within $\mathbf{P}^{\mathbf{NP}^{\mathbf{NP}}}$.
($2''$) GIPIT$\Longrightarrow$ Algorithm `K` is correct and runs within **AM**.

Checking (1") first, note that Assertion (1) of Theorem 2 implies that F has no complex roots $\Longrightarrow$ no more than a' of the closed intervals $\left[1 + x^{C'}, (x+1)^{C'})\right] \subset \left[1 + (t')^{C'}, \infty\right)$ contain a prime p such that the mod p reduction of F has a root in $(\mathbb{Z}/p\mathbb{Z})^n$. Note also that by Assertion (6) of Theorem 2, RIPIT implies that if F has a complex root then at least $5a'$ of the intervals $\left[1 + x^{C'}, (x+1)^{C'})\right] \subset \left[1 + (t')^{C'}, (N'a'+1)^{C'}\right]$ contains a prime p such that the mod p reduction of F has a root in $(\mathbb{Z}/p\mathbb{Z})^n$. So Algorithm `R` is clearly correct, assuming the number of such intervals is computable within $\#\mathbf{P}$.

To check the latter fact, note that verifying whether $\left[1 + x^{C'}, (x+1)^{C'})\right]$ contains the kind of prime stipulated above can be done in **P**: No such prime has more bits than $C'\lceil 1 + \log_2(N'a'+1)\rceil \leq O(\sigma(F)^{c'}(\sigma(F)^{c'} + \sigma(F)^2))$, which is polynomial in $\sigma(F)$. (Note also RIPIT implies that Step 0 is trivially executable within **P**.) Furthermore, primality can be checked in **P** thanks to [AKS02], or in **NP** via [Pra75], and checking the solvability of F over $(\mathbb{Z}/p\mathbb{Z})^2$ can clearly be done within **NP** as well. So, assuming RIPIT, our interval count indeed lies within $\#\mathbf{P}$ and the complexity of Algorithm `R` is indeed in $\mathbf{P}^{\mathbf{NP}^{\mathbf{NP}}}$ (thanks to Theorem 8). So we have proved ($1''$). (Note that it also easily follows that Algorithm `R` runs in **PSPACE** unconditionally.)

To check ($2''$), we follow almost exactly the same argument as for ($1''$). The only key difference is that now, if F has a complex root, then **all** the intervals $\left[1 + x^{C}, (x+1)^{C})\right] \subset \left[1 + t^{C}, (t+3a+1)^{C}\right]$ contains a prime p such that the mod p reduction of F has a root in $(\mathbb{Z}/p\mathbb{Z})^n$. So clearly, a declaration of ``` ``No Complex Roots'' ``` is always correct, while a declaration of ``` ``There is at Least One Complex Root'' ``` is wrong with probability $\leq \frac{1}{3}$. An argument completely parallel to our earlier observations on bit-size also easily implies that Algorithm K runs in **AM**, assuming GIPIT. So Algorithm K indeed runs in **AM**, and we have proved ($2''$). (Note also that it easily follows that Algorithm K runs in **PSPACE** unconditionally.)

Having proved Assertions (1), (2), (3) and (5), we are left with Assertion (4). To prove Assertion (4), assume DZH with parameter c. Since DZH then clearly continues to hold for all larger c as well, let us assume further (to simplify matters later) that $c \geq 83$. We then immediately obtain that

$$S'(x^{3M_K(c)}, x^{3/2}) \leq \frac{3}{2}\frac{\log x}{x^{3/2}} \text{ for all } x \geq 2^{M_K(c)}.$$

