hexagon:2611.00471v1

UPPER AND LOWER BOUNDS FOR THE SCHUR–SIEGEL–SMYTH TRACE PROBLEM

TEJASVI SINGH TOMAR

Abstract. The Schur–Siegel–Smyth trace constant C_{86} is the lower limit of $\mathrm{tr}(\alpha)/\deg(\alpha)$ over totally positive algebraic integers α. We prove $1.8022225 < C_{86} < 1.8070809$. For the upper bound we exhibit a measure on $[0,6]$ that satisfies the hypotheses of Smith's theorem on limits of distributions of conjugates, which we check with the help of 21 integer polynomials. This improves the upper bounds 1.8216 of Orloski and Talebizadeh Sardari and 1.8117251 of Pinho. The lower bound comes from the method of Orloski, Talebizadeh Sardari and Smith with fifteen polynomials, three of them of degree 10 found by McKee and Smyth. It is larger than the bound 1.80220 reported by Giraudin, whose verification evaluates its bounds in floating-point arithmetic with fixed safety margins; ours encloses every rounding error. For each bound, two separately written programs check the certificate in ball arithmetic. Both bounds are also proved in Lean 4, the upper bound under the assumption of Smith's theorem, also in a version in which all checks on the certificates are carried out by Lean's kernel. We also give evidence that certificates of this kind cannot lower the upper bound much further without integer polynomials of high degree.

1. Introduction

An algebraic integer is totally positive if all of its conjugates are real and positive. The Schur–Siegel–Smyth trace constant is

$$C_{86} = \liminf_{\alpha} \frac{\mathrm{tr}(\alpha)}{\deg(\alpha)},$$

where α runs through the totally positive algebraic integers. In other words, C_{86} is the largest c such that for each $\varepsilon > 0$ only finitely many totally positive algebraic integers satisfy $\mathrm{tr}(\alpha) < (c-\varepsilon)\deg(\alpha)$. We follow the numbering of the repository [24]; the constant is denoted λ_{SSS} in [14]. For a prime $p \geq 3$, the number $4\cos^2(\pi/p)$ is a totally positive algebraic integer of degree $(p-1)/2$ and trace $p-2$, so $C_{86} \leq 2$. Schur proved $C_{86} \geq \sqrt{e} = 1.6487\ldots$ [20], and Siegel proved $C_{86} > 1.7336$ [21].

Smyth [23] introduced the auxiliary function method: if $x - \sum_Q \lambda_Q \log|Q(x)| \geq \lambda$ for all $x > 0$, where Q runs through a finite set of nonzero integer polynomials and $\lambda_Q \geq 0$, then $C_{86} \geq \lambda$. He proved $C_{86} \geq 1.7719$, and better choices of polynomials have since raised the bound to $1.793145\ldots$ [25]. Serre showed that the method cannot prove a bound larger than a constant $c_S = 1.898302\ldots$ [1], [13, Section 1]. Orloski, Talebizadeh Sardari and Smith [14] added the condition that limits of the uniform measures on the conjugates have nonnegative logarithmic energy, which comes from the integrality of discriminants, and proved $C_{86} \geq 1.80203$. In their proof [14, Corollary 1.9], the reference measure is given by floating-point data and several of the required inequalities are checked numerically. Giraudin [5] has recently reported $C_{86} \geq 1.80220$ in the same framework, with eighteen polynomials and a step reference density. His inequality is verified by two programs that bisect $[0,14]$ into about 1.7 million intervals, with bounds

2020 *Mathematics Subject Classification.* 11R06, 11R80; 31A15, 65G20, 90C05.

Key words and phrases. Totally positive algebraic integers, Schur–Siegel–Smyth trace problem, distributions of conjugates, logarithmic potential, auxiliary functions, ball arithmetic, computer-assisted proof.

evaluated in floating-point arithmetic; the energy of the reference measure is computed in double and extended precision and decreased by 10^{-12}, and a further 10^{-9} is subtracted from every bound.

Upper bounds come from measures. Smith [22, Theorem 1.5] proved that a probability measure μ on an interval of length greater than 4 is the weak limit of the uniform measures on the roots of a sequence of distinct monic irreducible integer polynomials whose roots lie in the interval, as soon as $\int \log|Q|\,d\mu \geq 0$ for every nonzero $Q \in \mathbb{Z}[x]$. Applied to a measure of Serre, this gives $C_{86} < 1.89831$ [22, Theorem 1.1 and Example 5.16], so $C_{86} < 2$. Orloski and Talebizadeh Sardari [13] constructed better measures, checking the infinitely many conditions with a finite set of polynomials, and proved $C_{86} \leq 1.8216$. Pinho [15] enlarged their set of four polynomials to eleven and obtained $C_{86} < 1.8117251$, with a certificate checked in exact rational and ball arithmetic. Qu and Yang [17] showed that C_{86} is also the limit of $\operatorname{tr}(\alpha)/\deg(\alpha)$ along a sequence of totally positive units.

Theorem 1.1.

$$\frac{901111277}{500000000} \leq C_{86} \leq \frac{81383685642728309283453}{45035996273705240000000}.$$

In particular $1.8022225 < C_{86} < 1.8070809$. *So all but finitely many totally positive algebraic integers* α *satisfy* $\operatorname{tr}(\alpha) > 1.8022225\deg(\alpha)$, *and infinitely many satisfy* $\operatorname{tr}(\alpha) < 1.8070809\deg(\alpha)$.

The two fractions are 1.802222554 and 1.8070808325…, so Theorem 1.1 places C_{86} in an interval of length less than 0.005. The upper bound is new. For it we use a measure μ on $[0,6]$ that is a mixture of a measure with a piecewise linear density and a small multiple of the equilibrium measure of $[0,6]$, together with 21 integer polynomials: the seven of [14], the four quintics added by Pinho, three polynomials of degree 10 found by McKee and Smyth [9] and used by Giraudin, and seven further polynomials of degrees 2 to 8 found by column generation (Table 1). Lemma 3.1 reduces the conditions of Smith's theorem to one inequality on $[0,6]$ and one integral inequality for each of the 21 polynomials, which two programs check in ball arithmetic [8, 4], in which every computed quantity is an interval guaranteed to contain the exact value.

The lower bound uses the irreducible factors of the polynomials of [5] and is larger than the bound 1.80220 reported there. It is larger than 1.8022211895…, the numerical infimum of the dual function of the certificate of [5] [5, Remark 2]; for the constraints used there, [5, Remark 3] reports a discrete ceiling of 1.8022246. What differs is the verification. The certificate consists of integer polynomials and rational numbers: the multipliers, the nodes and weights of a piecewise linear reference density, and λ. Lemma 2.1 reduces the lower bound to an inequality $F \geq 0$ on $(0,\infty)$, and two programs check this inequality in ball arithmetic. Since the reference density is piecewise linear, its potential and energy have closed forms (Lemma 2.3), and no numerical integration is needed. We also give a self-contained proof of Lemma 2.1 that does not assume that limit measures have compact support.

Both bounds of Theorem 1.1 are also proved in Lean 4 [11] with Mathlib [10] (Section 5): the lower bound without hypotheses, and the upper bound under one named hypothesis, Smith's Theorem 1.5 for intervals. The finite checks on the certificates are evaluated by compiled code in one version of these proofs and by Lean's kernel in another.

Section 2 proves the lower bound and Section 3 the upper bound. Section 4 describes the two certificates, how they were found, and the output of the programs. Section 5 describes the Lean proofs, and Section 6 discusses how far the two methods can go.

2. The lower bound

2.1. **Limit measures and the energy.** For a finite Borel measure ρ on $\mathbb{R}$ we write $U_\rho(x) = \int \log|x-y|\,d\rho(y)$ for its logarithmic potential, $I(\rho,\eta) = \int U_\eta\,d\rho$ and $I(\rho) = I(\rho,\rho)$ for its logarithmic energy, whenever the integrals exist. A signed measure σ has finite energy if $\iint |\log|x-y||\,d|\sigma|(x)\,d|\sigma|(y) < \infty$. With this sign convention, $I(\sigma) \le 0$ for every signed measure σ of total mass zero with finite energy (the argument is recalled in the proof of Lemma 2.1), so I is concave on probability measures of finite energy.

