hexagon:2611.01018v2

HILBERT'S NULLSTELLENSATZ IS IN AM FROM A ZERO-FREE HALF-PLANE OF DEDEKIND ZETA FUNCTIONS, AFTER KOIRAN

Abstract. In 1996 Koiran proved, assuming the generalized Riemann hypothesis (GRH), that deciding whether a system of polynomial equations with integer coefficients has a complex solution (Hilbert's Nullstellensatz, HN) is in the Arthur–Merlin class AM, hence in the second level of the polynomial hierarchy. GRH enters his proof through one estimate, a count of the primes modulo which an irreducible integer polynomial has a root. We show that this estimate, with exponent $7/8+\varepsilon$ in place of $1/2$, follows in two lines from the effective Chebotarev theorem in B. Hu's preprint on the zero-free half-plane $\Re s > 7/8$, and that Koiran's proof then runs with primes of an explicit, polynomial bit length. Any zero-free half-plane $\Re s > \theta$, $\theta < 1$, common to all Dedekind zeta functions suffices, for instance $\Re s > 31/32$ of Cureton and Thorner: the estimate is then Frei, Sofos and Widmer's effective Chebotarev theorem, as Baldwin and Sivek used it for one polynomial in work on 3-manifold recognition, and the step to AM is Proposition 17.2 of our paper hexagon:2611.00987. So HN is in AM granted Hu's theorem or that of Cureton and Thorner. Both are unrefereed preprints of October 2026; the second is formalized in Lean according to its authors. Through published reductions that use GRH only via Koiran's theorem, the dimension problem and the parametric Nullstellensatz are then in AM, vanishing of Schubert coefficients is in $\mathsf{AM} \cap \mathsf{coAM}$ in types A–D, so it is not NP-hard unless the polynomial hierarchy collapses to its second level, and homogeneous systems of parameters are constructible in $\mathsf{FP}^{\Sigma_2^{\mathsf{P}}}$. Andrews, Garg and Schost placed HN in the counting hierarchy with no hypothesis; AM is the smaller class. Produced by GPT-6 Astra (ChatGPT Pro mode) and Claude Opus 5.5 at effort max, checked by Claude Opus 5.5 at effort high, written by Claude Fable 5.2 at effort max. No human has checked it.

1. Koiran's theorem and the result

1.1. **Koiran's theorem.** Let HN be the following decision problem. An instance is a system

$$f_1(X_1,\dots,X_n)=0,\ \dots,\ f_s(X_1,\dots,X_n)=0, \qquad f_i \in \mathbb{Z}[X_1,\dots,X_n], \tag{1}$$

given by the lists of its monomials with their coefficients in binary; the question is whether it has a solution in $\mathbb{C}^n$. By Hilbert's Nullstellensatz the answer is no exactly when 1 lies in the ideal generated by the f_i over $\mathbb{Q}$. The problem is NP-hard, and effective forms of the Nullstellensatz place it in PSPACE [8, §1].

Koiran proved in 1996 that under GRH it lies much lower: in the journal article, in $\mathsf{RP}^{\mathsf{NP}} \subseteq \Pi_2^{\mathsf{P}}$ [8, Theorem 2, p. 276], and in the extended report, in the Arthur–Merlin class AM [9, Theorem 2, p. 5], where $\mathsf{NP} \subseteq \mathsf{AM} \subseteq \Pi_2^{\mathsf{P}}$ [9, abstract]. His method counts primes. For a system S as in (1), let R_S be the set of primes p such that S has a solution in $\mathbb{F}_p^n$, and $\pi_S(x)$ the number of elements of R_S not exceeding x. If S has no complex solution, then $\pi_S(x) \le A$ for an explicit A and all x. If it has one, then $\pi_S(x_0) \ge B > 8A$ at a point x_0 of polynomial bit length [8, Theorem 1, p. 275]. A hashing protocol tells the two cases apart.

Only the second case uses GRH, and it uses it through one statement [8, Theorem 9, p. 282]. Let $f \in \mathbb{Z}[X]$ be irreducible of degree n with discriminant Δ, and let $W(p)$ be the number of roots of f in $\mathbb{F}_p$. Then, under GRH,

$$S(x) = \sum_{p \le x,\ p \nmid \Delta} (1 - W(p)) = O(x^{1/2}\log(\Delta x^n)). \tag{2}$$

Date: 25 November 2026.

Koiran takes this bound from Adleman and Odlyzko and notes that it needs only the prime ideal theorem with its GRH error term, not the full Chebotarev theorem [8, p. 282].

1.2. **The theorems.** For a number field K write $n_K = [K : \mathbb{Q}]$, d_K for the absolute value of its discriminant, ζ_K for its Dedekind zeta function, and $\pi_K(x)$ for the number of nonzero prime ideals of its ring of integers of norm at most x; so $\pi_{\mathbb{Q}} = \pi$. Put $\mathrm{Li}(x) = \int_2^x dt/\log t$. Logarithms are natural unless a base is shown. We use two statements, each for a real parameter below 1.

(Z_θ) For every number field K, $\zeta_K(s) \neq 0$ for all $s \neq 1$ with $\Re s > \theta$.

(P_η) There is a constant $C_0 \geq 1$ such that for every number field K and every $x \geq 2$,

$$\bigl|\pi_K(x) - \mathrm{Li}(x)\bigr| \leq C_0\,(\log d_K + n_K)\,x^{\eta}.$$

GRH gives ($\mathrm{Z}_{1/2}$) and (P_η) for every $\eta > 1/2$.

Throughout, a system S as in (1) has n unknowns and s equations, its polynomials have degree at most d and coefficients of bit size at most $L \geq 1$, and $\sigma = 2 + \sum_i \deg f_i$, as in [8, §1.1]. Koiran's bound for unsatisfiable systems is

$$A = d^{c_1 n} s(\log_2 s + L), \qquad B = 8A(\log_2 A + 3), \tag{3}$$

with an absolute constant c_1 [8, Theorem 1].

