Constructing rational Lyapunov certificates for planar homogeneous fields

Lluis Eriksson

24 October 2026
Research draft 2; revised bounds and attributed lower scale

Abstract

For each fixed odd degree d, we give a deterministic construction of strict rational Lyapunov functions for globally asymptotically stable planar homogeneous polynomial vector fields with rational coefficients. If B is the dense binary input length, both the construction time and the total dense output length are at most $2^{C_d(B+1)}$, for an effectively computable constant C_d. The output has the form $P/(x^2+y^2)^r$, where P is positive homogeneous of degree $2r+2$; it extends continuously differentiably to the origin. The argument covers nonvanishing angular velocity, angular sign changes, and angular zeros of arbitrary multiplicity. Its main ingredients are a uniform algebraic height bound for the rotational mean, a mean-zero angular correction using normalized nonnegative trigonometric powers, and a finite-power conversion that avoids directly approximating an exponentially large integrating factor. Rational converse theorems and planar stability decision are prior results. The contribution is a joint coefficient-dependent degree, encoding, and construction bound in dimension two. An attributed consequence of a prior Fourier bound shows that exponential dense output is unavoidable already for cubic fields. No general software implementation, sharp constant, polynomial-certificate theorem, or higher-dimensional conclusion is asserted.

1 The quantitative certificate question

Consider

$$\dot{z} = X(z), \qquad z = (x, y), \qquad X = (X_1, X_2) \in \mathbb{Q}[x, y]^2,$$

where both components are homogeneous of a fixed odd degree $d \geq 1$. Global asymptotic stability (GAS) means Lyapunov stability of the origin together with forward completeness and convergence to the origin for every initial state.

Ahmadi and El Khadir proved that a GAS homogeneous polynomial vector field admits a rational Lyapunov function with a power of the squared Euclidean norm as denominator [1, Theorem 3.1]. They also asked for bounds depending on the vector-field coefficients [1, Section 7]. The existence statement is therefore not new. In the plane, angular dynamics give stability criteria and decidability; the recent treatment of Korda explicitly separates this planar situation from higher-dimensional undecidability [2, 3].

The question addressed here is quantitative: how large a *rationally encoded* certificate need one construct from a rational planar input? An existence theorem alone supplies neither coefficient-height bounds nor an algorithm with a stated running time. A search over certificates with an unspecified degree does not supply those bounds either.

We use dense binary encoding. The input length B counts signed numerators, positive denominators, all Cartesian coefficient positions, and finite framing. The output length counts every rational coefficient of the expanded numerator and denominator. Redundant storage of a common denominator is allowed and counted. For fixed d, changing ordinary framing conventions changes constants only. Running time is bit complexity on a deterministic Turing machine, using elementary integer arithmetic if desired.

Theorem 1 (Quantitative planar rational certificates)**.** *For every odd $d \geq 1$, there is an effectively computable constant C_d and a deterministic algorithm with the following property. Given a homogeneous $X \in \mathbb{Q}[x,y]^2$ of degree d and dense input length B, the algorithm decides GAS. If the answer is positive, it constructs*

$$V(x,y) = \frac{P(x,y)}{\rho^r}, \qquad \rho = x^2 + y^2, \quad r \in \mathbb{Z}_{\geq 0}, \quad \deg P = 2r + 2, \tag{1}$$

with rational homogeneous $P > 0$ off the origin, such that $\mathcal{L}_X V < 0$ there. Set $V(0) = 0$. Then V is proper and C^1 on $\mathbb{R}^2$. The degrees, total dense rational output length, and running time are all at most

$$2^{C_d(B+1)}.$$

The dependence on d may be an arbitrarily large computable function. In particular, this is not a polynomial-time statement jointly in d, B, and the proof does not provide a practical numerical value of C_d. It does provide an effective procedure for obtaining such a value from finite real-algebraic elimination data.

The distinction between polynomial and rational certificates is essential. Liu and Fitzsimmons give a GAS planar homogeneous cubic with no real-analytic Lyapunov function, hence no polynomial Lyapunov function, while exhibiting an explicit rational one [4]. Our theorem supplies a bound within the rational class and does not settle the polynomial degree questions discussed by Ahmadi and Parrilo [5, Section 6]. Implicit algebraic Lyapunov functions, such as those studied by Abdelraouf, Feron and Shamma [6], form another class; the present output is an explicit rational quotient.