Let α be a totally positive algebraic integer of degree d with conjugates $\alpha_1,\dots,\alpha_d$, and let $\mu_\alpha = \frac{1}{d}\sum_j \delta_{\alpha_j}$ be the uniform probability measure on them. Then $\int x\,d\mu_\alpha = \operatorname{tr}(\alpha)/d$. Recall that C_{86} is the largest c such that for each $\varepsilon > 0$ only finitely many totally positive algebraic integers satisfy $\operatorname{tr}(\alpha) < (c-\varepsilon)\deg(\alpha)$.

Lemma 2.1. *Let $\mathcal{A}$ be a finite set of nonzero polynomials in $\mathbb{Z}[x]$, let $\lambda \in \mathbb{R}$, $\lambda_Q \ge 0$ for $Q \in \mathcal{A}$ and $\lambda_0 \ge 0$, and let ν be a compactly supported probability measure on $\mathbb{R}$ with a bounded density. Suppose that*

$$F(x) = x - \lambda - \sum_{Q\in\mathcal{A}} \lambda_Q \log|Q(x)| - \lambda_0\bigl(2U_\nu(x) - I(\nu)\bigr) \ge 0 \tag{2.1}$$

for every $x > 0$ that is not a root of a polynomial in $\mathcal{A}$. Then $C_{86} \ge \lambda$.

This is the dual form of the method of Orloski, Talebizadeh Sardari and Smith [14, Section 1.4] with a single reference measure ν, and for $\lambda_0 = 0$ it is Smyth's auxiliary function method [23]. The key input is that limits μ of the measures μ_α satisfy $I(\mu) \ge 0$. For compactly supported μ this also follows from a result of Smith [22, Proposition 5.7]: if $\int \log|Q|\,d\mu \ge 0$ for every nonzero $Q \in \mathbb{Z}[x]$, then $I(\mu) \ge 0$ in our sign convention. As said in the introduction, our proof of Lemma 2.1 is self-contained and does not assume that μ has compact support. It uses the discriminants of the minimal polynomials directly and truncates the logarithm near the diagonal.

Proof. Let $L = C_{86}$, so $L \le 2$. By the maximality of L, for every $\delta > 0$ infinitely many totally positive algebraic integers satisfy $\operatorname{tr}(\alpha) < (L+\delta)\deg(\alpha)$, and only finitely many satisfy $\operatorname{tr}(\alpha) < (L-\delta)\deg(\alpha)$. Hence we can choose distinct totally positive algebraic integers α_n of degrees d_n with $\operatorname{tr}(\alpha_n)/d_n \to L$. For each D, only finitely many totally positive algebraic integers have degree at most D and trace at most $3D$, because their conjugates lie in $(0,3D]$ and the coefficients of their minimal polynomials are bounded integers. Hence $d_n \to \infty$. We discard the finitely many α_n that are roots of polynomials in $\mathcal{A}$, and finitely many more so that $\int x\,d\mu_n \le L+1$ for all n, where $\mu_n = \mu_{\alpha_n}$.

Arithmetic input. Let P_n be the minimal polynomial of α_n. For $Q \in \mathcal{A}$, the product $\prod_j Q(\alpha_{n,j}) = \pm\operatorname{Res}(P_n,Q)$ is a nonzero integer, so $\int \log|Q|\,d\mu_n \ge 0$. The discriminant $\prod_{i\ne j}(\alpha_{n,i}-\alpha_{n,j})$ of P_n is a nonzero integer up to sign, so

$$\frac{1}{d_n^2}\sum_{i\ne j} \log|\alpha_{n,i}-\alpha_{n,j}| \ge 0. \tag{2.2}$$

Limit and integrability. By Markov's inequality $\mu_n((R,\infty)) \le (L+1)/R$, so the sequence is tight. After passing to a subsequence, μ_n converges weakly to a probability measure μ on $[0,\infty)$, and $\int x\,d\mu \le L$ because x is continuous and nonnegative. For $R \ge e$ and $x \ge R$ we have $\log(1+x) \le 2(\log R/R)\,x$, so

$$\sup_n \int_{x>R} \log(1+x)\,d\mu_n \le \frac{2(L+1)\log R}{R} \to 0 \qquad (R\to\infty).$$

Therefore $\int \varphi\, d\mu_n \to \int \varphi\, d\mu$ for every continuous φ on $[0,\infty)$ with $|\varphi(x)| \le c(1+\log(1+x))$, and the same holds for continuous ψ on $[0,\infty)^2$ with $|\psi(x,y)| \le c(1+\log(1+x)+\log(1+y))$ and the product measures $\mu_n \times \mu_n \to \mu \times \mu$.

The constraints pass to the limit. Fix $Q \in \mathcal{A}$ and $M > 0$, and let $\varphi_M = \max(\log|Q|, -M)$. This function is continuous, $\varphi_M \ge \log|Q|$, and $|\varphi_M(x)| \le M + c_Q(1+\log(1+x))$. Hence $\int \varphi_M\, d\mu = \lim_n \int \varphi_M\, d\mu_n \ge \limsup_n \int \log|Q|\, d\mu_n \ge 0$. As $M \to \infty$, φ_M decreases to $\log|Q|$, and $\varphi_0 = \max(\log|Q|, 0) \le c_Q(1+\log(1+x))$ is μ-integrable, so monotone convergence gives $\int \log|Q|\, d\mu \ge 0$. Similarly, let $\psi_M(x,y) = \max(\log|x-y|, -M)$, which is continuous with $|\psi_M| \le M + \log(1+x) + \log(1+y)$. The diagonal terms of $\sum_{i,j} \psi_M(\alpha_{n,i}, \alpha_{n,j})$ equal $-M$, so (2.2) gives

$$0 \le \frac{1}{d_n^2} \sum_{i \ne j} \log|\alpha_{n,i} - \alpha_{n,j}| \le \iint \psi_M\, d\mu_n\, d\mu_n + \frac{M}{d_n}.$$

Letting $n \to \infty$ gives $\iint \psi_M\, d\mu\, d\mu \ge 0$. As $M \to \infty$, ψ_M decreases to $\log|x-y|$, and $\psi_0 \le \log(1+x)+\log(1+y)$ is $\mu\times\mu$-integrable, so monotone convergence gives $I(\mu) \ge 0$. In particular $I(\mu)$ is finite, $\iint |\log|x-y||\, d\mu\, d\mu < \infty$, and μ has no atoms.

Energy inequality. We claim that $I(\mu) \le 2I(\mu,\nu) - I(\nu)$. Let $\sigma = \mu - \nu$, a signed measure of total mass zero. For $r > 0$ we have $-\log r = \frac{1}{2}\int_0^\infty (e^{-sr^2} - e^{-s})\, \frac{ds}{s}$, and the integrand has constant sign, so $\int_0^\infty |e^{-sr^2} - e^{-s}|\, \frac{ds}{s} = 2|\log r|$. The double integral $\iint |\log|x-y||\, d|\sigma|\, d|\sigma|$ is finite: for $\mu\times\mu$ by the previous step, and for $\nu\times\nu$ and $\mu\times\nu$ because ν has compact support and a bounded density w, so that $\int \log^-|x-y|\, d\nu(y) \le 2\|w\|_\infty$, while $\log^+|x-y| \le \log(1+|x|) + \log(1+|y|)$ and $\int \log(1+x)\, d\mu \le \log(1+L)$ by Jensen's inequality. In particular the diagonal $\{x=y\}$ is $|\sigma|\times|\sigma|$-null. Fubini's theorem therefore gives

$$-I(\sigma) = \frac{1}{2}\int_0^\infty \Big(\iint e^{-s|x-y|^2}\, d\sigma(x)\, d\sigma(y) \Big) \frac{ds}{s} \ge 0,$$

since $\sigma(\mathbb{R}) = 0$ and the Gaussian kernel is positive definite. By bilinearity, $I(\sigma) = I(\mu) - 2I(\mu,\nu) + I(\nu)$, which proves the claim.