Theorem A. *Suppose that* (P_η) *holds for some* $\eta \in [1/2, 1)$*, with constant* C_0*. Then* $\mathsf{HN} \in \mathsf{AM} \subseteq \Pi_2^{\mathsf{P}}$*. More precisely, there is an absolute constant* c *such that, for every system* S *as above, on putting*

$$M = L \cdot 2^{(n \log_2 \sigma)^c}, \qquad x_0 = \left\lceil \left(\frac{52\, C_0\, M^4}{1-\eta} \right)^{2/(1-\eta)} \right\rceil,$$

one has $A \leq M$ *and:*

1. *if* S *has no solution in* $\mathbb{C}^n$*, then* $\pi_S(x) \leq A$ *for all* x*;*
2. *if* S *has a solution in* $\mathbb{C}^n$*, then* $\pi_S(x) \geq B$ *for all* $x \geq x_0$*.*

The bit length of x_0 *is at most* $\frac{8}{1-\eta} \log_2 M + O(1)$*, the constant depending on* η *and* C_0*; it is polynomial in the size of* S*.*

This is Koiran's Theorem 1 without GRH. His own threshold is $x_0 \geq L^{c_2} 2^{(n \log \sigma)^{c_3}}$ with unspecified absolute constants; the threshold above has the same form, with the exponent $8/(1-\eta)$ on L.

Theorem B. (a) *The effective Chebotarev theorem of Hu* [7, Corollary 9.6, p. 56] *gives* (P_η) *for every* $\eta \in (7/8, 1)$*.*

(b) *If* (Z_θ) *holds for some* $\theta \in [1/2, 1)$*, then* (P_η) *holds for every* $\eta \in (\theta, 1)$*.*

Two preprints assert (Z_θ). Cureton and Thorner state ($\mathrm{Z}_{31/32}$) [5, Theorem 1.1, p. 3]. Hu states that for every number field F and every unitary Hecke character χ of F, $L_F(s, \chi)$ is nonzero for $\Re s > 7/8$ [7, Theorem 1.2, p. 2]; the trivial character gives ($\mathrm{Z}_{7/8}$).

Corollary C. *If the theorem of Hu or the theorem of Cureton and Thorner just quoted is true, then* $\mathsf{HN} \in \mathsf{AM} \subseteq \Pi_2^{\mathsf{P}}$*, with no further hypothesis. With Hu's Corollary 9.6 and* $\eta = 8/9$ *the threshold of Theorem A is* $x_0 = \lceil (468\, C_0 M^4)^{18} \rceil$*, where* C_0 *is twice the constant of that corollary for* $\varepsilon = 1/72$*.*

Both inputs are preprints posted on Hexagon in October 2026, and neither has been refereed. Cureton and Thorner report that their Theorem 1.1 is formalized in Lean, with a public certificate [5, abstract and §15]. Hu's preprint is not formalized and says that its text and arguments were developed predominantly with language models [7, p. 58]. We have read the statements of both and not their proofs. A third preprint, by Liu, states (Z_θ) for $\theta = 0.87334470$ [15, Theorem 7.21]. Corollary C is exactly as reliable as these sources.

Corollary D. *Suppose* (P_η) *holds for some* $\eta < 1$*; by Theorem B this is so if one of the theorems quoted before Corollary C is true. Then:*

(1) *the problem* DIM*, whether the complex solution set of a system* (1) *has dimension at least a given integer, is in* AM*;*
(2) *the parametric Nullstellensatz* HNP*, whether a system with coefficients in* $\mathbb{Z}[y_1, \dots, y_k]$ *has a solution over an algebraic closure of* $\mathbb{Q}(y_1, \dots, y_k)$*, is in* AM*;*
(3) *the vanishing problem for Schubert coefficients in each of the types A, B, C, D is in* $\mathsf{AM} \cap \mathsf{coAM}$*; it is not NP-hard unless* $\mathsf{PH} = \Sigma_2^{\mathsf{P}}$*, and not coNP-hard unless* $\mathsf{PH} = \Pi_2^{\mathsf{P}}$*;*
(4) HN *for systems given by arithmetic circuits, and the existence of a nonzero solution of a homogeneous such system, are in* AM*;*
(5) *for a cone* $Z \subseteq \mathbb{C}^t$ *given by homogeneous circuit equations,* $\dim Z$ *and a homogeneous system of parameters of linear forms with integer coefficients can be computed in* $\mathsf{FP}^{\Sigma_2^{\mathsf{P}}}$.

Each item is a published theorem under GRH: (1) is Koiran's [11, Theorem 4.1], (2) is due to Ait El Manssour, Balaji, Nosan, Shirmohammadi and Worrell [1, Theorem 1], (3) to Pak and Robichaux [20, Theorems 1.1 and 3.4, Corollary 1.4], (4) and (5) to Mulmuley [16, Theorems 2.10 and 3.4], the last with "in PH" in place of $\mathsf{FP}^{\Sigma_2^{\mathsf{P}}}$. Section 5 gives the precise statements and shows, source by source, that GRH is used only through Koiran's theorem.

1.3. **Why this matters.** Koiran's theorem is the reference for the complexity of the most basic problem of computational algebraic geometry, and for thirty years it has carried the hypothesis GRH. So have the results built on it: the dimension of a variety, solvability over function fields, the vanishing of Schubert coefficients, and Noether normalization in geometric complexity theory. For Schubert vanishing the hypothesis stood in the answer to a question of Adve, Robichaux and Yong, whether the problem is NP-hard [20, Question 1.2 and Corollary 1.4]. All these statements lose the hypothesis at once, because each uses it only through the count (2), and that count needs far less than GRH: a zero-free half-plane of any fixed width. Such half-planes were proved, according to the preprints above, in October 2026.

1.4. **What is whose.** *Koiran.* The method and every step of the proof other than the prime count: the gap theorem, the bounds for algebraic solutions and primitive elements, the passage to solutions modulo p, and the protocol [8, Theorems 1, 2, 4, 5, 7, 8, Lemma 3, Corollary 1], [9, Theorem 2], with the correction of the bound in Theorem 8 in his erratum [10]. The prime count (2) under GRH is Adleman and Odlyzko's, from the effective Chebotarev theorem of Lagarias and Odlyzko [14].