Proof structure. Section 2 reduces the problem to an angular inequality. Section 3 establishes effective separation from zero for the quantities used in the construction. Sections 4 and 5 construct a rational trigonometric polynomial v of mean zero satisfying $F + Gv < 0$. Section 6 turns its primitive into (1). Section 7 accounts for computation, expansion and verification.

2 Polar reduction and the certificate target

Write $x = R\cos\theta$, $y = R\sin\theta$, with $R > 0$, and put $\phi = 2\theta$. Define

$$A = xX_1 + yX_2, \qquad C = xX_2 - yX_1.$$

On the unit circle set $F = A|_{R=1}$, $G = C|_{R=1}$, regarding both as functions of ϕ. Because $d+1$ is even, they are real trigonometric polynomials of degree at most

$$n_d = (d+1)/2$$

in ϕ, with rational real and imaginary Fourier parts. Their coefficient lengths are $O_d(B+1)$. The polar equations are

$$\dot{R} = R^d F(\phi), \qquad \dot{\theta} = R^{d-1} G(\phi), \qquad \dot{\phi} = 2R^{d-1} G(\phi). \tag{2}$$

Every fixed number of derivatives of F, G has norm $2^{O_d(B+1)}$.

For a 2π-periodic function h, write

$$\langle h \rangle = \frac{1}{2\pi} \int_0^{2\pi} h(\phi)\, d\phi.$$

If $p > 0$ is smooth and periodic, then $V = R^2 p(\phi)$ satisfies

$$\mathcal{L}_X V = 2R^{d+1}(Fp + Gp'). \tag{3}$$

Here and throughout, primes are derivatives with respect to ϕ.

We use the following necessary stability conditions. If G has no zero, a reflection, if needed, makes $G > 0$. Integrating $d \log R / d\theta = F/G$ over a turn shows that GAS requires

$$a = -\langle F/G \rangle > 0. \tag{4}$$

A nonnegative integral gives a noncontracting turn or a periodic orbit. If G has a zero, the corresponding ray is invariant. GAS then requires

$$F < 0 \quad \text{on } \{G = 0\}. \tag{5}$$

If $F = 0$ there, a nonzero equilibrium lies on the ray; if $F > 0$, the radial trajectory fails to converge to zero. These conditions, and their sufficiency, are classical in planar homogeneous stability; compare [3, Corollary 21.2]. Below we prove sufficiency again by actually constructing a strict proper certificate. Thus the proof needs no unproved converse stability criterion.

Our intermediate target is a rational real trigonometric polynomial v and rational $\delta > 0$ such that

$$\langle v \rangle = 0, \qquad F + Gv \le -\delta \quad \text{on the circle.} \tag{6}$$

We shall ensure that the degree, norm, total coefficient encoding, and δ^{-1} are $2^{O_d(B+1)}$. The norm bound, in addition to an encoding bound, is important for the later conversion.

3 Uniform algebraic separation

We use effective quantifier elimination over the real numbers in fixed formula size; see, for example, [7, Theorem 2.18]. The elementary consequence needed here is recorded with its uniformity requirement.

Lemma 2 (Height of a single-valued semialgebraic quantity)**.** *Fix a first-order formula over $\mathbb{Q}$, with rational input parameters c, whose output fiber in the real variable u, on its domain, is a singleton. If the input parameters have total length at most B, every positive finite output satisfies*

$$2^{-K(B+1)} \le u \le 2^{K(B+1)}$$

for an effectively computable constant K depending only on the formula.

Proof. Eliminate quantifiers once, with c, u free, and clear the fixed rational denominators of the resulting polynomial atoms. After substituting the rational tuple c and clearing its denominators, every nonzero univariate integer atom has degree at most a fixed D and coefficient magnitude at most $H = 2^{K_0(B+1)}$.

Some such nonzero atom must vanish at the singleton output u. Otherwise all nonzero atoms have locally constant signs near u; atoms specialized to the zero polynomial are constant as well. The Boolean formula would then be constant on a neighborhood of u, contradicting its singleton fiber. This argument explicitly allows specialized atoms that vanish identically.