Now recall that for $A \geq 1$, we have $Ax^{A-1} \leq (x+1)^A - x^A \leq A(x+1)^{A-1}$ (cf. our earlier integral inequality following Corollary 1). So Corollary 1, with $X := x^{3M_K(c)}$, $Y := (x+1)^{3M_K(c)} - x^{3M_K(c)}$, and $T := X^{1/2M_K(c)} = x^{3/2}$, then yields

$$\psi_K\left((x+1)^{3M_K(c)}\right) - \psi_K\left(x^{3M_K(c)}\right) \geq 3M_K(c)x^{3M_K(c)-1}\left(1 - \frac{3}{2}\frac{\log x}{x^{3/2}}\right) - H(x)$$

for all $x \geq \max\{e^{10/M_K(15)}, e^{5\cdot 2/3}\} \approx 28.032$, where

$H(x) := 2^{M_K(51)}\left(9M_K(c)^2\frac{(x+1)^{3M_K(c)}\log^2(x+1)}{x^{3/2}} + \frac{3}{2}\frac{(x+1)^{3M_K(c)}\log(x+1)}{x^{3/2}} + 3M_K(c)\log(x+1)\right).$

Now, via a few simple estimates identical to those from Section 2.1, we can easily show that

$$H(x) \leq 2^{M_K(63)}(x+1)^{3M_K(c)-1.5}\log^2(x+1).$$

So we immediately obtain the following more concise inequality, valid for all $x \geq e^{10/3}$:

$$\psi_K\left((x+1)^{3M_K(c)}\right) - \psi_K\left(x^{3M_K(c)}\right) \geq x^{3M_K(c)-1}\left(1 - \frac{3}{2}\frac{\log x}{x^{3/2}} - 2^{M_K(63)}\frac{\log^2(x+1)}{(x+1)^{1/2}}\right). \quad (3)$$

We are now almost done: Lemma 1, combined with the simple estimate $2^{M_K(21)} \geq 6(n_K + \log d_K) \geq 1 + \frac{7n_K}{2}$, tells us that to prove GIPIT, it suffices to prove the following inequality for all $x \geq e^{10/3}$:

$$\psi_K\left((x+1)^{3M_K(c)}\right) - \psi_K\left(x^{3M_K(c)}\right) \geq 2^{M_K(21)}(x+1)^{3M_K(c)/2} \quad (4)$$

In particular, a quick check on `Maple` easily shows that the $x \geq 2.9 \times 10^{19}$ implies that the inequalities

$$\frac{3}{2}\frac{\log x}{x^{3/2}} \leq 1/4 \text{ and } 2^{M_K(63)}\frac{\log^2(x+1)}{(x+1)^{1/2}} \leq 1/4$$

hold, and thus Inequality (3) becomes the following simpler inequality:

$$\psi_K\left((x+1)^{3M_K(c)}\right) - \psi_K\left(x^{3M_K(c)}\right) \geq \frac{1}{2}x^{3M_K(c)-1}. \quad (5)$$

So, noting that $2^{3M_K(c)/2}\left(\frac{x}{x+1}\right)^{3M_K(c)/2} \geq 1$ for all $x \geq 1$, we see by Inequalities (5) and (4) that to prove GIPIT we need only prove

$$x^{3M_K(c)/2-1} \geq 2 \cdot 2^{M_K(21)} 2^{3M_K(c)/2}$$

Since $c \geq 15 \implies M_K(c) \geq 2 \implies$, and since $M_K(13) \geq (1 + M_K(21))/2$, $3M_K(c)/2 \leq M_K(c+9)$, and $3M_K(c)/4 \leq M_K(c-7)$, we obtain the above inequality to be true provided $x \geq \max\{2^{M_K(c+6)}, 2.9 \times 10^{19}\}$. In particular, noting that $2^{M_K(89)} \geq 2.9 \times 10^{19}$ and $3M_K(c) \leq M_K(c+24)$, we obtain GIPIT with parameter $c^* := c + 24$. ■

4 Prime Distribution and Proving Theorem 2

Proof of Theorem 2: Assertion (1) follows easily from the following argument, which has appeared earlier in various incarnations, e.g., [Koi96, HMPS00, Roj00]: By assumption, Theorem 5 tells us that the mod p reduction of F has a root in $(\mathbb{Z}/p\mathbb{Z})^n \implies p$ divides α. Since the number of prime divisors of an integer α is no more than $1 + \log \alpha$ (since any prime power other than 2 is bounded below by $e < 2.7183$), an elementary calculation yields Assertion (1).