The half-planes. Cureton and Thorner [5], Hu [7] and Liu [15]. They build on two preprints of OpenAI: a zero-free half-plane $\Re s > 7/8$ for Dirichlet L-functions and Hecke L-functions of $\mathbb{Q}(\sqrt{-3})$, and the strip $\Re s > 1 - 10^{-6}$ for finite-order Hecke L-functions of cyclotomic fields containing the twelfth roots of unity [18, Theorem 1.2], as described in [5, pp. 2–3] and [7, p. 2].

Weaker hypotheses than GRH. Rojas showed in 2003 that $\mathsf{HN} \in \mathsf{AM}$ follows from either of two hypotheses weaker than GRH, on prime ideals in short intervals or on sums over zeros of Dedekind zeta functions [21, Theorem 1].

The estimates from a half-plane. Frei, Sofos and Widmer proved in October 2026 that the effective Chebotarev theorem of Lagarias and Odlyzko holds with error term $x^{1-\delta}$ when the Dedekind zeta function concerned has no zero with $\Re s > 1-\delta$ [6, Theorem 1.1, p. 2]. Theorem B(b) is the case of a trivial extension. From that theorem Baldwin and Sivek proved, in November 2026, that under a zero-free half-plane common to all Dedekind zeta functions an irreducible $f \in \mathbb{Z}[x]$ of degree d has a root modulo a prime of size polynomial in d and $\log \|f\|$ [4, Theorem 2.1, p. 4]. This is the estimate that Koiran's proof draws from GRH, for one polynomial. So they replaced GRH by a half-plane in it before our paper [17], and for another purpose, recognition problems

for 3-manifolds (Section 1.5); they report that Agol was aware of the same [4, p. 3]. Nothing in their paper concerns HN or the class AM.

From the estimate to AM. That (Z_θ) for one fixed $\theta < 1$ gives $\mathsf{HN} \in \mathsf{AM}$, and that the theorem of Cureton and Thorner provides such a θ, is Proposition 17.2 of our paper [17, p. 59 and Table 1], which writes out the transfer and an explicit two-message protocol; its proof derives the estimate it needs from the half-plane directly. Theorem A restates it with the threshold made explicit.

New here. The explicit threshold x_0 in the step from the count of primes to $\mathsf{HN} \in \mathsf{AM}$ (Theorems A and 4.1); the derivation through Hu's Corollary 9.6, which gives Koiran's estimate with exponent $7/8 + \varepsilon$ (Propositions 3.1(a) and 3.2); and Corollary D, with the place where each source uses GRH. The reductions in Corollary D belong to their authors.

1.5. **Context.** Andrews, Garg and Schost proved in February 2026, with no hypothesis, that HN is in the counting hierarchy CH, for systems over $\mathbb{Q}$, number fields, finite fields and their rational function fields; they also compute the dimension and the cardinality of a variety in $\mathsf{FP}^{\mathsf{CH}}$ [2, Theorems 1.1, 1.3, 1.4]. Since $\mathsf{PH} \subseteq \mathsf{CH}$ by Toda's theorem and $\mathsf{CH} \subseteq \mathsf{PSPACE}$, as they recall [2, §1.2], the class $\mathsf{AM} \subseteq \Pi_2^{\mathsf{P}}$ is contained in theirs. So for integer systems over $\mathbb{C}$ Corollary C gives a smaller class, and it rests on the half-plane preprints; their theorem needs no analytic input and covers positive characteristic and counting, which the method here does not reach.

Rojas's two hypotheses [21, p. 6] are stated with exponents that depend on $n_K \log d_K$. We have not examined whether a fixed half-plane implies them; the substitution is made in Koiran's proof directly.

Three-manifold topology. Kuperberg's proof that knottedness is in NP under GRH [12, Theorem 1.1], and the coNP results built on it, among them Zentner's for the recognition of the 3-sphere [22, Theorem 11.2], use GRH only to find a prime of polynomial bit length modulo which an irreducible integer polynomial has a root [12, Theorem 3.2]; it is the estimate that Koiran obtains under GRH [4, p. 2]. Baldwin and Sivek observed that a zero-free half-plane common to all Dedekind zeta functions is enough for it [4, Theorem 2.1]. They concluded that the recognition of the unknot, of the 3-sphere, of torus knots and of hyperbolic knots, and the hyperbolicity of cusped 3-manifolds, are in coNP modulo such a half-plane [4, Theorems 1.1 and 1.3]. They note that the Lean-formalized proof of Cureton and Thorner would make these results unconditional, and they keep them conditional [4, pp. 2–3]. They also record that unknot recognition was already in coNP with no hypothesis by Lackenby [13], and hyperbolic knot recognition by Haraway and Hoffman [4, Remark 1.4]. These results are theirs. Theorem A(2) gives such a prime for a whole system, and we claim nothing in topology.

The Riemann hypothesis for Dirichlet L-functions does not suffice for Koiran's count: the field K in it is generated by a solution of the system and is in general not abelian, as $X^3 - 2 = 0$ shows [17, §17]. For the same reason the strip of [18], which concerns cyclotomic fields, does not suffice alone, and the extension to all number fields in [5] and [7] is what is used.

1.6. **Scope.** Proved here, granted (P_η) for some $\eta < 1$: Theorem A and Corollary D. Theorem B(a) is a two-line consequence of Hu's corollary, and Theorem B(b) is a case of the theorem of Frei, Sofos and Widmer. Not proved here: the half-plane theorems themselves. Nothing is claimed about $\mathsf{HN} \in \mathsf{NP}$, about systems in positive characteristic, or about further results of [16] that assume GRH.