The Cauchy bound gives $|u| \le 1 + H$. Strip a power of the variable from the vanishing atom. If $0 < u < 1$, its remaining constant coefficient is a nonzero integer and hence

$$1 \le \sum_{j=1}^{D} |a_j| u^j \le DHu.$$

Increasing K proves both assertions. The elimination procedure and the coefficient bounds are effective. □

Minima of fixed-degree rational trigonometric polynomials have fixed-size semialgebraic graphs: describe the unit circle by two real coordinates, assert a lower bound at every circle point, and assert equality at one point. The same observation applies to a positive minimum, its reciprocal, and to sign tests.

A less immediate quantity is the rotating mean. Merely observing that this mean is algebraic for each input would not give Lemma 2; a uniform graph is required.

Lemma 3 (Uniform graph for the rotating mean)**.** *For fixed d, on the domain where C is strictly positive on the unit circle, the map*

$$X \longmapsto \langle F/G \rangle$$

has an effectively constructible, single-valued first-order graph over $\mathbb{Q}$, of size depending only on d.

Proof. Put

$$H(t) = \frac{A(1,t)}{(1+t^2)C(1,t)}.$$

Since $C(0,1) > 0$, $C(1,t)$ has exact degree $d+1$; it has no real root. Therefore H has no real pole and is $O(t^{-2})$ at infinity. The substitution $t = \tan\theta$, using the π-periodicity in θ, followed by the residue theorem gives

$$\langle F/G \rangle = \frac{1}{\pi} \int_{\mathbb{R}} H(t)\, dt = 2i \sum_{\operatorname{Im} z > 0} \operatorname{Res}_z H. \tag{7}$$

This is the residue normalization used in [3, Theorem 20.3]. In particular, the factor π cancels before any real-algebraic formula is formed.

The denominator has degree $d+3$. Enumerate its finitely many patterns of distinct complex roots and their positive multiplicities. In each pattern, root real and imaginary parts, coefficient factorization identities, pairwise distinction, and signs of imaginary parts are first-order real conditions over $\mathbb{Q}$. If z has multiplicity k in the unreduced denominator, its residue is

$$\frac{1}{(k-1)!} \frac{d^{k-1}}{dt^{k-1}} \big((t-z)^k H(t)\big)\Big|_{t=z}.$$

After cancellation of the specified root factor, all denominator factors evaluated here are nonzero. These rational operations can be expressed with auxiliary product equations and nonzero-denominator conditions. The expression is valid also for a removable pole, whose residue is zero. Derivative orders and degrees depend only on d.

Take real and imaginary parts, sum residues in the upper half-plane, and quantify the auxiliary variables. The finite disjunction over patterns gives the required graph. Relabeling roots does not change the sum; hence the output fiber is a singleton, including multiple-root and cancellation cases. □

Lemma 4 (A uniform radial penalty at angular zeros)**.** *If G has a zero and (5) holds, there is an integer $1 \le K \le 2^{O_d(B+1)}$ for which*

$$F - KG^2 \le -1/K. \tag{8}$$

A suitable K can be chosen effectively from d, B.

Proof. Compactness gives a neighborhood of $\{G = 0\}$ where F is bounded above by a negative constant. Off that neighborhood, $|G|$ has a positive minimum. A sufficiently large K therefore satisfies (8). Feasibility is monotone in K, since $F - KG^2 + 1/K$ decreases with $K > 0$, and is closed. The feasible set in $K \ge 1$ has a least element K_0.

Its graph is a fixed-size first-order formula: on the circle require

$$KF - K^2G^2 \le -1$$

and require that no smaller $K \ge 1$ is feasible. Lemma 2 bounds K_0 above by $2^{O_d(B+1)}$. An integer upper bound, determined by the effective constants in that lemma, works by monotonicity. □

For later bookkeeping, compute all the fixed-in-d elimination formulas just discussed, including the rotational sign test and the minima used below. Their finite degrees, coefficient heights and monomial counts determine an integer k_d. Enlarge it to bound the elementary Fourier conversion and derivative estimates. We may thus take

$$E = 2^{k_d(B+1)} \tag{9}$$

as a common upper bound only for the basic quantities with fixed-degree or fixed-formula descriptions, and their positive reciprocals. Later auxiliary bounds may use fixed powers of E. In particular, E need not bound the amplitude or mean of the high powers ψ introduced in Section 5; those values can be doubly exponential, and Section 5 handles them by normalization. This is computable preprocessing depending on d, rather than advice depending noncomputably on the input.