The proofs of Assertions (2)–(5) then rely on effective univariate reduction and some density estimates for prime ideals. In particular, we will derive Assertion (2) by examining the following cleaner abstraction: Let $\pi_F(x)$ denote the number of primes $p \leq x$ such that the mod p reduction of F has a root in $(\mathbb{Z}/p\mathbb{Z})^n$. Clearly then, it is enough to find sufficiently good upper bounds on y (as a function of x) and t_F such that for all $x \geq t_F$,

$$\pi_F(x+y) - \pi_F(x) \geq 1. \tag{6}$$

To do this, we will pass through various reductions, eventually culminating in enforcing a particular lower bound on $\pi_K(x+y) - \pi_K(x)$, for some number field K depending naturally on F. In particular, GIPIT will immediately imply a lower bound good enough to imply Assertion (4), and without GIPIT we can still derive the weaker Assertion (3) by employing older theorems on the distribution of prime ideals in $\mathcal{O}_K$. Our framework will then imply Assertions (5) and (6) almost trivially.

To start, let $h_1, \ldots, h_n, \hat{h}_F \in \mathbb{Z}[t]$ and $r_1, \ldots, r_n$ respectively be the polynomials and integers arising from applying Theorem 3 to our input F. Letting f be the square-free part of $\hat{h}_F$, note that if $p \not| \operatorname{lcm}(r_1, \ldots, r_n)$ **and** the mod p reduction of f has a root in $(\mathbb{Z}/p\mathbb{Z})^n$, then the mod p reduction of F has a root in $(\mathbb{Z}/p\mathbb{Z})^n$. This is because Assertion (2) of Theorem 3 implies that $F(h_1(t)/r_1, \ldots, h_n(t)/r_n) \equiv \mathbf{O}$ in the ring $\mathbb{Q}[t]/\langle f \rangle$, which in turn implies an identity in the ring $(\mathbb{Z}/p\mathbb{Z})[t]$ once one substitutes the mod p multiplicative inverses of $r_1, \ldots, r_n$.

Assertion (3) of Theorem 3 then implies that to prove Inequality (6) it suffices to instead enforce

$$N_f(x+y) - N_f(x) \geq 1, \text{ for all } x \geq \max\left\{\Omega(nV_F^6(\sigma(F) + n\log D)), 1 + \log d_K\right\}, \tag{7}$$

where $N_f(x)$ denotes the total number of linear factors of the mod p reduction of f for all primes $p \leq x$, and $K := \mathbb{Q}[x_1]/\langle f \rangle$. (The lower bound of $1 + \log d_K$ is necessary to avoid problems with miscounting repeated factors.)

Now note that $p \not| d_K$ implies that the mod p reduction of f has a linear factor iff p lies below a prime in $\mathcal{O}_K$ of residue class degree 1 [Lan94, Ch. I, Sec. 8, Prop. 25, pp. 27–28]. Note also that $\mathfrak{p}$ (of residue class degree 1) lies over $p \Longrightarrow \mathcal{N}\mathfrak{p}=p$. So let $\pi^1_K(x)$ denote the number of unramified primes $\mathfrak{p}$ of $\mathcal{O}_K$ with $\mathcal{N}\mathfrak{p}\leq x$ and residue class degree 1. It is then clear that $|\pi^1_K(x)-N_f(x)|\leq(n_K-1)(1+\log d_K)$ (since the correspondence between factors and primes breaks down only for $p|d_K$) and the left-hand side is **constant** for all x larger than any prime dividing d_K.