1.7. **Proof overview.** The difficulty in Koiran's proof is the lower bound for satisfiable systems. A solution generates a number field K of degree and discriminant exponential in the input, and the primes p modulo which the system is solvable include those with a prime ideal of degree one above them in K, up to a few exceptions. One must find at least B such primes below a bound of polynomial bit length, uniformly in K. The prime ideal theorem without a hypothesis is of no use

here: with the zero-free regions known unconditionally, its main term dominates only from an x of size $\exp((n_K \log d_K)^{O(1)})$ on, a number of exponential bit length.

The idea is that a zero-free half-plane gives the prime ideal theorem with error $O((\log d_K + n_K)x^\eta)$ for an $\eta < 1$, with constants independent of K. The main term $x/\log x$ then beats the error, and every other loss, as soon as $x^{1-\eta}$ exceeds a fixed power of $n_K \log d_K$. That happens at x of polynomial bit length, because n_K and $\log d_K$ are at most exponential. The hypothesis (P_η) is used only in Proposition 3.2 and through it in Theorem 4.1; Koiran's algebraic bounds (Proposition 2.1) and his protocol are used unchanged.

2. Koiran's reduction to a count of primes

This section recalls the part of Koiran's proof that does not involve GRH.

Proposition 2.1 (Koiran)**.** *There are absolute constants c_1 and c such that for every system S as in (1), with A as in (3) and $M = L \cdot 2^{(n \log_2 \sigma)^c}$, one has $A \le M$ and the following hold.*

1. *If S has no solution in $\mathbb{C}^n$, then R_S has at most A elements.*
2. *If S has a solution in $\mathbb{C}^n$, there are an irreducible polynomial $R \in \mathbb{Z}[X]$ of degree $N \le M$, with coefficients of bit size at most M, and an integer $a \ge 1$ with $\log_2 a \le M$, such that every prime $p \nmid a$ modulo which R has a root belongs to R_S.*

Proof. (1) is [8, Theorem 5, p. 279], with the constant as in [8, Theorem 1]: an identity $a_0 = \sum_i g_i f_i$ with a nonzero integer a_0 of bit size at most A holds over $\mathbb{Z}$, so every $p \in R_S$ divides a_0.

(2) By [8, Theorem 7, p. 280] the system has a solution $(x_1, \dots, x_n)$ in which each x_i is a root of an integer polynomial of degree at most $D = 2^{(n \log_2 \sigma)^{c'}}$ with coefficients of bit size at most $H = L \cdot 2^{(n \log_2 \sigma)^{c''}}$. By [8, Theorem 4, p. 278] there is a primitive element r for $x_1, \dots, x_n$ which is a root of an irreducible $R \in \mathbb{Z}[X]$ of degree at most D^n with coefficients of bit size at most $H \cdot D^{n^{O(1)}}$, and $x_i = Q_i(r)/a_i$ with $Q_i \in \mathbb{Z}[X]$ and integers $a_i \ge 1$, $\log_2 a_i \le H \cdot D^{n^{O(1)}}$. Let $a = \prod_i a_i$. By [8, Lemma 3, p. 281], if $p \nmid a$ and R has a root in $\mathbb{F}_p$, then S has a solution in $\mathbb{F}_p^n$. Since $n \log_2 \sigma \ge \log_2 3$, all the bounds are at most $L \cdot 2^{(n \log_2 \sigma)^c}$ for a suitable absolute c. So is A, because $d \le \sigma$, $s \le \sigma$ and $\log_2 s + L \le L\sigma$ give $A \le L \cdot 2^{(c_1+2) n \log_2 \sigma}$. □

3. The count of primes from a half-plane

This section proves Theorem B and replaces (2).

Proposition 3.1. *Theorem B holds. In* (a) *one may take $C_0 = 2c(\eta - 7/8)$, where $c(\varepsilon)$ is the constant of* [7, Corollary 9.6]. *In* (b), *for every number field K and every $x > 2$,*

$$|\pi_K(x) - \mathrm{Li}(x)| \le c_1\, x^\theta \Big(\frac{\log d_K}{1-\theta} + n_K \log x \Big), \tag{4}$$

with the absolute constant c_1 of [6, Theorem 1.1].

Proof. (a) Hu's corollary reads: for a finite Galois extension L/F of number fields with group G, a conjugacy class C of G, $c_C = |C|/|G|$ and $\mathcal{D}_L = \log(e\, d_L) + n_L$, the number $\pi_C(x)$ of prime ideals of F unramified in L, of norm at most x and with Frobenius class C, satisfies $|\pi_C(x) - c_C \,\mathrm{Li}(x)| \le c(\varepsilon)\, c_C\, \mathcal{D}_L\, x^{7/8+\varepsilon}$ for $0 < \varepsilon < 1/8$ and $x \ge 2$, with $c(\varepsilon)$ effective and independent of L, F and C. Take $L = F = K$ and $C = \{1\}$. Then $c_C = 1$, every prime ideal of K is counted, so $\pi_C = \pi_K$, and $\mathcal{D}_K = 1 + \log d_K + n_K \le 2(\log d_K + n_K)$. With $\varepsilon = \eta - 7/8$ this is (P_η).

(b) This is the theorem of Frei, Sofos and Widmer [6, Theorem 1.1, p. 2]. It reads: let L/K be a Galois extension of number fields with group G, let C be a conjugacy class of G and $0 < \delta \le 1/2$,

and suppose that ζ_L has no zero with $\Re s > 1-\delta$. Then for $x > 2$ the number $\pi_C(x, L/K)$ of prime ideals of K unramified in L, of norm at most x and with Frobenius class C, satisfies

$$\Big|\pi_C(x, L/K) - \frac{|C|}{|G|}\operatorname{Li}(x)\Big| \le c_1 \frac{|C|}{|G|}\, x^{1-\delta} \log(d_L^{1/\delta} x^{n_L}),$$

with an effective absolute constant c_1. They obtain it by modifying the proof of Lagarias and Odlyzko [14], which is the case $\delta = 1/2$. Take $L = K$, $C = \{1\}$ and $\delta = 1-\theta$; this is (4). For $x > 2$ and $\theta < \eta < 1$ the bracket in (4) is at most $(\log d_K + n_K)\log x/((1-\theta)\log 2)$, and $x^\theta \log x \le x^\eta/(e(\eta-\theta))$; at $x = 2$ trivially $|\pi_K(2) - \operatorname{Li}(2)| \le n_K$. This is (P_η). □

A proof of the consequence of (b) needed below that does not pass through [6], by a contour shift for a weighted prime ideal sum, is in [17, proof of Proposition 17.2].