4 Nonvanishing angular velocity

Assume $G > 0$ and $a = -\langle F/G \rangle > 0$. Let

$$f = -F/G, \qquad v_0 = f - a, \qquad g = \min G.$$

Then $\langle v_0 \rangle = 0$ and

$$F + Gv_0 = -aG.$$

Lemmas 2 and 3 give $a, g \geq E^{-1}$, with E enlarged if needed. Quotient differentiation gives rational bounds $Q, D, T \geq 1$ on $\|f\|_\infty, \|f'\|_\infty, \|f''\|_\infty$, all of value $2^{O_d(B+1)}$ and bit length $O_d(B+1)$. Choose a rational $H \geq \max(1, \|G\|_\infty)$ of the same size and set

$$\varepsilon = \frac{1}{4E^2 H}.$$

We construct an exactly mean-zero rational approximation without having to compute the integral a numerically.

Lemma 5 (Certified rational Fourier approximation)**.** *In time $2^{O_d(B+1)}$, one can construct a real rational trigonometric polynomial R_N such that*

$$\|R_N - f\|_\infty < \varepsilon/2, \qquad \deg R_N, \ \textit{total coefficient length} \ \leq 2^{O_d(B+1)}.$$

Proof. Choose integers

$$N \geq \max(1, 8T/\varepsilon), \qquad M > 2N, \qquad M \geq \frac{64(2N+1)(D+NQ)}{\varepsilon}.$$

Two integrations by parts give $|\widehat{f}_k| \leq T/k^2$ for $k \neq 0$. The Fourier tail outside $[-N, N]$ is at most $2T/N \leq \varepsilon/4$.

Approximate each coefficient in this interval by the equally spaced M-point rectangular quadrature. For $h_k(\phi) = f(\phi)e^{-ik\phi}$, $\|h_k'\|_\infty \leq D + NQ$. Integrating the error from each left endpoint shows that its normalized quadrature error is at most $\pi(D+NQ)/M$. Summing over all $2N+1$ modes gives an error at most $\varepsilon/16$, since $\pi < 4$.

At each node, compute dyadic approximations to f and to the phase with complex absolute errors at most

$$u = \min\left(1, \frac{\varepsilon}{16(2N+1)(Q+2)}\right).$$

Their product error is at most $(Q+2)u$. Averaging and summing modes adds at most $\varepsilon/16$. Compute positive modes, define negative ones by exact conjugation, and take the real part of the zeroth mode. These choices preserve the same error bounds and enforce reality. The total is less than $\varepsilon/2$.

Here all evaluations are effective bit operations. Reduce phase indices using $kj \bmod M$; all trigonometric arguments then lie in a fixed bounded interval. Machin's identity

$$\pi = 4\big(4\arctan(1/5) - \arctan(1/239)\big)$$

with alternating-series tails, and Taylor series for sine and cosine on a bounded interval, provide rational approximations in polynomial time in the requested precision. Evaluate F, G at these approximations with enough guard bits that the error in G is at most $g/2$, and use rational division for f. For an explicit error budget, enlarge the basic $E \geq 2$ to bound $\|F\|_\infty$ and g^{-1}. Evaluate F, G with errors at most $\zeta = u/(16E^3)$. Then $\widetilde{G} \geq 1/(2E)$ and

$$\left|\frac{\widetilde{F}}{\widetilde{G}} - \frac{F}{G}\right| \leq 2E\zeta + 2E^3\zeta \leq u/4.$$

Reserve another $u/4$ for dyadic rounding, and approximate each phase component with error at most $u/4$. This gives the claimed sample and complex phase accuracies, with spare margin. The

coefficient and frequency bounds reduce evaluation of F, G to sine and cosine accuracy $\zeta/(c_d E)$, for a computable constant c_d. All required logarithms, including $\log M, \log N, \log(1/u)$, are $O_d(B+1)$.