Next, note that by [Roj00, Lemma 5], $\sigma(f)=\sigma(\hat{h}_F)+(V_F+c_0)\log 2$, where $c_0=2-\frac{3}{4\log 2}\leq 0.91798$. So, by Proposition 1, we need only prove the inequality below in order to prove (7):

$$\pi^1_K(x+y)-\pi^1_K(x)\geq 1 \text{ for all } x\geq\Omega(nV^6_F(\sigma(F)+n\log D)), \tag{8}$$

assuming now (and henceforth) that $x\geq 1+\log d_K$.

We are now ready for our final reduction: Since any prime $\mathfrak{p}$ of $\mathcal{O}_K$ of residue class field degree ≥ 2 lying over p must satisfy $\mathcal{N}\mathfrak{p}\geq p^2$, we must have $p\leq\sqrt{x}$. Since the number of such primes $\mathfrak{p}$ over p is $\leq n_K/2$, we must then have $0\leq\pi_K(x)-\pi^1_K(x)\leq\frac{n_K\sqrt{x}}{2}$. Thus, to prove our original desired Inequality (6), it suffices to prove the following inequality:

$$\pi_K(x+y)-\pi_K(x)\geq 1+\frac{n_K\sqrt{x+y}}{2} \text{ for all } x\geq\Omega(nV^6_F(\sigma(F)+n\log D)), \tag{9}$$

We can now prove Assertions (2)–(6): First, note that by Inequality (1) of Section 1.1, we obtain Inequality (9) for large x depending on K upon taking $y:=x^{\max\left\{0.626,1-\frac{0.99}{n_K}\right\}}$. In particular, upon a little more substitution, we obtain Assertion (2) with $C_F=n_K$. Moreover, by Theorem 3, $n_K\leq V_F$. So, noting that $\frac{1}{\log 2}\leq 1.45$, $V_F\leq D^n$, and $n\log D\leq(n+\log D)^2\leq\sigma(F)^2$, we obtain Assertion (3).

Next, note that by our preceding observations, $\log(nV^6_F(\sigma(F)+n\log D))=O(\sigma(F)^2)$. So GIPIT implies Inequality (9) and we thus obtain Assertion (4). Using Inequality (9) in almost exactly the same way, Assertion (6) follows as well.

To conclude, note that GRH easily implies (cf. our proof of Theorem 4) the upper bound $S'(X,T)\leq 2^{M_K(44)}\frac{T\log T}{\sqrt{x}}$. Mimicking our proof of Assertion (4) of Theorem 1, we then easily obtain the stated upper bounds for C_F and $\log t_F$. So we are done. ■

4.1 The Proof of Theorem 3

The proof follows almost exactly the same development as [Roj01, Secs. 6.1.3 and 6.1.5], except that Theorem 23 there (an estimate on the maximum coefficient size of a variant of the toric resultant) is combined with [Som02, Cor. 2.5]. This allows us to omit a factor exponential in n that would have otherwise appeared in Assertion (3) above. ■

Acknowledgements

In early 2002, Paula B. Cohen suggested to me that Enrico Bombieri might be interested in a paper of mine ([Roj00]). I sent my paper to Professor Bomieri, who kindly took the time to read it and, around March 2002, point out an error in one of the proofs. (The result in question was [Roj00, Thm. 4, Part (b)] and the error changes the numerical estimates of [Roj00, Sec. 6.1.6, Rem. 13] but does not invalidate the result.) The present paper arose when I checked the details and noted that the earlier assumptions of GRH could be considerably weakened. I am therefore deeply indebted to Professor Bombieri and Professor Cohen for helping inspire the present paper. Later, around May 2002, I had the good fortune of meeting Lior Silberman at the Workshop on Zeta-Functions and Associated Riemann Hypotheses at the Courant Institute of Mathematical Sciences, New York University. He provided a copy of [Sil02] just when I needed some extremely explicit Čebotarev-like estimates. I am thus also indebted to Lior for writing and sharing his notes with such generosity and good timing.