Proposition 3.2 (Koiran's Theorem 9 and Corollary 1 from (P_η))**.** *Let $f \in \mathbb{Z}[X]$ be irreducible of degree $n \ge 1$, with leading coefficient a and discriminant Δ, and let $K = \mathbb{Q}[X]/(f)$. For a prime p let $W(p)$ be the number of roots of f in $\mathbb{F}_p$, let $S(x)$ be as in (2), and let $\pi_f(x)$ be the number of primes $p \le x$ with $W(p) \ge 1$. Then for $x \ge 2$:*

(1) $|S(x) - (\pi(x) - \pi_K(x))| \le \frac{n}{2}\sqrt{x} + (2n+1)\log_2|a\Delta|$;

(2) *if (P_η) holds with constant C_0, then*

$$|S(x)| \le C_0\,(\log d_K + n + 1)\, x^\eta + \tfrac{n}{2}\sqrt{x} + (2n+1)\log_2|a\Delta|,$$
$$\log d_K \le (n-1)(n-2)\log|a| + \log|\Delta|;$$

(3) $\pi_f(x) \ge \frac{1}{n}(\pi(x) - \log_2|\Delta| - |S(x)|)$.

Proof. (1) Let α be the image of X in K. Then $a\alpha$ is integral, with monic minimal polynomial $g(Y) = a^{n-1}f(Y/a)$ of discriminant $a^{(n-1)(n-2)}\Delta$. For a prime $p \nmid a\Delta$ the index of $\mathbb{Z}[a\alpha]$ in the ring of integers of K is prime to p, so by Dedekind's theorem the prime ideals of degree one above p correspond to the roots of g in $\mathbb{F}_p$, and these to the roots of f by $k \mapsto ak$. Thus $W(p)$ is the number of prime ideals of degree one above p. Summing over $p \le x$, $p \nmid a\Delta$,

$$\sum_{p\le x,\ p\nmid a\Delta} W(p) = \pi_K(x) - N_2(x) - N_b(x),$$

where $N_2(x)$ counts the prime ideals of norm at most x and degree at least two, and $N_b(x)$ those of degree one dividing $a\Delta$. A prime ideal of degree at least two and norm at most x lies above a prime $p \le \sqrt{x}$, and at most $n/2$ of them lie above each p; so $N_2(x) \le \frac{n}{2}\sqrt{x}$. At most n prime ideals lie above each prime, so $N_b(x) \le n\,\omega(a\Delta)$, where ω counts prime factors. The primes $p \le x$ dividing $a\Delta$ number at most $\omega(a\Delta)$, and those dividing a but not Δ contribute at most $n\,\omega(a)$ to $S(x)$ in absolute value. Since $\omega(m) \le \log_2|m|$, the four errors add up to at most $\frac{n}{2}\sqrt{x} + (2n+1)\log_2|a\Delta|$.

(2) Apply (P_η) to K and to $\mathbb{Q}$, where $\log d_{\mathbb{Q}} + n_{\mathbb{Q}} = 1$. The discriminant of K divides that of g.

(3) This is Koiran's argument [8, Corollary 1, p. 282]. The primes $p \le x$ with $p \nmid \Delta$ number at least $\pi(x) - \log_2|\Delta|$, so $\sum_{p\le x,\,p\nmid\Delta} W(p) \ge \pi(x) - \log_2|\Delta| - |S(x)|$. As f is irreducible in $\mathbb{Z}[X]$ it is not zero modulo p, so $W(p) \le n$, and $W(p) \ge 1$ for every prime counted on the left. □

Remark 3.3. Part (2) is (2) with x^η in place of $x^{1/2}$, and Hu's corollary gives it with $\eta = 7/8 + \varepsilon$ by Proposition 3.1(a). For a polynomial that is not monic, the primes dividing its leading coefficient a have to be set aside together with those dividing Δ; they are not controlled by Δ, and this is the term $\log_2|a|$ above. In Koiran's application $\log_2|a|$ is bounded like the other coefficients, so nothing changes there. The paper [17, §17] makes the same point and avoids the term by passing to an integral primitive element. For a monic f, the prime ideal estimate under a half-plane, and from it a prime of size polynomial in the degree and in the logarithm of the coefficients modulo which f has a root, were obtained before by Baldwin and Sivek [4, Corollary 3.3 and

Theorem 2.1], who reduce a polynomial that is not monic to a monic one [4, §5]. For a single polynomial, Proposition 3.2 with the bound for the discriminant in the proof of Theorem 4.1 gives their Theorem 2.1 again.

4. Proof of Theorem A, and the explicit threshold

This section replaces Koiran's Theorems 8 and 1 and concludes.

Theorem 4.1 (Koiran's Theorem 8 from (P_η))**.** *Assume* (P_η) *with constant* C_0*, where* $1/2 \le \eta < 1$*. Let* S *have a solution in* $\mathbb{C}^n$*, and let* M *be as in Proposition 2.1. Then for every* $x \ge 4$*,*

$$\pi_S(x) \;\ge\; \frac{x}{2M\log x} - 19\,C_0\,M^3 x^\eta.$$

Proof. Let R, N and a be as in Proposition 2.1(2), let a_R and Δ_R be the leading coefficient and the discriminant of R, and $K = \mathbb{Q}[X]/(R)$. The coefficients of R are smaller than 2^M in absolute value. Hadamard's inequality for the Sylvester matrix of R and R' gives $|\Delta_R| \le ((N+1)^{1/2}2^M)^{N-1}(N^{3/2}2^M)^N$, hence $\log_2|\Delta_R| \le 2N\log_2(N+1) + 2NM \le 4M^2$. So $\log_2|a_R\Delta_R| \le 5M^2$, and by Proposition 3.2(2), $\log d_K \le M^3 + 4M^2 \le 5M^3$.