Round sample components to a common dyadic grid before forming products. Thus an averaged coefficient has denominator M times a common dyadic power; unrelated sample denominators are not multiplied successively. Per-operation bit lengths are polynomial in $B+1$ for fixed d. There are $M(2N+1) = 2^{O_d(B+1)}$ sample-mode operations, so direct summation already gives the stated bound. No transcendental oracle or assumed fast Fourier convergence is used. □

Set $v = R_N - \langle R_N \rangle$, subtracting the exact rational constant coefficient. Since $\langle f \rangle = a$,

$$\|v - v_0\|_\infty < \varepsilon, \qquad F + Gv \le -aG + H\varepsilon \le -\frac{3}{4E^2}.$$

Thus (6) holds with $\delta = 1/(2E^2)$. Its degree, norm and encoding have the required bounds.

5 Angular zeros, including sign changes

If $G \equiv 0$, condition (5) gives $F < 0$ everywhere and $V = \rho$ suffices. Otherwise choose K from Lemma 4 and put $\delta_0 = 1/K$. Choose rational $H, S \ge 1$ with

$$\|G\|_\infty \le H, \qquad \|G'\|_\infty, \|G''\|_\infty \le S,$$

of value $2^{O_d(B+1)}$ and bit length $O_d(B+1)$. If $\langle G \rangle = 0$, take $v = -KG$. It already has mean zero and satisfies (6) with $\delta = \delta_0$.

Otherwise let $s = \operatorname{sgn}(\langle G \rangle)$. We use

$$v = -KG + c\psi, \qquad c = \frac{K \langle G \rangle}{\langle \psi \rangle}, \tag{10}$$

where $\psi \ge 0$ is a rational trigonometric polynomial with positive mean. The mean of v is exactly zero. It remains to bound the harmful part of $Gc\psi$ by $\delta_0/2$.

5.1 Changing angular sign

Let $\kappa > 0$ be a rational lower bound for $-\min(sG)$ with $\kappa^{-1} = 2^{O_d(B+1)}$, supplied by Lemma 2. A factor-two approximation is unnecessary; any such lower bound works. At a minimum point, an interval of circular radius

$$w = \min(1, \kappa/(2S))$$

satisfies $sG \le -\kappa/2$. For a positive integer N set

$$\psi = (1 - sG/H)^{2N}.$$

On that interval, Bernoulli's inequality gives

$$\psi \ge (1 + \kappa/(2H))^{2N} \ge N\kappa/H, \qquad \langle \psi \rangle \ge \frac{wN\kappa}{\pi H}.$$

Where $sG \geq 0$, one has $\psi \leq 1$, so

$$Gc\psi \leq \frac{KH^2}{\langle\psi\rangle} \leq \frac{\pi KH^3}{wN\kappa}.$$

Where $sG < 0$, the product is nonpositive. Choosing

$$N \geq \frac{8KH^3}{\delta_0 w\kappa} \tag{11}$$

makes the harmful contribution less than $\delta_0/2$. All factors and reciprocals in (11) are $2^{O_d(B+1)}$, so $N = 2^{O_d(B+1)}$ is sufficient.

5.2 One angular sign with zeros

Here $g = sG$ satisfies $0 \leq g \leq H$, with at least one zero. At any zero ϕ_0, $g'(\phi_0) = 0$; hence

$$g(\phi_0 + t) \leq St^2/2.$$

Set

$$\psi = (1 - g/H)^{2N}, \qquad w = \min\left(1, \sqrt{\frac{H}{2SN}}\right).$$

For $|t| \leq w$, $g/H \leq 1/(4N)$, whence

$$\psi \geq (1 - 1/(4N))^{2N} \geq 1/2, \qquad \langle\psi\rangle \geq w/(2\pi).$$

The elementary maximum of $g(1 - g/H)^{2N}$ is at most $H/(2N)$. It follows that

$$Gc\psi \leq \frac{\pi KH^2}{Nw}.$$

Since

$$\frac{1}{Nw} = \max\left(\frac{1}{N}, \sqrt{\frac{2S}{H}}\frac{1}{\sqrt{N}}\right),$$

it suffices to take

$$N \geq \max\left(\frac{8KH^2}{\delta_0}, \frac{128K^2H^3S}{\delta_0^2}\right). \tag{12}$$

Each branch is then at most $\pi\delta_0/8 < \delta_0/2$. The radius w is used only in the proof; its square root need not be computed by the construction. This case covers every angular zero multiplicity.