I also thank David Joyner and Madhu Sudan, and two anonymous referees, for detailed comments on an earlier version of this paper. Finally, I would like to thank Brian Conrey for pointing out some nice references such as Selberg's paper [Sel43], and Enrico Bombieri and Peter Sarnak for kindly listening to my earlier versions of DZH and GIPIT.

References

[AKS02] Agrawal, Manindra; Kayal, Neeraj; and Saxena, Nitin, *"PRIMES is in P,"* submitted for publication, downloadable from `http://www.cse.iitk.ac.in/news/primality.html`

[BF91] Babai, László and Fortnow, Lance, *"Arithmetization: a New Method in Structural Complexity Theory,"* Comput. Complexity **1** (1991), no. 1, 41–66.

[BM88] Babai, László and Moran, Shlomo, *"Arthur-Merlin Games: A Randomized Proof System and a Hierarchy of Complexity Classes,"* Journal of Computer and System Sciences, 36:254–276, 1988.

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

[BH96] Baker, R. C. and Harman, G., *"The difference between consecutive primes,"* Proc. London Math. Soc. (3) 72 (1996), no. 2, pp. 261–280.

[BO01] Balog, Antal and Ono, Ken, *"The Chebotarev Density Theorem in Short Intervals and Some Questions of Serre,"* J. Number Theory 91 (2001), no. 2, pp. 356–371.

[BIKPP96] Beam, Paul; Impagliazzo, Russel; Krajicek, Janos; Pitassi, Toniann; and Pudlak, Pavel, *"Lower Bounds on Hilbert's Nullstellensatz and Propositional Proofs,"* Proceedings of the London Mathematical Society **73** (1996), pp. 1–26.

[BY91] Berenstein, C. A. and Yger, A., *"Effective Bézout identities in* $\mathbb{Q}[x_1, \ldots, x_n]$*,"* Acta Math. **166** (1991), pp. 69–120.

[BCSS98] Blum, Lenore; Cucker, Felipe; Shub, Mike; and Smale, Steve, *Complexity and Real Computation,* Springer-Verlag, 1998.

[Bro87] Brownawell, W. D., *"Bounds for the degrees in the Nullstellensatz,"* Ann. of Math. **126** (1987), pp. 577–591.

[CGH88] Caniglia, L. Galligo, A., Heintz, J., *Borne simplemente exponentielle pour les degrés dans le théorème des zéros sur un corps de charactéristique quelconte,* C. R. Acad. Sci. Paris **307** (1988), pp. 255–258.

[CGH89] Caniglia, Léandro; Galligo, André; and Heintz, Joos, *"Some new effectivity bounds in computational geometry,"* Applied algebra, algebraic algorithms and error-correcting codes (Rome, 1988), pp. 131–151, Lecture Notes in Comput. Sci., 357, Springer, Berlin, 1989.

[Can87] Canny, John F., *"The Complexity of Robot Motion Planning Problems,"* ACM Doctoral Dissertation Award Series, ACM Press (1987).

[Can88] _____________, *"Some Algebraic and Geometric Computations in PSPACE,"* Proc. 20$^{\underline{\text{th}}}$ ACM Symp. Theory of Computing, Chicago (1988), ACM Press.

[CE00] Emiris, Ioannis Z. and Canny, John, *"A Subdivision-Based Algorithm for the Sparse Resultant,"* J. ACM **47** (2000), no. 3, pp. 417–451.

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

[Csa76] Csanky, L., *"Fast Parallel Matrix Inversion Algorithms,"* SIAM J. Comput. **5** (1976), no. 4, pp. 618–623.

[DMcK72] Dym, H. and McKean, H. P., *Fourier Series and Integrals,* Probability and Mathematical Statistics, vol. 14, Academic Press, 1972.