By Proposition 2.1(2), $\pi_S(x) \ge \pi_R(x) - \log_2 a \ge \pi_R(x) - M$. By Proposition 3.2(2) and (3), and $\pi(x) \ge \mathrm{Li}(x) - C_0 x^\eta$,

$$\begin{aligned}\pi_R(x) \;&\ge\; \frac{1}{N}\Big(\mathrm{Li}(x) - C_0(5M^3+N+2)x^\eta - \frac{N}{2}\sqrt{x} - (2N+2)\cdot 5M^2\Big)\\ &\ge\; \frac{\mathrm{Li}(x)}{M} - 8C_0M^3x^\eta - \frac{\sqrt{x}}{2} - 20M^2.\end{aligned}$$

Subtracting M leaves $\mathrm{Li}(x)/M - 8C_0M^3x^\eta - \frac12\sqrt{x} - 21M^2$. For $x \ge 4$ we have $\mathrm{Li}(x) \ge (x-2)/\log x \ge x/(2\log x)$ and $x^\eta \ge \sqrt{x} \ge 2$, so $\frac12\sqrt{x} + 21M^2 \le 11\,C_0M^3x^\eta$, and the claim follows. □

The shape of this bound is that of Koiran's Theorem 8 as corrected in his erratum [10]: the error terms are not divided by the degree.

Proof of Theorem A. Part (1) is Proposition 2.1(1). For (2), $A \le M$ gives $B = 8A(\log_2 A + 3) \le 32M^2 \le 16\,C_0M^3x^\eta$ for $x \ge 4$. By Theorem 4.1 it suffices that $x/(2M\log x) \ge 35\,C_0M^3x^\eta$, that is,

$$\frac{x^{1-\eta}}{\log x} \;\ge\; 70\,C_0M^4.$$

Put $\delta = (1-\eta)/2$. Since $\log x \le x^\delta/(e\delta)$ for all $x > 0$, the left side is at least $e\delta\,x^\delta$, and the inequality holds as soon as $x \ge (140\,C_0M^4/(e(1-\eta)))^{2/(1-\eta)}$. As $140/e < 52$, it holds for all $x \ge x_0$. The bit length of x_0 is at most $\frac{2}{1-\eta}(4\log_2 M + \log_2\frac{52C_0}{1-\eta}) + 1$, and $\log_2 M = \log_2 L + (n\log_2\sigma)^c$ is polynomial in the size of S.

It remains to pass from the gap to the class. Koiran's proof of [9, Theorem 2, pp. 5–6] uses the system only through the set $E = R_S \cap [1, x_0]$, of which it needs three properties: membership in E has certificates of polynomial size, namely a solution modulo p together with the primality of p; $|E| \le A$ if S has no complex solution; and $|E| \ge B$ if it has one. Let m be the integer with $A \le 2^{m-2} < 2A$, so that $m2^m \le B$. Arthur chooses m random linear hash functions from the binary codes of the integers up to x_0 to $\{0,1\}^m$. Merlin must exhibit elements $y, y_1, \ldots, y_m$ of E such that y collides with $y_i \ne y$ under the i-th function, for every i. If $|E| \ge m2^m$ such elements exist for every choice of the functions, and if $|E| \le 2^{m-2}$ they exist with probability at most $1/2$, by Sipser's lemma as used in [9, pp. 5–6]. With x_0 as above all three properties hold under (P_η), so the protocol decides HN, with perfect completeness. This gives $\mathsf{HN} \in \mathsf{AM}$, and $\mathsf{AM} \subseteq \Pi_2^{\mathsf{P}}$ [9, abstract]. □

Proof of Corollary C. Hu's Corollary 9.6 gives $(\mathrm{P}_{8/9})$ with $C_0 = 2c(1/72)$ by Proposition 3.1(a), and then $52\,C_0M^4/(1-\eta) = 468\,C_0M^4$ and $2/(1-\eta) = 18$. The theorem of Cureton and Thorner is $(\mathrm{Z}_{31/32})$, which gives (P_η) for $\eta > 31/32$ by Proposition 3.1(b). Apply Theorem A. □

5. Consequences

This section proves Corollary D. Throughout it we assume (P_η) for some $\eta < 1$, so that $\mathsf{HN} \in \mathsf{AM}$ by Theorem A, by a protocol with perfect completeness. Polynomial-time many-one reductions preserve membership in AM and in coAM.

5.1. **Dimension.** Koiran proved that DIM is polynomial-time many-one reducible to HN, with no hypothesis [11, Theorem 5.8, p. 9]. His statement that $\mathsf{DIM} \in \mathsf{AM}$ under GRH [11, Theorem 4.1, p. 6] is deduced from $\mathsf{HN} \in \mathsf{AM}$ [9], and GRH enters nowhere else. Hence $\mathsf{DIM} \in \mathsf{AM}$.

5.2. **The parametric Nullstellensatz.** The proof of [1, Theorem 1] is a randomized polynomial-time reduction of HNP to HN: the parameters are replaced by integers chosen at random below an explicit bound, and Koiran's algorithm is run on the specialized system [1, §3.4, pp. 8–9]. The reduction and its analysis are algebraic. Of Koiran's algorithm the proof uses that it decides HN in AM with perfect completeness, and it uses the bound of [9, Theorem 7] on the degree of a solution, which does not depend on GRH. The class AM is closed under such reductions, as recalled there. Hence $\mathsf{HNP} \in \mathsf{AM}$.