Conclusion. Since μ has no atoms, the finitely many roots of the polynomials in $\mathcal{A}$ and the point 0 are μ-null, so $F \ge 0$ holds μ-almost everywhere. Each term of F is μ-integrable, so integrating gives

$$L \ge \int x\, d\mu \ge \lambda + \sum_Q \lambda_Q \int \log|Q|\, d\mu + \lambda_0\big(2I(\mu,\nu) - I(\nu)\big) \ge \lambda + \lambda_0 I(\mu) \ge \lambda. \qquad \square$$

Remark 2.2. Only $Q(\alpha) \ne 0$ is used, so the polynomials in $\mathcal{A}$ need not be irreducible or have real roots. The measure ν can be any compactly supported probability measure with a bounded density: in particular, $I(\nu) \ge 0$ is not needed, and ν need not satisfy the constraints $\int \log|Q|\, d\nu \ge 0$.

2.2. **Piecewise linear reference densities.** We take for ν a continuous piecewise linear density. Let $e_0 < e_1 < \cdots < e_N$ be rational nodes and, for $1 \le k \le N-1$, let h_k be the hat function on $[e_{k-1}, e_{k+1}]$ with peak at e_k, normalized to $\int h_k = 1$. For nonnegative weights $\rho_1, \ldots, \rho_{N-1}$ with $s = \sum_k \rho_k > 0$, let $g = \sum_k \rho_k h_k$ and $\nu = g/s$. With $\lambda_0 = s$, the function (2.1) becomes

$$F(x) = x - \lambda - \sum_Q \lambda_Q \log|Q(x)| - 2U_g(x) + \frac{I(g)}{s}. \tag{2.3}$$

The second derivative of g in the sense of distributions is $g'' = \sum_i C_i \delta_{e_i}$, with rational coefficients C_i determined by the slopes of g, and $\sum_i C_i = \sum_i C_i e_i = 0$ because g vanishes outside $[e_0, e_N]$.

Lemma 2.3. *Let* $H(t) = \frac{t^2}{2}\log|t| - \frac{3}{4}t^2$ *and* $J(t) = \frac{t^4}{24}\log|t| - \frac{25}{288}t^4$, *with* $H(0) = J(0) = 0$. *Then*

$$U_g(x) = \sum_i C_i H(e_i - x), \qquad I(g) = \sum_{i,j} C_i C_j J(e_i - e_j).$$

Proof. A direct computation gives $H''(t) = \log|t|$ and $J'' = H$, so $J''''(t) = \log|t|$. The functions H and J are even, H is C^1 and J is C^3. Since g is Lipschitz with compact support, two integrations by parts give $\int \log|x-y|\, g(y)\, dy = \int H''(y-x)g(y)\, dy = \int H(y-x)\, dg''(y)$, with vanishing boundary terms. This is the first formula. For the second we integrate by parts twice in each variable. □

Lemma 2.3 reduces F and $I(g)$ to finitely many elementary terms with exact rational arguments $e_i - x$ at rational points x. The same formulas give $F''(x) = \sum_Q \lambda_Q \frac{Q'(x)^2 - Q(x)Q''(x)}{Q(x)^2} - 2\sum_i C_i \log|e_i - x|$ away from the nodes and the roots.

2.3. **Verification.** We verify (2.3) for a certificate consisting of the polynomials $Q \in \mathcal{A}$, rational multipliers λ_Q, rational nodes and weights, a rational λ, and two rational cut points $0 < x_{\mathrm{lo}} < x_{\mathrm{hi}}$. All quantities are rebuilt from these data. The verification splits $(0,\infty)$ into $(0, x_{\mathrm{lo}}]$, $[x_{\mathrm{lo}}, x_{\mathrm{hi}}]$ and $[x_{\mathrm{hi}}, \infty)$. Every quantity on which the conclusion depends is computed exactly in rational arithmetic or enclosed in a real ball of Arb [8], that is, an interval given by a midpoint and a radius that is guaranteed to contain the exact value. Floating-point numbers are used only to guess where the roots lie and how to split the range.

The tails. Assume that $0 < x_{\mathrm{lo}} \le \min(\operatorname{supp} g)$, and let λ_x be the multiplier of the polynomial x (zero if $x \notin \mathcal{A}$). Since U_g is decreasing on $(-\infty, \min(\operatorname{supp} g)]$, for $0 < x \le x_{\mathrm{lo}}$ we have

$$F(x) \ge -\lambda - \lambda_x \log x_{\mathrm{lo}} - \sum_{Q \ne x} \lambda_Q \log M_Q - 2U_g(0) + \frac{I(g)}{s},$$

where M_Q is an upper bound for $|Q|$ on $[0, x_{\mathrm{lo}}]$, and we check that the right side is positive. The term $-\lambda_x \log x_{\mathrm{lo}}$ makes it positive when $\lambda_x > 0$ and x_{lo} is small. On the right, assume that the support of g lies in $[0, x_{\mathrm{hi}}]$ and $x_{\mathrm{hi}} \ge 1$. For $x \ge x_{\mathrm{hi}}$ we have $|Q(x)| \le \|Q\|_1 x^{\deg Q}$, where $\|Q\|_1$ is the sum of the absolute values of the coefficients, and $U_g(x) \le s \log x$, because $0 < x - y \le x$ for y in the support of g. Hence $F(x) \ge x - a\log x - b$ with $a = 2s + \sum_Q \lambda_Q \deg Q$ and $b = \lambda - I(g)/s + \sum_Q \lambda_Q \log\|Q\|_1$. If $x_{\mathrm{hi}} \ge a$, the right side increases on $[x_{\mathrm{hi}}, \infty)$, and we check that it is positive at x_{hi}.

The middle range. Around each real root in $(x_{\mathrm{lo}}, x_{\mathrm{hi}})$ of a polynomial $Q \in \mathcal{A}$ with $\lambda_Q > 0$ we choose a window: an interval W with rational endpoints on which a single ball evaluation of F, with each $\log|Q|$ replaced by the logarithm of an upper bound for $|Q|$ on W, gives a positive lower bound. This bound is valid on all of W, roots included. If the ball contains a node e_i, the term $H(e_i - x)$ is enclosed by $|H(t)| \le r^2(\frac{1}{2}\log\frac{1}{r} + \frac{3}{4})$ for $|t| \le r < 0.6$, which holds because $t^2\log(1/t)$ is increasing on $[0, e^{-1/2}]$. The nodes and the window ends cut the rest of $[x_{\mathrm{lo}}, x_{\mathrm{hi}}]$ into intervals on which F is smooth, except for logarithmic singularities of F'' at nodes that are endpoints of the interval. On each such interval we use the bound below, and we bisect the interval when it does not give a positive lower bound. The correctness of the result does not depend on how the roots were located: on an interval that contains a root of some Q with $\lambda_Q > 0$, the ball enclosure of F'' described below is not finite, so the interval is never accepted.

Lemma 2.4. *Let f be continuously differentiable on $[p,q]$ with f' absolutely continuous, and let $\Delta = q-p$. Then for $p \le x \le q$,*

$$f(x) \ge \min\big(f(p), f(q)\big) - \frac{\Delta}{4}\int_p^q \big(f''(t)\big)_+\, dt.$$

Proof. Let ℓ be the linear function with $\ell(p) = f(p)$ and $\ell(q) = f(q)$. Then $f(x) = \ell(x) - \int_p^q G(x,t) f''(t)\, dt$, where $G(x,t) = (t-p)(q-x)/\Delta$ for $t \le x$ and $G(x,t) = (x-p)(q-t)/\Delta$ for $t \ge x$. Since $0 \le G \le \Delta/4$, the integral is at most $\frac{\Delta}{4}\int_p^q (f'')_+$, and $\ell(x) \ge \min(f(p), f(q))$. □

We evaluate $F(p)$ and $F(q)$ with $Q(p)$, $Q(q)$ and the differences $e_i - p$, $e_i - q$ computed exactly. Write $F'' = R + S$, where S is the sum of the terms $-2C_i \log|e_i - x|$ over the nodes $e_i \in \{p, q\}$. Since $(R+S)_+ \le R_+ + \sum(-2C_i \log|e_i - x|)_+$, we have

$$\int_p^q (F'')_+ \le \Delta\, \bar{R}_+ + \sum_{e_i \in \{p,q\}} \int_0^{\Delta} \big(-2C_i \log t\big)_+\, dt,$$

where $\bar{R}$ is an upper bound for R on $[p,q]$ obtained by a single ball evaluation on a ball that contains $[p,q]$. With $m = \min(\Delta, 1)$, the last integral equals $2C_i m(1 - \log m)$ if $C_i > 0$, equals $2|C_i|(\Delta \log \Delta - \Delta + 1)$ if $C_i < 0$ and $\Delta > 1$, and vanishes otherwise. Alternatively, a term with $C_i < 0$ can be bounded on $[p,q]$ by $2|C_i| \log \Delta$ and added to $\bar{R}$.