5.3 Coefficient growth and the normalization mechanism

In both cases ψ has degree $J_\psi \leq 2Nn_d$. Starting with a common denominator for G, H of $O_d(B + 1)$ bits, its power has coefficient bit lengths $O_d(N(B + 1) + N)$. Its mean is exactly its constant Fourier coefficient. Division by that nonzero rational number in (10) preserves a single-exponential coefficient-size bound. The total encoding is therefore $2^{O_d(B+1)}$.

A coefficient-size bound alone would allow a doubly exponential function value. We need the stronger norm estimate. Nonnegativity of ψ implies

$$|\widehat{\psi}_k| \le \langle\psi\rangle \quad \Longrightarrow \quad \frac{\psi}{\langle\psi\rangle} \le 2J_\psi + 1.$$

Thus

$$\|v\|_\infty \le 2KH(J_\psi + 1) = 2^{O_d(B+1)}. \tag{13}$$

This is the reason for using a normalized nonnegative power instead of directly approximating an integrating factor. In all angular-zero cases, (6) now holds with $\delta = \delta_0/2$, or with the stronger margin when $\langle G\rangle = 0$.

6 Finite-power conversion

Let v be the rational trigonometric polynomial constructed above. Its zero mean gives a rational real trigonometric primitive U, chosen with $\langle U\rangle = 0$ and $U' = v$. If $J = \deg v$, dividing Fourier coefficients by ik gives

$$\deg U \le J, \qquad \|U\|_\infty \le 2J\,\|v\|_\infty,$$

and single-exponential total encoding. A Fourier ℓ^1 bound $L_U \ge \|U\|_\infty$ can be computed rationally, using the sum of absolute real and imaginary parts if needed. It has value $2^{O_d(B+1)}$, by (13) and the coefficient bound $|\widehat{v}_k| \le \|v\|_\infty$. Choose rational $H_F \ge \max(1, \|F\|_\infty)$ and an integer

$$m \ge \max(1, 2L_U, 2H_F L_U/\delta). \tag{14}$$

Then $m = 2^{O_d(B+1)}$ is sufficient.

Put $q = 1 + U/m \ge 1/2$ and $p = q^m$. The following exact identity avoids an error estimate for a logarithmic derivative:

$$Fp + Gp' = q^{m-1}(Fq + Gv) = q^{m-1}((F + Gv) + FU/m) \le -\frac{\delta}{2}q^{m-1} < 0. \tag{15}$$

If $U = 0$, output ρ. Otherwise take $J = \deg U \ge 1$. Using

$$e^{i\phi} = \frac{(x + iy)^2}{\rho},$$

homogenize U as U_h/ρ^J, with rational homogeneous U_h of degree $2J$. The output is

$$V = \rho\left(1 + \frac{U_h}{m\rho^J}\right)^m = \frac{(\rho^J + U_h/m)^m}{\rho^{Jm-1}}. \tag{16}$$

The numerator is positive off the origin and has degree $2Jm$; $r = Jm - 1 \ge 0$. Equations (3) and (15) prove strict decay.

For a fixed input, p is smooth, periodic, positive and bounded away from zero. Therefore $V = R^2 p(2\theta)$ is positive and proper, $V = O(R^2)$, and its gradient off the origin is $O(R)$. Its derivative at the origin is zero, and the gradient extends continuously there. This proves the stated C^1 extension. Properness and strict decay give forward completeness and GAS: a trajectory stays in a compact sublevel set; on every compact annulus the decay is bounded away from zero. Thus the necessary tests of Section 2 are also sufficient.