[EM99] Elkadi, Mohamed and Mourrain, Bernard, *"A new algorithm for the geometric decomposition of a variety,"* Proceedings of the 1999 International Symposium on Symbolic and Algebraic Computation (Vancouver, BC), pp. 9–16, ACM, New York, 1999.

[GJ79] Garey, Michael R. and Johnson, David S. *Computers and Intractability: A Guide to the Theory of NP-Completeness,* A Series of Books in the Mathematical Sciences, W. H. Freeman and Co., San Francisco, Calif., 1979.

[FGM90] Fitchas, Noaï, Galligo, André, and Morgenstern, Jacques, *"Precise Sequential and Parallel Complexity Bounds for Quantifier Elimination Over Algebraically Closed Fields,"* Journal of Pure and Applied Algebra, 67:1–14, 1990.

[HMPS00] Hägele, Klemens; Morais, Juan Enrique; Pardo, Luis Miguel; Sombra, Martin, *"On the Intrinsic Complexity of the Arithmetic Nullstellensatz,"* Journal of Pure and Applied Algebra **146** (2000), no. 2, pp. 103–183.

[H-B77] Heath-Brown, D. R., *"On the Density of Zeros of the Dedekind Zeta-function,"* Acta Arithmetica **33** (1977), no. 2, pp. 169–181.

[Her26] Hermann, Greta, *"Der Frage der endlich vielen Schritte in der Theorie der Polynomideale,"* Math. Ann. **95** (1926), pp. 736–788.

[Hoh30] Hoheisel, G., *"Primzahlprobleme in der Analysis,"* Sitz. Preuss. Akad. Wiss. Phys.-Math. Kl. (1930), pp. 580–588.

[HW00] Huang, Ming-Deh and Wong, Yiu-Chung, *"Extended Hilbert irreducibility and its applications,"* Ninth Annual ACM-SIAM Symposium on Discrete Algorithms (San Francisco, CA, 1998), J. Algorithms 37 (2000), no. 1, pp. 121–145.

[IJ79] Iwaniec, Henryk and Jutila, Matti, *"Primes in short intervals,"* Ark. Mat. 17 (1979), no. 1, pp. 167–176.

[Koi96] Koiran, Pascal, *"Hilbert's Nullstellensatz is in the Polynomial Hierarchy,"* DIMACS Technical Report 96-27, July 1996. (This preprint considerably improves the published version which appeared Journal of Complexity **12** (1996), no. 4, pp. 273–286.)

[Koi97] ____________, *"Randomized and Deterministic Algorithms for the Dimension of Algebraic Varieties,"* Proceedings of the 38th Annual IEEE Computer Society Conference on Foundations of Computer Science (FOCS), Oct. 20–22, 1997, ACM Press.

[Kol88] Kollár, János, *"Sharp effective Nullstellensatz,"* J. Amer. Math. Soc. 1 (1988), no. 4, pp. 963–975.

[KP94] Krick, Teresa and Pardo, Luis-Miguel, *"Une approche informatique pour l'approximation diophantienne,"* C. R. Acad. Sci. Paris **318** (1994), pp. 407–412.

[LO77] Lagarias, Jeff and Odlyzko, Andrew, *"Effective Versions of the Chebotarev Density Theorem,"* Algebraic Number Fields: L-functions and Galois Properties (Proc. Sympos. Univ. Durham, Durham, 1975), 409–464, Academic Press, London, 1977.

[Lan49] Landau, Edmund, *"Einführung in die Elementare und Analytische Theorie der Algebraischen Zahlen und der Ideale,"* (German) Chelsea Publishing Company, New York, N. Y., 1949.

[Lan94] Lang, Serge, *"Algebraic Number Theory,"* 2nd ed., Springer-Verlag, New York, 1994.

[Lec03] Lecerf, Grégoire, *" Computing the equidimensional decomposition of an algebraic closed set by means of lifting fibers,"* J. Complexity 19 (2003), no. 4, pp. 564–596.