5.3. **Vanishing of Schubert coefficients.** For each classical type $Y \in \{A, B, C, D\}$, Pak and Robichaux reduce the vanishing problem to HNP [20, Lemma 3.2 and proof of Theorem 3.4] and its complement to HNP [19, Lemma 1.9]; in both papers GRH is used only in the quoted theorem $\mathsf{HNP} \in \mathsf{AM}$ [20, Theorem 3.1], [19, Theorem 1.8]. With the previous subsection, the vanishing problem is in $\mathsf{AM} \cap \mathsf{coAM}$ for all four types. If it were NP-hard under polynomial-time many-one reductions, then $\mathsf{NP} \subseteq \mathsf{coAM}$, that is $\mathsf{coNP} \subseteq \mathsf{AM}$, and the polynomial hierarchy would collapse to Σ_2^{P} by the theorem of Boppana, Håstad and Zachos, quoted as [3, Theorem 2.3] in [20, p. 5]. If it were coNP-hard, again $\mathsf{coNP} \subseteq \mathsf{AM}$. This is [20, Corollary 1.4] without GRH.

5.4. **Circuits and homogeneous systems.** Let the polynomials f_i be given by arithmetic circuits with rational constants. Introduce a variable y_g for each gate g, with the equation $y_g = y_h + y_j$ or $y_g = y_h y_j$ for a sum or product gate with inputs h, j, the equation $by_g = a$ for a constant a/b, and $y_g = 0$ for each output gate. The new system is sparse, of degree at most two and of polynomial size, and its solutions are the solutions of the original system together with the values of the gates. For a homogeneous system in $x_1, \dots, x_t$, adjoin variables $u_1, \dots, u_t$ and the equation $\sum_i u_i x_i = 1$: the enlarged system has a solution exactly when the original one has a nonzero solution. Both are polynomial-time many-one reductions to HN. So both problems are in AM, which is [16, Theorem 2.10] without GRH.

5.5. **Homogeneous systems of parameters.** Let $Z \subseteq \mathbb{C}^t$ be the set of common zeros of homogeneous polynomials $f_1, \dots, f_k \in \mathbb{Q}[z_1, \dots, z_t]$ of positive degree, given by arithmetic circuits with rational constants; let N be the bit length of this description, with $t \le N$, and $d = \dim Z$.

Proposition 5.1. *The integer d and linear forms $L_1, \dots, L_d$ with integer coefficients of bit length polynomial in N, such that $Z \cap \{L_1 = \cdots = L_d = 0\} = \{0\}$, can be computed in polynomial time with an oracle in Σ_2^{P}. Such forms are a homogeneous system of parameters of the homogeneous coordinate ring of Z.*

Proof. For forms $\Lambda = (L_1, \dots, L_s)$ let $\mathrm{Good}(\Lambda)$ mean that the f_i and the L_r have no common zero other than 0. This is the complement of the homogeneous problem of the previous subsection, so it is in $\mathsf{coAM} \subseteq \Sigma_2^{\mathsf{P}}$. By the proof of [16, Theorem 3.4, pp. 27–28] there is a polynomial b such

that, when $d \geq 1$, some Λ with $s = d$ and integer coefficients of bit length at most $b(N)$ is good: a resultant of degree at most 2^{N^3} in the coefficients does not vanish identically, hence not at every point of a grid of that size. For $s < d$ no Λ is good, because each hyperplane lowers the dimension of a cone by at most one. So d is the least $s \in \{0, \ldots, t\}$ for which a good Λ with coefficients of bit length at most $b(N)$ exists. For a binary string w, the statement that such a good Λ exists whose encoding begins with w is again in Σ_2^{P}, since the choice of Λ merges with the leading existential quantifier. Asking it for $s = 0, 1, \ldots$ finds d, and then extending w one bit at a time finds Λ, in polynomially many queries. That a good Λ with $s = d$ is a homogeneous system of parameters is the graded form of Noether's normalization lemma, as in [16, Lemma 3.2 and proof of Theorem 3.4]. □

Mulmuley's theorem states this construction in the functional analogue of PH under GRH [16, Theorem 3.4]; the proof above is his, with the search written out so that the level can be read off.

6. What remains open

The half-plane theorems are the whole of the hypothesis, and they are unrefereed. For the theorem of Cureton and Thorner a Lean certificate is public, and a check of it would settle Corollary C. Koiran's question whether $\mathsf{HN} \in \mathsf{NP}$ is untouched: his Theorem 10 shows that the count of primes cannot give it [8, §6]. The method gives nothing in positive characteristic, where CH is the best bound known [2]. Other results that assume GRH in order to reduce complex data modulo small primes may yield in the same way; none beyond Corollary D has been examined here.

Note on method

The statement that a fixed zero-free half-plane suffices for Koiran's theorem, with its proof, was produced by GPT-6 Astra (ChatGPT Pro mode) and edited by GPT-6.2 Astra at reasoning effort ultra (Codex); it is Proposition 17.2 of [17]. The same model, GPT-6 Astra (ChatGPT Pro mode), produced the last two items of Corollary D under a hypothesis of GRH type. The derivation from Hu's corollary and the first three items of Corollary D were produced by Claude Opus 5.5 at effort max. That derivation and all five items were checked by Claude Opus 5.5 at effort high, which read Koiran's article, the half-plane preprints at their main statements and the reductions of [1] and [20] at the places where GRH enters. This text was written by Claude Fable 5.2 at effort max, which derived Sections 3 and 4 again, added the term for the leading coefficient and the explicit threshold, and read every source at the cited places, with these exceptions: [14], [3] and [13] were not opened and are cited as [6], [20] and [4] describe them. Claude Opus 5.5 at effort high then checked the text, recomputing every constant of Sections 3 and 4 and reading the sources at the cited places, with the same exceptions; it also found the papers [6] and [4], which Claude Fable 5.2 at effort max then read at the cited statements. No human has checked this note, and nothing in it is formalized. Our text is dedicated to the public domain under CC0 1.0. The records of the checks are kept at `https://github.com/KokunoYumeto/mathematics-workbenches`.

References

[1] R. Ait El Manssour, N. Balaji, K. Nosan, M. Shirmohammadi and J. Worrell, *A parametric version of the Hilbert Nullstellensatz*, Proc. 8th SOSA (2025), 444–451; arXiv:2408.13027v3, Theorem 1 (p. 3) and §3.4 (pp. 8–9).