Implementation. Two programs carry out this procedure. They were written separately, share no code apart from the ball arithmetic library [4], and rebuild every quantity from the certificate. Since they implement the same method, their agreement does not test the method itself, which is proved above. It tests the implementations, in particular of the potential, the energy and the root location, which the two programs compute in different ways. The first computes the coefficients C_i and evaluates U_g and $I(g)$ by Lemma 2.3, with 200-bit balls. It brackets the real roots by floating-point approximations confirmed by exact sign changes, and confirms their number with a Sturm sequence. On an interval it encloses each Q and its first two derivatives through their exact Taylor coefficients at the rational midpoint, because Horner's scheme on balls overestimates polynomials of degree 10 with large coefficients too much. When a node with $C_i > 0$ is an endpoint, it accepts the interval only if $\Delta \le 1$, where the integral above equals $2C_i\Delta(1 - \log\Delta)$; for the terms with $C_i < 0$ at an endpoint it uses the alternative bound $2|C_i| \log \Delta$. The second uses the coefficients C_i only for F'', and recomputes them from the values of g at the nodes. It writes $g(y) = a + by$ on each piece $[e_k, e_{k+1}]$ and computes U_g from the primitive

$$\int (a+by) \log|x-y|\, dy = (a+bx)\, G_1(y-x) + b\, G_2(y-x),$$

where $G_1(t) = t\log|t| - t$ and $G_2(t) = \frac{t^2}{2}\log|t| - \frac{t^2}{4}$; on balls around 0 it uses $|G_1(t)| \le r\log\frac{1}{r} + r$ for $|t| \le r < 0.36$ and $|G_2(t)| \le \frac{r^2}{2}\log\frac{1}{r} + \frac{r^2}{4}$ for $|t| \le r < 0.6$. It computes $I(g)$ from closed-form primitives of $t^n \log|t|$ over pairs of pieces, and it works with 256-bit balls. It encloses all complex roots of each Q, and requires every root whose enclosure meets the real line to be simple and to have a bracket with an exact sign change, the brackets being disjoint; it then narrows each bracket by exact bisection to width at most 2^{-110}. On an interval I it bounds the part of F'' that comes from Q through the roots, by $-(\log|Q|)'' = \sum_\rho \mathrm{Re}(x-\rho)^{-2} \le \sum_\rho \mathrm{dist}(\rho, I)^{-2}$, and it bounds $|Q|$ on I by $|a_Q| \prod_\rho \max_{x\in I}|x-\rho|$, so that no polynomial is evaluated on a wide ball.

3. The upper bound

3.1. **A criterion.** As in Section 2, $U_\mu(z) = \int \log|z-y|\,d\mu(y)$ denotes the logarithmic potential of a finite Borel measure μ on $\mathbb{R}$, now for $z \in \mathbb{C}$.

Lemma 3.1. *Let $X > 4$, and let μ be a Borel probability measure on $[0, X]$ whose potential U_μ is finite and continuous on $\mathbb{C}$. Let $\mathcal{B}$ be a finite set of primitive polynomials in $\mathbb{Z}[x]$ of positive degree, irreducible over $\mathbb{Q}$, no two of which differ only in sign, and let $b_Q > 0$ for $Q \in \mathcal{B}$, with $\beta = \sum_Q b_Q \deg Q < 1$. Suppose that*

- (U1) *$h(x) = U_\mu(x) - \sum_{Q\in\mathcal{B}} b_Q \log|Q(x)| \geq 0$ for every $x \in \operatorname{supp}\mu$ that is not a root of a polynomial in $\mathcal{B}$, and*
- (U2) *$\int \log|Q|\,d\mu \geq 0$ for every $Q \in \mathcal{B}$.*

Then $\int \log|P|\,d\mu \geq 0$ for every nonzero $P \in \mathbb{Z}[x]$, and $C_{86} \leq \int x\,d\mu$.

Proof. Since U_μ is finite, μ has no atoms, and for a polynomial P with leading coefficient a and roots $\rho_1, \dots, \rho_d$ the function $\log|P(x)| = \log|a| + \sum_k \log|x-\rho_k|$ is μ-integrable, with

$$\int \log|P|\,d\mu = \log|a| + \sum_k U_\mu(\rho_k). \tag{3.1}$$

Step 1: $h(z) \geq 0$ for every $z \in \mathbb{C}$ that is not a root of a polynomial in $\mathcal{B}$. Define $h(z)$ for $z \in \mathbb{C}$ by the formula in (U1), with the value $+\infty$ at the roots. Since U_μ is continuous and $b_Q > 0$, the function $h\colon \mathbb{C} \to (-\infty, \infty]$ is lower semicontinuous, and it is superharmonic on $D = \mathbb{C} \setminus \operatorname{supp}\mu$, where U_μ is harmonic. As $|z| \to \infty$ we have $h(z) = (1-\beta)\log|z| - \sum_Q b_Q \log|a_Q| + o(1) \to \infty$, where a_Q is the leading coefficient of Q. Choose $R > X$ such that $h > 0$ on $\{|z| \geq R\}$, and let $D_R = D \cap \{|z| < R\}$, which is connected because it is a disc from which a compact subset of a diameter has been removed. At a point $\zeta \in \operatorname{supp}\mu$ we have $\liminf_{z\to\zeta} h(z) \geq h(\zeta) \geq 0$, by lower semicontinuity and (U1), and on the circle $|z| = R$ we have $h > 0$. The maximum principle for the subharmonic function $-h$ on the bounded domain D_R [18, Theorem 2.3.1] therefore gives $h \geq 0$ on D_R, and hence on $\mathbb{C}$.

Step 2: $\int \log|P|\,d\mu \geq 0$ for every nonzero $P \in \mathbb{Z}[x]$. The integral is additive in P, and a nonzero integer c contributes $\log|c| \geq 0$, so it suffices to consider P primitive, irreducible over $\mathbb{Q}$ and of degree $d \geq 1$. If $P = \pm Q$ with $Q \in \mathcal{B}$, we use (U2). Otherwise P has no common root with any $Q \in \mathcal{B}$, because both are primitive and irreducible and $P \neq \pm Q$. Let a be the leading coefficient of P and $\rho_1, \dots, \rho_d$ its roots. For $Q \in \mathcal{B}$, the resultant $\operatorname{Res}(P, Q) = a^{\deg Q} \prod_k Q(\rho_k)$ is a nonzero integer, so $\sum_k \log|Q(\rho_k)| \geq -\deg Q \log|a|$. By Step 1, $U_\mu(\rho_k) \geq \sum_Q b_Q \log|Q(\rho_k)|$, and summing over k in (3.1) gives

$$\int \log|P|\,d\mu \geq \log|a| - \sum_{Q\in\mathcal{B}} b_Q \deg Q\, \log|a| = (1-\beta)\log|a| \geq 0.$$

Step 3: the sequence. The interval $[0, X]$ has logarithmic capacity $X/4 > 1$ [19, Example I.3.5]. By Step 2 and [22, Theorem 1.5], there are distinct monic irreducible polynomials $R_1, R_2, \dots \in \mathbb{Z}[x]$ with all roots in $[0, X]$ whose root distributions $\frac{1}{\deg R_k} \sum_{R_k(\rho)=0} \delta_\rho$ converge weakly to μ. At most one R_k equals x, and the roots of every other R_k lie in $(0, X]$, so R_k is the minimal polynomial of a totally positive algebraic integer α_k, and these α_k are distinct. Since x is continuous on $[0, X]$, $\operatorname{tr}(\alpha_k)/\deg(\alpha_k) = \int x\,d\mu_{R_k} \to \int x\,d\mu$, where μ_{R_k} is the root distribution of R_k. So for every $\varepsilon > 0$ infinitely many totally positive algebraic integers satisfy $\operatorname{tr}(\alpha) < (\int x\,d\mu + \varepsilon)\deg(\alpha)$, and $C_{86} \leq \int x\,d\mu$. □

Smith states the condition of his theorem as $\int \log|Q|\,d\mu \geq 0$ for every nonzero $Q \in \mathbb{Z}[x]$, where $\log 0 = -\infty$, so that the condition fails when μ charges a root of Q; here μ has no atoms.