7 Algorithm, bit accounting, and verification

The decision procedure uses only fixed-in-d circle sign tests and the graph of Lemma 3. If G is nonvanishing, test (4) after orientation; otherwise test (5). Reject when the applicable test fails. The elimination formulas can be computed once from d. Evaluating their integer polynomial signs at rational input uses polynomial time in $B+1$, with constants and polynomial degrees depending on d. With elementary arithmetic, fixed polynomial expressions can be evaluated in $O_d((B+1)^2)$ after enlarging the constant. The preprocessing time is a computable function of d, and can be absorbed by increasing C_d.

For accepted inputs, Section 4 gives an explicit quadrature construction; Section 5 uses exact rational Laurent-polynomial powers and constant-coefficient extraction. Circle sign tests for selecting the case remain at fixed field degree. No quantifier elimination is run on the exponentially large final numerator.

In the angular-zero case, a common input denominator prevents denominator multiplication at each addition. Naive polynomial multiplication to exponent $2N$, even without fast exponentiation, has cost polynomial in N, the output degree, and the largest intermediate coefficient bit length. All of these are $2^{O_d(B+1)}$. The primitive, rational coefficient sums, and integer choice (14) have the same scale. In the rotating case the explicit sample-mode bound in Lemma 5 gives it directly.

For final expansion, J, m and the coefficient bit lengths of U are each $2^{O_d(B+1)}$. Homogenization adds binomial coefficients of $O(J)$ bits and $O(J)$ summands. Clear a common denominator whose bit length is at most the sum of the coefficient bit lengths, also $2^{O_d(B+1)}$. If the resulting integer form has coefficient bit length L, its m-th power has coefficient bit length

$$O\big(m(L+\log(J+1))\big).$$

It has $O(Jm)$ coefficients. The same bounds apply to the dense expansion of ρ^{Jm-1}. Products of a fixed number of single exponentials enlarge only the constant in their exponent. Consequently, both the *total* dense encoding and naive expansion time are $2^{O_d(B+1)}$, not just their individual coefficient lengths. Undoing a reflection changes signs or swaps variables and preserves these bounds.

An exact output check. For any candidate P, r, compute

$$S = -(\rho \mathcal{L}_X P - rP\mathcal{L}_X \rho).$$

Then $\mathcal{L}_X(P/\rho^r) = -S/\rho^{r+1}$. Both P and S are homogeneous forms of even degree. A homogeneous even-degree form H is positive away from zero if and only if

$$H(1,0) > 0, \qquad H(0,1) > 0, \qquad H(t,1) \text{ has no real root.}$$

Indeed the last two conditions give positivity on the affine chart $y \neq 0$, and the first gives the missing projective direction. A constant dehomogenization is tested directly, while still requiring $H(1,0) > 0$; for example, $H = y^2$ must be rejected. Clear positive denominators, compute the square-free part, and apply a normalized subresultant/Sturm sequence with controlled coefficient growth. The signs at the two infinities follow from leading coefficients and degree parities. The bit cost is polynomial in the degree and integer coefficient length; a suitable subresultant construction is given by Du, Sharma and Yap [8, Theorem 2(i)]. An arbitrary unnormalized

rational remainder implementation is not being assigned this complexity guarantee; see also [9]. With the bounds already proved this check also costs $2^{O_d(B+1)}$. It checks the certificate, not the correctness of the general construction theorem.

This completes the proof of Theorem 1.

8 The lower scale is already implicit in a prior Fourier bound

The upper scale in Theorem 1 is accompanied by a simple lower consequence of existing work. We state its derivation to delimit what is new here.

Proposition 6 (Consequence of Liu–Fitzsimmons)**.** *For the cubic family with integer $k \geq 1$ and polar coefficients $F = -1 + k\cos\phi$, $G = 1$, every strict certificate P/ρ^{N-1}, with positive real homogeneous P of degree $2N$, satisfies $N > k/2 - 1$. Taking $k = 2^b$ forces dense output length $2^{\Omega(B)}$, where $B = \Theta(b)$ is its rational input length.*