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

[Mil76] Miller, Gary L., *"Riemann's Hypothesis and Tests for Primality,"* J. Comput. System Sci. **13** (1976), no. 3, 300–317.

[Mit68] Mitsui, Takayoshi *"On the Prime Ideal Theorem,"* J. Math. Soc. Japan **20** (1968), pp. 233–247.

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

[Phi90] Philippon, Patrice, *"Dénominateurs dans le théorème des zeros de Hilbert,"* Acta Arith. **58** (1990), pp. 1–25.

[Pla84] Plaisted, David A., *"New NP-Hard and NP-Complete Polynomial and Integer Divisibility Problems,"* Theoret. Comput. Sci. 31 (1984), no. 1–2, 125–138.

[Pra75] Pratt, Vaughan R., *"Every Prime has a Succinct Certificate,"* SIAM J. Comput. **4** (1975), 327–340.

[Roj00] Rojas, J. Maurice, *"Algebraic Geometry Over Four Rings and the Frontier to Tractability,"* Contemporary Mathematics, vol. 270, Proceedings of a Conference on Hilbert's Tenth Problem and Related Subjects (University of Gent, November 1-5, 1999), edited by Jan Denef, Leonard Lipschitz, Thanases Pheidas, and Jan Van Geel, pp. 275–321, AMS Press (2000).

[Roj01] ________________, *"Computational Arithmetic Geometry I: Sentences Nearly in the Polynomial Hierarchy,"* J. Comput. System Sci., STOC '99 special issue, vol. 62, no. 2, march 2001, pp. 216–235.

[Sch80] Schwarz, Jacob T., *"Fast Probabilistic Algorithms for Verification of Polynomial Identities,"* Journal of the ACM, 27:701–717, 1980.

[Sel43] Selberg, Atle, *"On the Normal Density of Primes in Small Intervals, and the Difference Between Consecutive Primes,"* Archiv for Mathematik og Naturvidenskab B. 47 (1943), No. 6, pp. 87–105.

[Sil02] Silberman, Lior, *"Effective Versions of the Čebotarev Density Theorem,"* downloadable from `http://www.math.princeton.edu/~lior/work` . (This paper is a rewrite of [LO77] with the goal of giving reasonable explicit bounds on all effective constants that were left uncomputed in [LO77].)

[Sma00] Smale, Steve, *"Mathematical Problems for the Next Century,"* Mathematics: Frontiers and Perspectives, pp. 271–294, Amer. Math. Soc., Providence, RI, 2000.

[Sok68] Sokolovskiĭ, A. V., *"A Theorem on the Zeros of Dedekind's Zeta-Function and the Distance Between 'Neighboring' Prime Ideals,"* Acta Arith. **13** (1967/1968), pp. 321–334.

[Som99] Sombra, Martin, *"A sparse effective Nullstellensatz,"* Adv. Appl. Math. **22** (1999), pp. 271–295.

[Som02] ______________, *"Minima Successifs des Variétés Toriques Projectives,"* Math ArXiV preprint `math.NT/0209195`, submitted for publication.

[SVW01] Sommese, Andrew J.; Verschelde, Jan; and Wampler, Charles W., *"Numerical decomposition of the solution sets of polynomial systems into irreducible components,"* SIAM J. Numer. Anal. 38 (2001), no. 6, pp. 2022–2046.

[Sto85] Stockmeyer, Larry, *"On Approximation Algorithms for* #**P***,"* SIAM Journal on Computing, 14(4):849–861, 1985.

[TF00] Tenenbaum, Gérald and Mendès France, Michel, *The Prime Numbers and Their Distribution,* Student Mathematical Library, vol. 6, AMS Press, Rhode Island, 2000.

[Zac86] Zachos, S., *"Probabilistic Quantifiers, Adversaries, and Complexity Classes: An Overview,"* Proc. 1st Structure in Complexity Theory Conference, vol. 223, Lecture Notes in Computer Science, Springer-Verlag, 1986.