Step 2 is the argument of [22, Proposition 5.15], whose hypothesis is that $h \geq 0$ on all of $\mathbb{C}$ (Smith writes the potential with the opposite sign). Step 1 reduces this hypothesis to the support of μ, so no estimates outside $[0, X]$ are needed; it uses $\beta < 1$, which makes h tend to ∞ at infinity. Bounds of this kind were first obtained in [22, Example 5.16] and [13], and Pinho's certificate checks the same conditions [15].

3.2. **The measure.** We take $X = 6$ and

$$\mu = (1-\varepsilon)\mu_0 + \varepsilon\omega, \qquad \varepsilon = 1/100000,$$

where ω is the equilibrium measure of $[0, 6]$ and $\mu_0 = G(x)\,dx$ has a continuous piecewise linear density as in Section 2.2: for rational nodes $0 = e_0 < e_1 < \cdots < e_N = 6$ and rational weights $w_k \geq 0$ with $\sum_k w_k = 1$, we put $G = \sum_{k=1}^{N-1} w_k h_k$, where h_k is the hat function on $[e_{k-1}, e_{k+1}]$ with peak at e_k and $\int h_k = 1$. By Lemma 2.3, $U_{\mu_0}(x) = \sum_i C_i H(e_i - x)$, where the C_i are the jumps of the slope of G. The measure ω has density $1/(\pi\sqrt{x(6-x)})$ on $(0, 6)$, and with $t = (z-3)/3$,

$$U_\omega(z) = \log\frac{3}{2} + \log\bigl|t + \sqrt{t^2-1}\bigr|,$$

where the branch of the square root is chosen so that $|t + \sqrt{t^2-1}| \geq 1$ [19, Example I.3.5 and (I.4.4)]. So U_ω is continuous on $\mathbb{C}$, $U_\omega = \log\frac{3}{2}$ on $[0, 6]$, and $U_\omega \geq \log\frac{3}{2}$ everywhere. The potential U_{μ_0} is continuous because G is bounded and has compact support, so U_μ is continuous, and $\operatorname{supp}\mu = [0, 6]$.

The certificate gives the polynomials $Q \in \mathcal{B}$, which are monic, and rational numbers $b_Q > 0$. We apply Lemma 3.1 with the weights $(1-\varepsilon)b_Q$. The conditions become

$$\beta = (1-\varepsilon)\sum_Q b_Q \deg Q < 1, \tag{3.2}$$

$$(1-\varepsilon)\Bigl(U_{\mu_0}(x) - \sum_Q b_Q \log|Q(x)|\Bigr) + \varepsilon\log\frac{3}{2} \geq 0 \qquad (0 \leq x \leq 6), \tag{3.3}$$

$$\int \log|Q|\,d\mu = (1-\varepsilon)\sum_{Q(\rho)=0} U_{\mu_0}(\rho) + \varepsilon\sum_{Q(\rho)=0} U_\omega(\rho) \geq 0 \qquad (Q \in \mathcal{B}), \tag{3.4}$$

and the bound is $\int x\,d\mu = (1-\varepsilon)\sum_k w_k \frac{e_{k-1}+e_k+e_{k+1}}{3} + 3\varepsilon$. Since $U_\omega \geq \log\frac{3}{2}$, condition (3.4) follows from

$$(1-\varepsilon)\sum_{Q(\rho)=0} U_{\mu_0}(\rho) + \varepsilon\deg Q\log\frac{3}{2} \geq 0.$$

So the admixture of ω adds $\varepsilon\log\frac{3}{2}$ to the left side of (3.3) and $\varepsilon\deg Q\log\frac{3}{2}$ to the integrals in (3.4), and raises the bound by $\varepsilon(3 - \int x\,d\mu_0)$. It absorbs the small negative values that the measure μ_0 found by linear programming has after rounding (Section 4.2).

3.3. **Verification.** Two programs check (3.2), (3.3) and (3.4), and compute $\int x\,d\mu$ exactly. Both check in exact arithmetic that the weights are nonnegative and sum to 1, that the nodes increase and lie in $[0, 6]$, that $b_Q \geq 0$, and that the polynomials are distinct, primitive and irreducible (by factorization in FLINT [4]) with only real roots; and both check (3.2) exactly. All other quantities are enclosed in balls.

The first program brackets the real roots of each Q by rational intervals of width at most 2^{-110}, confirmed by exact sign changes and counted with a Sturm sequence, and evaluates (3.4) with U_{μ_0} on these brackets. For (3.3) it proceeds as in Section 2.3: around each root of a polynomial $Q \in \mathcal{B}$ it chooses a window on which one ball evaluation gives a positive lower bound, with $\log|Q|$ replaced by the logarithm of an upper bound for $|Q|$, and on the intervals

between the nodes and the window ends it applies Lemma 2.4 to the left side of (3.3), bisecting where the bound is not positive. The upper bound for the second derivative on an interval $[p, q]$ adds the polynomial part $\sum_Q b_Q(Q'^2 - QQ'')/Q^2$, evaluated with exact Taylor coefficients at the midpoint, to bounds for the terms $C_i \log|e_i - x|$ of U''_{μ_0}: an integral bound for a node at an endpoint, the supremum for the other nodes near the interval, and a Taylor bound at the midpoint for distant nodes.

The second program was written independently of the first, from Lemma 3.1 and the certificate format only, and shares no code with it apart from FLINT. It computes U_{μ_0} and U'_{μ_0} on each piece from the antiderivatives of $(a + b\,t)\log|t|$, encloses the roots with FLINT, and proves (3.3) on each interval between consecutive breakpoints (the nodes, the rational roots, and windows of width at most 2^{-110} around the irrational roots) by a second-order Taylor bound at the midpoint, in which the regular part of the second derivative is bounded on the interval and the logarithmic singularity of a node at an endpoint is integrated; it bisects on failure. On each window it bounds the left side of (3.3) from below by one ball evaluation, with $\log|x - \theta|$ for the root θ replaced by the logarithm of the width of the window. The two programs compute the potential, the root enclosures and the positivity bounds in different ways.

4. The certificates

Table 1 lists the polynomials of both certificates. The first seven are those of [14, Corollary 1.9]. Pinho [15] added the two quartics and the next five polynomials to the four polynomials x, $x - 1$, $x^2 - 3x + 1$ and $x^3 - 5x^2 + 6x - 1$ of [13]; the polynomial $x - 2$ is not in his set. All polynomials in the table are monic, irreducible and have only real roots, which lie in $[0, 6)$.

4.1. **The lower bound.** The reference density has 10,386 nodes in $[0.0488, 5.3520]$, chosen by the collocation method described below. The weights ρ_k are multiples of 2^{-48}, and 10,237 of the 10,384 weights are nonzero. The support of g lies in the same interval, $s = 0.535256$ and $I(\nu) = I(g)/s^2 = -2.75 \cdot 10^{-6}$; by Remark 2.2, Lemma 2.1 does not require $I(\nu) \geq 0$. Finally, $\lambda = 901111277/500000000$, $x_{\mathrm{lo}} = 1/100$ and $x_{\mathrm{hi}} = 30$. All fifteen polynomials have positive multipliers, but $x^3 - 6x^2 + 9x - 1$, whose multiplier is about $2.5 \cdot 10^{-7}$, is not needed: both programs also accept the certificate without it (Table 2).

Three earlier certificates are also in the accompanying repository: one found by the same method with 6,173 nodes and $\lambda = 63361515736283/35157522000000 > 1.8022179$; one with the same fifteen polynomials, 2,683 nodes and $\lambda = 901101631/500000000 = 1.802203262$, and one with the twelve polynomials of Table 1 other than those of degree 10, 1,753 nodes and $\lambda = 185185220/102755699 > 1.8021892$. Both programs accept them.