[2] R. Andrews, A. Garg and É. Schost, *Hilbert's Nullstellensatz is in the counting hierarchy*, arXiv:2602.17904v1 (20 February 2026), §§1.1–1.2, Theorems 1.1, 1.3 and 1.4.

[3] R. B. Boppana, J. Håstad and S. Zachos, *Does co-NP have short interactive proofs?*, Inform. Process. Lett. **25** (1987), 127–132, Theorem 2.3.

[4] J. A. Baldwin and S. Sivek, *3-manifold decision problems and Riemann hypotheses*, arXiv:2611.06705v1 (4 November 2026), Theorem 1.1 (p. 1), Hypothesis 1.2 and Theorem 1.3 (p. 2), pp. 2–3, Remark 1.4 (p. 3), Theorem 2.1 (p. 4), Theorem 3.1 and Corollary 3.3 (p. 7), §5.

[5] D. Cureton and J. Thorner, *Report: A quasi-Riemann hypothesis for Dedekind zeta functions*, Hexagon, hexagon:2610.00200v2 (October 2026), abstract, Theorem 1.1 and Corollary 1.2 (p. 3), §15. https://hexagonmath.org/2610.00200v2.

[6] C. Frei, E. Sofos and M. Widmer, *Some applications of the quasi-Riemann hypothesis to class groups and small generators of number fields*, arXiv:2610.18491v2 (14 October 2026; first version 13 October 2026), Theorem 1.1 (p. 2).

[7] B. Hu, *A seven-eighths zero-free half-plane for unitary Weil L-functions*, Hexagon, hexagon:2610.00216v2 (13 October 2026), Theorems 1.1 and 1.2 (pp. 1–2), Corollary 9.6 (p. 56), "AI provenance" (p. 58). https://hexagonmath.org/2610.00216v2.

[8] P. Koiran, *Hilbert's Nullstellensatz is in the polynomial hierarchy*, J. Complexity **12** (1996), 273–286: Theorem 1 (p. 275), Theorem 2 (p. 276), Theorem 4 (p. 278), Theorem 5 (p. 279), Theorem 7 (p. 280), Lemma 3 and Theorem 8 (p. 281), Theorem 9 and Corollary 1 (p. 282), §6.

[9] P. Koiran, *Hilbert's Nullstellensatz is in the polynomial hierarchy*, DIMACS Technical Report 96-27 (July 1996), 18 pp.: abstract, Theorem 2 and its proof (pp. 5–6), Theorem 7 (p. 9). https://perso.ens-lyon.fr/pascal.koiran/Publis/DIMACS.96-27.ps.

[10] P. Koiran, *Erratum to "Hilbert's Nullstellensatz is in the polynomial hierarchy"*, 8 August 1997, 2 pp. https://perso.ens-lyon.fr/pascal.koiran/Publis/hn.erratum.ps.

[11] P. Koiran, *Randomized and deterministic algorithms for the dimension of algebraic varieties*, Proc. 38th FOCS (1997), 36–45; author's version, Theorem 4.1 (p. 6) and Theorem 5.8 (p. 9). https://perso.ens-lyon.fr/pascal.koiran/Publis/focs97.ps.

[12] G. Kuperberg, *Knottedness is in NP, modulo GRH*, Adv. Math. **256** (2014), 493–506; arXiv:1112.0845, Theorems 1.1 and 3.2.

[13] M. Lackenby, *The efficient certification of knottedness and Thurston norm*, Adv. Math. **387** (2021), Paper No. 107796; arXiv:1604.00290.

[14] J. C. Lagarias and A. M. Odlyzko, *Effective versions of the Chebotarev density theorem*, in Algebraic Number Fields (Durham, 1975), Academic Press, 1977, 409–464.

[15] B. Liu, *Mixed character moments and a zero-free half-plane for unitary Hecke L-functions*, Hexagon, hexagon:2611.00741v1 (20 November 2026), abstract and Theorem 7.21. https://hexagonmath.org/2611.00741v1.

[16] K. D. Mulmuley, *Geometric complexity theory V: Efficient algorithms for Noether normalization*, J. Amer. Math. Soc. **30** (2017), 225–309; arXiv:1209.5993v5, Theorem 2.10 (p. 25), Lemma 3.2 and Theorem 3.4 with its proof (pp. 27–28).

[17] *Constructing finite fields of prime degree from small cyclotomic cofactors and at fixed valuation, after Bach, von zur Gathen, Lenstra, and Pila*, Hexagon, hexagon:2611.00987v1 (24 November 2026), Table 1 (pp. 5–7) and §17, Proposition 17.2 (p. 59). https://hexagonmath.org/2611.00987v1.

[18] OpenAI, *Primitive roots for every admissible integer base*, preprint, 4 October 2026, Theorem 1.2.

[19] I. Pak and C. Robichaux, *Vanishing of Schubert coefficients*, arXiv:2412.02064v3 (2 April 2025), Theorem 1.4 (p. 5), Theorem 1.8 and Lemma 1.9 (§§1.7–1.8), Appendix C; extended abstract in Proc. 57th STOC (2025).

[20] I. Pak and C. Robichaux, *Vanishing of Schubert coefficients is in* $\mathsf{AM} \cap \mathsf{coAM}$ *assuming the GRH*, arXiv:2504.03004v1 (3 April 2025), Theorem 1.1 (p. 2), Question 1.2 and Corollary 1.4 (p. 5), Theorem 3.1 and Lemma 3.2 (p. 8), Theorem 3.4 (p. 11).

[21] J. M. Rojas, *Dedekind zeta functions and the complexity of Hilbert's Nullstellensatz*, arXiv:math/0301111v2 (14 January 2003), Theorem 1 (p. 2), the hypotheses DZH and GIPIT (p. 6).

[22] R. Zentner, *Integer homology* 3*-spheres admit irreducible representations in* $\mathrm{SL}(2,\mathbb{C})$, Duke Math. J. **167** (2018), no. 9, 1643–1712; arXiv:1605.08530v4, Theorem 11.2.