How it was found. The search plays no role in the proof. The reference density was found by collocation. Its support is a union of 66 intervals, obtained from the support of an approximate solution with 4,149 hats and split at every root of a polynomial with positive multiplier. Each interval carries at least 60 nodes, spaced like Chebyshev–Lobatto points, and the hats centred at the ends of the intervals carry no mass. For fixed intervals, the conditions $F = 0$ at the hat centres, $\int \log|Q|\,d\nu = 0$ for the polynomials with positive multiplier, and $I(\nu) = 0$ form a linear system in the weights and the multipliers together with one quadratic equation, which we solved directly. The ends of the intervals were moved 26 times, until every weight was nonnegative and no end moved. With ν fixed, a linear program on about $3.3 \cdot 10^5$ points re-optimised the multipliers and gave $\lambda = 1.802219008$, with minimum $-4.6 \cdot 10^{-8}$ of F on these points. Starting from this solution, we then gave every interval on which F fell below -10^{-6} between nodes 30% more nodes and solved again. After seven such rounds the measure had 10,254 hats and F fell at most $1.3 \cdot 10^{-6}$ below zero between nodes; 17 negative weights were set to 0, so that $I(\nu)$ is

TABLE 1. The polynomials of the two certificates with their weights, rounded to ten decimal places: the multipliers λ_Q of the lower-bound certificate of Theorem 1.1, which are multiples of 2^{-48}, and the weights b_Q of the upper-bound certificate, which are multiples of 2^{-44}. A dash means that Q is not in the certificate. The three polynomials of degree 10 are from [9].

Q	λ_Q	b_Q
x	0.5034276784	0.0585032675
$x-1$	0.4379921423	0.0491080836
$x-2$	0.0423886965	0.0333960240
x^2-3x+1	0.1563506267	0.0221368799
x^3-5x^2+6x-1	0.0581548388	0.0226234061
$x^4-7x^3+13x^2-7x+1$	0.0172965782	0.0114475294
$x^4-7x^3+14x^2-8x+1$	0.0176047286	0.0125654815
$x^5-9x^4+28x^3-35x^2+15x-1$	0.0023197148	0.0069739625
$x^5-9x^4+26x^3-29x^2+11x-1$	0.0006606314	0.0088863765
$x^5-9x^4+27x^3-32x^2+13x-1$	0.0003887454	0.0039245213
$x^5-9x^4+27x^3-31x^2+12x-1$	0.0025850757	0.0080087411
x^3-6x^2+9x-1	0.0000002526	–
$x^{10}-18x^9+134x^8-537x^7+1265x^6-1798x^5+1526x^4-743x^3+194x^2-24x+1$	0.0003929732	0.0057035573
$x^{10}-18x^9+135x^8-549x^7+1320x^6-1920x^5+1662x^4-813x^3+206x^2-24x+1$	0.0003957846	0.0055010705
$x^{10}-18x^9+134x^8-538x^7+1273x^6-1822x^5+1560x^4-766x^3+200x^2-24x+1$	0.0004134755	0.0054838227
$x^8-15x^7+90x^6-277x^5+467x^4-428x^3+200x^2-42x+3$	–	0.0054037982
$x^8-15x^7+89x^6-269x^5+445x^4-402x^3+187x^2-40x+3$	–	0.0047710666
$x^7-13x^6+63x^5-143x^4+157x^3-78x^2+16x-1$	–	0.0049122996
x^2-4x+2	–	0.0129514327
x^2-4x+1	–	0.0131738152
$x^6-11x^5+43x^4-72x^3+51x^2-14x+1$	–	0.0067676993
x^3-6x^2+9x-3	–	0.0066472539

no longer 0. The linear program for the multipliers then gave $\lambda = 1.802223655$, with minimum $-6.4 \cdot 10^{-8}$ of F on its points. We rounded the weights to multiples of 2^{-48} and took λ smaller by $1.1 \cdot 10^{-6}$.

Output of the two programs. Both accept the certificate. Their enclosures of $s^2 I(\nu)$ agree to all 38 digits that the first program prints. The lower bound on the left tail is 0.4867. On the right tail, $a = 2.7229$ and $x_{\mathrm{hi}} - a \log x_{\mathrm{hi}} - b = 18.03$. The polynomials with $\lambda_Q > 0$ have 68 real roots in $[x_{\mathrm{lo}}, x_{\mathrm{hi}}]$, each of which gets a window. On the rest of $[x_{\mathrm{lo}}, x_{\mathrm{hi}}]$ the first program made 142,137 interval checks and the second 142,343. The smallest lower bound for F at an endpoint of a checked interval, in the second program, was $1.02 \cdot 10^{-6}$, at $x = 1.413232$. Both programs still accept the certificate with λ increased by 10^{-6} and reject it with λ increased by $1.1 \cdot 10^{-6}$.

4.2. **The upper bound.** The density G has 2,325 nodes in $[0, 6]$, mostly with spacings 1/250, 1/1000 and 1/2000 (2,287 of the 2,324 gaps) and 37 other gaps, of up to 0.763, and 1,510 of the 2,323 weights w_k are nonzero. The support of μ_0 lies in $[0.054, 5.227]$ and has many gaps. The weights are rational with $\sum_k w_k = 1$, and $\beta = 0.88363\ldots$. The bound is $\int x\, d\mu = (1-\varepsilon) \int x\, d\mu_0 + 3\varepsilon = 81383685642728309283453/450359962737052400000000$, where $\int x\, d\mu_0 = 1.80706890\ldots$.

How it was found. With $\varepsilon = 0$, minimizing $\int x\,d\mu_0$ over the weights $w_k \geq 0$ with $\sum_k w_k = 1$ and $b_Q \geq 0$, subject to $\int \log|Q|\,d\mu_0 \geq 0$ for $Q \in \mathcal{B}$, a bound on $\sum_Q b_Q \deg Q$, and (3.3) at the points of a grid, is a linear program, because (3.3) and (3.4) are linear in (w, b). We first solved it for step densities and chose the polynomials by column generation: starting from the fifteen polynomials of the lower certificate, three of them of degree 10 from [9], we added polynomials whose reduced cost is negative from a list of 23,631 irreducible totally positive polynomials of degree at most 8, until none was left. The final set has 22 polynomials, and $x^3 - 6x^2 + 9x - 1$ gets weight 0. For this set we solved the linear program with 2,323 hats, using HiGHS [7] through SciPy, with nodes on a grid over the support of the step solution. After each solution we added to the grid the local minima at which the left side of (3.3) is negative on a fine grid of 600,000 points. After the eighth solution the minimum on the fine grid was $-1.7 \cdot 10^{-7}$, and the value was 1.8070689. We then rounded the weights w_k to multiples of 2^{-50} and rescaled them to sum 1, rounded the b_Q down to multiples of 2^{-44}, and chose $\varepsilon = 1/100000$. The term $\varepsilon \log \frac{3}{2} = 4.05 \cdot 10^{-6}$ covers the small negative values that remain: between the points of the fine grid, $U_{\mu_0} - \sum_Q b_Q \log|Q|$ dips to about $-4.5 \cdot 10^{-7}$ near $x = 0.74436$, and 14 of the 21 integrals $\int \log|Q|\,d\mu_0$ are slightly negative, down to about $-3.8 \cdot 10^{-13}$. With $\varepsilon = 10^{-6}$ both programs reject the certificate at that point (Table 2).

An earlier solution of the same linear program, on a coarser fine grid, gave a certificate with the same polynomials and nodes, other weights, and $\varepsilon = 1/20000$; it proves $C_{86} \leq 1660935360692531465493/919101964769480000000 < 1.8071286$. Both programs accept it as well, with 15,509 and 10,051 interval checks.

Output of the two programs. Both accept the certificate and compute the bound exactly. The integrals in (3.4) agree to all printed digits in the two programs; the smallest is $4.05 \cdot 10^{-6}$, for $Q = x$, and they are close to $\varepsilon \deg Q \log \frac{3}{2}$ for every Q. For (3.3), the first program made 18,677 interval checks and used 102 root windows, and the second made 14,091 interval checks and used 99 windows, treating the three rational roots 0, 1 and 2 as breakpoints instead. In the second program the smallest proven lower bound on an interval was $3.1 \cdot 10^{-9}$, and the smallest value at the midpoint of a checked interval was $3.89 \cdot 10^{-6}$, at $x = 0.676625$, in the normalization $F = U_{\mu_0} - \sum_Q b_Q \log|Q| + \varepsilon \log \frac{3}{2}/(1 - \varepsilon)$. No midpoint fell at the dip near $x = 0.74436$, where F is about $3.6 \cdot 10^{-6}$.

Tests of the programs. Both reject modified certificates (Table 2). For the lower bound we varied λ, dropped polynomials, changed a coefficient of one of them, scaled multipliers and weights, and moved x_{hi}; for the upper bound we decreased ε, scaled the weights b_Q and dropped polynomials. Each program either finds a point where an inequality fails or cannot confirm a root window and stops.

5. The Lean proofs

Both bounds are proved in Lean 4 [11] with Mathlib [10]. For $B \in \mathbb{R}$ let TPTraceLe(B) be the set of algebraic integers $\alpha \in \mathbb{C}$ whose minimal polynomial has only positive real roots and that satisfy $\mathrm{tr}(\alpha) \leq B \deg(\alpha)$, where $\mathrm{tr}(\alpha)$ is the sum of these roots. The theorem `Trace86.trace_lower_N` states that TPTraceLe($\lambda_L - \varepsilon$) is finite for every $\varepsilon > 0$, where $\lambda_L = 901111277/500000000$, and it has no hypotheses. Its corollary `Trace86.trace_lower_dec_N` states that TPTraceLe(1.8022225) is finite. The theorem `Trace86.trace_upper_N` states that if the proposition `SmithThm15` holds, then TPTraceLe($\lambda_U + \varepsilon$) is infinite for every $\varepsilon > 0$, where λ_U is the upper bound of Theorem 1.1. By the definition of C_{86}, the two theorems give $\lambda_L \leq C_{86}$ and, assuming `SmithThm15`, $C_{86} \leq \lambda_U$.

TABLE 2. Modified certificates. Accepted: the program verifies the certificate. Rejected: a checked bound fails, or the program cannot confirm a root window and stops. The polynomials are numbered as in Table 1.

modification	first program	second program
lower bound		
λ increased by $5 \cdot 10^{-7}$ or 10^{-6}	accepted	accepted
λ increased by $1.1 \cdot 10^{-6}$, $1.2 \cdot 10^{-6}$, $2 \cdot 10^{-6}$, $3 \cdot 10^{-6}$ or 10^{-5}	rejected	rejected
polynomial 2, 4, 8 or 11 dropped	rejected	rejected
one or all three polynomials of degree 10 dropped	rejected	rejected
polynomial 12 dropped	accepted	accepted
coefficient of x^5 in polynomial 14 increased by 1	rejected	rejected
λ_Q of polynomial 15 multiplied by 1.1; λ_x multiplied by 1.01	rejected	rejected
all ρ_k multiplied by 1.001; largest ρ_k multiplied by 1.1	rejected	rejected
$x_{\mathrm{hi}} = 6$	rejected	rejected
upper bound		
$\varepsilon = 10^{-6}$, 10^{-7} or 10^{-14}	rejected	rejected
all b_Q multiplied by 1.001	rejected	rejected
polynomial 2 or 22 dropped	rejected	rejected

The proposition `SmithThm15` is Smith's Theorem 1.5 [22] for an interval $[a, b]$ with $b - a > 4$. Since Mathlib sets $\log 0 = 0$, its premise states Smith's condition for each nonzero $Q \in \mathbb{Z}[x]$ as three conditions: μ does not charge the roots of Q, the function $\log|Q|$ is μ-integrable, and $\int \log|Q|\, d\mu \geq 0$. Together they are equivalent to Smith's condition with $\log 0 = -\infty$. All other mathematical steps are proved in Lean, including the energy inequality behind Lemma 2.1, the closed forms of Lemma 2.3, and the minimum principle and the resultant argument of Lemma 3.1.

The finite checks on the certificates are carried out by checkers written in Lean, whose soundness is proved in Lean, and they are evaluated with `native_decide`: 153 checks for the lower bound (pieces of $[1/100, 30)$, the energy bound and the two tails) and 78 for the upper bound (73 pieces of $[1/100, 6]$ and five further checks, among them the interval $[0, 1/100]$, the degree condition (3.2), the integrals (3.4) and the value of the bound). Each check enters the proof as an auxiliary axiom tied to its statement. So, besides the three standard axioms of Lean, the trusted base includes Lean's compiler and the native evaluation of these checks. With the checks as named axioms, the exported proofs of both bounds are accepted by three independent kernel implementations: Lean's own kernel through `leanchecker`, nanoda [12], with the checks permitted as axioms by name, and lean4lean [2]. The proof of the lower bound was also replayed module by module in Lean's kernel. In a second version of both proofs, every check is decided by Lean's kernel, with `decide +kernel`, so that Lean's compiler is not part of the trusted base. The theorems `Trace86.trace_lower_K` and `Trace86.trace_upper_K` have the same statements as `Trace86.trace_lower_N` and `Trace86.trace_upper_N` and use the same certificates and checkers. The checks are split into modules: for the lower bound, 14,957 modules for the end points of the pieces of the interval, one end point each, 599 modules for the pieces, 25 pieces each, 9,142 modules for the pieces of the energy bound, and four modules for the data and the tails; for the upper bound, 7,169 modules for the pieces of the interval, two pieces each, 21 modules for the integrals (3.4), one for each polynomial, and two further modules. These theorems, and their forms `trace_lower_dec_K` and `trace_upper_dec_K` for the decimal bounds 1.8022225 and 1.8070809, depend only on the three standard axioms `propext`, `Classical.choice` and `Quot.sound`. Building this version takes about 310 CPU-hours for the lower bound and about 55 for the upper bound, with up to about 7.6 GB of memory for one

module. All 24,865 modules of the proof of the lower bound and all 7,313 modules of the proof of the upper bound were replayed in Lean's kernel. With the generated checks stated as axioms, the complete proofs of both bounds were also accepted by `leanchecker`, nanoda and lean4lean, and so were the five modules with the literal data and the global checks and 59 of the generated modules.

6. How far the two methods can go

The lower bound. The last two steps of the proof of Lemma 2.1 show that $\int x\,d\mu \ge \lambda$ for every probability measure μ on $[0,\infty)$ with $I(\mu) \ge 0$ and $\int \log|Q|\,d\mu \ge 0$ for $Q \in \mathcal{A}$ (if $\int x\,d\mu = \infty$ there is nothing to prove). So no certificate with the polynomial set $\mathcal{A}$ gives more than the infimum $\lambda_{\mathcal{A}}$ of $\int x\,d\mu$ over these measures. For the fifteen polynomials of the lower certificate, the program of Section 4.1 gives 1.802223655, and a second-order cone program over step densities, a restriction of the problem that defines $\lambda_{\mathcal{A}}$, gives 1.8022490 with 1,300 steps and 1.8022344 with 2,600 steps, so numerically $\lambda_{\mathcal{A}} \le 1.8022344$; without the three polynomials of degree 10 it gives 1.8022435 with 1,300 steps. These fifteen polynomials include the irreducible factors of the eighteen polynomials of [5]. In floating-point arithmetic we found no irreducible totally positive polynomial of degree at most 6 and trace at most $3d$, of degree 7 and trace at most $2.5d$, or of degree 8 and trace at most $2d$ (503,124 polynomials in all) whose constraint $\int \log|Q|\,d\mu \ge 0$ is violated by the optimal measure with a piecewise linear density (2,866 hats) for these fifteen polynomials. So lower bounds much above 1.8022 seem to need other constraints.

The upper bound. Here every nonzero $P \in \mathbb{Z}[x]$ must satisfy $\int \log|P|\,d\mu \ge 0$. The next proposition shows that a measure with a bounded density and positive energy satisfies these conditions for all squarefree, in particular all irreducible, polynomials of large degree. Since $\int \log|P|\,d\mu$ is additive in P, only irreducible polynomials of small and intermediate degree matter.

Proposition 6.1. *Let μ be a compactly supported probability measure on $\mathbb{R}$ with a density bounded by M and energy $I(\mu) = \eta > 0$, and let $P \in \mathbb{Z}[x]$ be squarefree of degree $d \ge 1$ with leading coefficient a. Then for every $S > 0$,*

$$\int \log|P|\,d\mu \ge \frac{\log|a|}{d} + d\Big(\frac{\eta}{2} - M\sqrt{\frac{\pi}{S}} - \frac{E_1(S)}{2}\Big) - \frac{\gamma + \log S + E_1(S)}{4},$$

where $E_1(S) = \int_S^\infty e^{-u}\,du/u$ and γ is Euler's constant.

Proof. For $S > 0$ and $x, y \in \mathbb{C}$ let $k_S(x,y) = \int_0^S (e^{-s|x-y|^2} - e^{-s})\,ds/s$. Then $k_S(x,x) = \gamma + \log S + E_1(S)$, and $k_S(x,y) = -2\log|x-y| + E_1(S) - E_1(S|x-y|^2)$ for $x \ne y$, so that $-2\log^+|x-y| \le k_S(x,y) \le k_S(x,x)$. Since the Gaussian kernel is positive definite, $\iint k_S\,d\sigma\,d\sigma = \int_0^S \big(\iint e^{-s|x-y|^2}\,d\sigma\,d\sigma\big)\,ds/s \ge 0$ for every finite signed measure σ on $\mathbb{C}$ with compact support and $\sigma(\mathbb{C}) = 0$, by Fubini's theorem and these bounds. Let $z_1, \dots, z_d$ be the roots of P, let $\nu = \frac{1}{d}\sum_i \delta_{z_i}$, and apply this to $\sigma = \nu - \mu$. Since P is squarefree, its discriminant $a^{2d-2}\prod_{i<j}(z_i - z_j)^2$ is a nonzero integer, and with $E_1 \ge 0$,

$$\iint k_S\,d\nu\,d\nu \le \frac{4(d-1)\log|a| + d(d-1)E_1(S) + d\,(\gamma + \log S + E_1(S))}{d^2}.$$

Since $|z-y| \ge |\operatorname{Re} z - y|$ for real y, E_1 is decreasing, and $\int_{\mathbb{R}} E_1(St^2)\,dt = 2\sqrt{\pi/S}$, we have

$$\iint k_S\,d\nu\,d\mu \ge -\frac{2}{d}\sum_i U_\mu(z_i) - 2M\sqrt{\frac{\pi}{S}}, \qquad \iint k_S\,d\mu\,d\mu \le -2\eta + E_1(S).$$

Combining the three estimates with $\iint k_S \, d\sigma \, d\sigma \geq 0$ and with $\int \log|P| \, d\mu = \log|a| + \sum_i U_\mu(z_i)$ gives the claim, after dropping a term $E_1(S)/4 \geq 0$. □

For instance, the density of μ_0 in our upper certificate is at most 16.1. For a measure with density at most 16.1 and energy 10^{-3}, the best choice of S in Proposition 6.1 covers only the degrees $d \geq 14{,}946$, and for energy 10^{-2} the degrees $d \geq 1{,}247$. The finitely many polynomials of smaller degree must be handled otherwise, for instance by a condition like (U1). In floating-point arithmetic, at the optimum of the linear program of Section 4.2 we found no polynomial with negative reduced cost among the irreducible totally positive polynomials of degree at most 6 and trace at most $3d$ (207,843 polynomials), of degree 7 and trace at most $2.5d$ (277,292), of degree 8 and trace at most $2.2d$ (75,181), and of degree 9 and trace 17 (667), nor among the integer polynomials of degree at most 4 with leading coefficient 1 or 2 and other coefficients at most 6 in absolute value. Of the polynomials of degree at least 9 that we tried, only the three of degree 10, whose trace is 1.8 times the degree, improved the bound. So we expect that lowering the upper bound substantially needs integer polynomials of high degree and small trace.

Data availability

The two certificates, the four verification programs with their output, the modified certificates of Table 2, the search programs and the Lean sources are archived at doi:10.5281/zenodo.23563971 and in the repository `https://github.com/tejasvi/schur-siegel-smyth-trace-bounds-v4`. The verification programs need Python 3 and python-flint 0.9 [16]; some also need numpy.

Use of AI tools

Generative AI tools were used to find and prove the results, to write the programs, and to draft the text. The author reviewed the arguments and the programs and takes responsibility for the content.

References

[1] J. Aguirre and J. C. Peral, *The trace problem for totally positive algebraic integers*, with an appendix by J.-P. Serre, in: Number Theory and Polynomials, London Math. Soc. Lecture Note Ser. **352**, Cambridge Univ. Press, Cambridge, 2008, 1–19.

[2] M. Carneiro, *Lean4Lean: Verifying a typechecker for Lean, in Lean*, arXiv:2403.14064, 2024.

[3] S. Diamond and S. Boyd, *CVXPY: a Python-embedded modeling language for convex optimization*, J. Mach. Learn. Res. **17** (2016), no. 83, 1–5.

[4] The FLINT team, *FLINT: Fast Library for Number Theory*, version 3.6.0, `https://flintlib.org`.

[5] D. N. Giraudin, *A new lower bound for the Schur–Siegel–Smyth trace problem*, arXiv:2609.29298v1, 2026.

[6] P. J. Goulart and Y. Chen, *Clarabel: an interior-point solver for conic programs with quadratic objectives*, arXiv:2405.12762, 2024.

[7] Q. Huangfu and J. A. J. Hall, *Parallelizing the dual revised simplex method*, Math. Program. Comput. **10** (2018), 119–142.

[8] F. Johansson, *Arb: efficient arbitrary-precision midpoint-radius interval arithmetic*, IEEE Trans. Comput. **66** (2017), 1281–1292.

[9] J. McKee and C. Smyth, *Salem numbers of trace -2 and traces of totally positive algebraic integers*, in: Algorithmic Number Theory (ANTS VI), Lecture Notes in Comput. Sci. **3076**, Springer, Berlin, 2004, 327–337.

[10] The mathlib Community, *The Lean mathematical library*, in: Proc. 9th ACM SIGPLAN Int. Conf. Certified Programs and Proofs (CPP 2020), 2020, 367–381.

[11] L. de Moura and S. Ullrich, *The Lean 4 theorem prover and programming language*, in: Automated Deduction – CADE 28, Lecture Notes in Comput. Sci. **12699**, Springer, 2021, 625–635.

[12] *nanoda_lib*, a type checker for Lean 4, `https://github.com/ammkrn/nanoda_lib`.

[13] B. J. Orloski and N. Talebizadeh Sardari, *A quantitative converse of Fekete's theorem*, arXiv:2304.10021v2, 2024.
[14] B. J. Orloski, N. Talebizadeh Sardari and A. Smith, *New lower bounds for the Schur–Siegel–Smyth trace problem*, Math. Comp. **94** (2025), 2005–2040; arXiv:2401.03252.
[15] R. Pinho, *An explicit upper-bound certificate for the Schur–Siegel–Smyth trace constant*, Zenodo, doi:10.5281/zenodo.23486957, 2026; certificate and checker at `https://github.com/rpinho/c86-trace-certificate`, commit 116a58f.
[16] python-flint: Python bindings for FLINT, version 0.9.0, `https://github.com/flintlib/python-flint`.
[17] B. Qu and C. Yang, *Limit distribution of algebraic integral points on curves*, arXiv:2609.39505v1, 2026.
[18] T. Ransford, *Potential theory in the complex plane*, London Math. Soc. Stud. Texts **28**, Cambridge Univ. Press, Cambridge, 1995.
[19] E. B. Saff and V. Totik, *Logarithmic potentials with external fields*, Grundlehren Math. Wiss. **316**, Springer, Berlin, 1997.
[20] I. Schur, *Über die Verteilung der Wurzeln bei gewissen algebraischen Gleichungen mit ganzzahligen Koeffizienten*, Math. Z. **1** (1918), 377–402.
[21] C. L. Siegel, *The trace of totally positive and real algebraic integers*, Ann. of Math. (2) **46** (1945), 302–312.
[22] A. Smith, *Algebraic integers with conjugates in a prescribed distribution*, Ann. of Math. (2) **200** (2024), 71–122; we cite the numbering of arXiv:2111.12660v2.
[23] C. J. Smyth, *Totally positive algebraic integers of small trace*, Ann. Inst. Fourier (Grenoble) **34** (1984), no. 3, 1–28.
[24] T. Tao et al., *Optimization constants in mathematics*, online repository, `https://teorth.github.io/optimizationproblems/`, 2026.
[25] C. Wang, J. Wu and Q. Wu, *Totally positive algebraic integers with small trace*, Math. Comp. **90** (2021), 2317–2332.

ORCID: `https://orcid.org/0000-0003-4668-3639`