Proof. The family is GAS by [4, Section IV.D]. For $p(\phi) = P(\cos(\phi/2), \sin(\phi/2))$, put $h = (\log p)'$. Lemma III.3 of [4], after $\phi = 2\theta$, gives $|\widehat{h}_1| < N$. The certificate inequality says $w = 1 - k\cos\phi - h > 0$. Since $\langle h\rangle = 0$, $\langle w\rangle = 1$ and $|\widehat{w}_1| \leq 1$. Thus $k/2 \leq |\widehat{w}_1| + |\widehat{h}_1| < 1 + N$. The Cartesian field is $X = (-\rho x + k(x^2 - y^2)x - \rho y, -\rho y + k(x^2 - y^2)y + \rho x)$. Its input length is $\Theta(\log(k+1))$, whereas dense P has $2N + 1$ positions. □

This is a consequence we extract from the cited lemma and family, not a lower-bound theorem stated verbatim there or a separate discovery claim. For fixed odd $d \geq 3$, multiplication of this field by $\rho^{(d-3)/2}$ preserves the strict certificate condition and GAS. Accordingly, the single-exponential worst-case dense-output scale cannot in general be replaced by a subexponential one. Constants in the exponent and sharper coefficient-length bounds are not matched. The lower statement concerns this certificate class and dense storage; binary exponents and compressed arithmetic circuits are different output models. The new contribution remains the general constructive upper bound.

9 Exact illustrative constructions

The first example below is cubic; the two subsequent examples are quintic. They illustrate angular cases and permit exact symbolic checks, without benchmarking a general solver or claiming optimal degree. For the quintic examples, a prescribed pair F, G yields a polynomial field by

$$X = \rho^2(Fx - Gy,\ Fy + Gx). \tag{17}$$

The denominators in the expressions below cancel.

9.1 A nonconstant rotating angular velocity

For an integer $k \geq 1$, consider

$$X_1 = -x^3 + (2k-3)x^2y - xy^2 - y^3, \qquad X_2 = 3x^3 - x^2y + (2k+1)xy^2 - y^3.$$

Here $F = k\sin\phi - 1$, $G = 2 + \cos\phi > 0$. With $q_0 = 3x^2 + y^2$, exact differentiation gives

$$k\rho\mathcal{L}_X q_0 - (k-1)q_0\mathcal{L}_X\rho = -2\rho^2 q_0.$$

Consequently $V = q_0^k/\rho^{k-1}$ is a strict certificate with $\mathcal{L}_X V = -2\rho V$. Its angular profile is $(2+\cos\phi)^k$, which is positive, so properness and the C^1 extension follow as before. This is an illustrative closed calculation, not an implementation of the general rotating quadrature.

9.2 Changing angular sign

Take

$$G = \sin\phi = \frac{2xy}{\rho}, \qquad F = 2\sin^2\phi - \frac{1}{2}, \qquad v = -2\sin\phi, \qquad U = 2\cos\phi.$$

Then $F + Gv = -1/2$, including both zeros and signs of G. With $m = 16$, $\|F\|_\infty \le 3/2$ and $\|U\|_\infty \le 2$ imply

$$F(1 + U/16) + Gv \le -\frac{1}{2} + \frac{3}{16} = -\frac{5}{16}.$$

A certificate is therefore

$$V = \frac{\left(\rho + (x^2 - y^2)/8\right)^{16}}{\rho^{15}}.$$

Its numerator degree is 32, and its denominator degree is 30. The inner quadratic is positive because it is at least $7\rho/8$. The input field (17) has rational homogeneous quintic components.

9.3 One angular sign with a zero

Take $g = (1-\cos\phi)/2 = y^2/\rho$, $G = g$, and $F = 2g^2 - 1/2$. The small choice $\psi = (1-g)^2$, with $\langle\psi\rangle = 3/8$, already works:

$$v = -2g + \frac{8}{3}(1-g)^2 = \frac{7}{3}\cos\phi + \frac{1}{3}\cos 2\phi, \qquad U = \frac{7}{3}\sin\phi + \frac{1}{6}\sin 2\phi.$$

For $0 \le g \le 1$,

$$\frac{4}{27} - g(1-g)^2 = -(g - \tfrac{1}{3})^2(g - \tfrac{4}{3}) \ge 0.$$

Hence $F + Gv \le -17/162$. Since $\|U\|_\infty \le 5/2$, $m = 128$ gives the strictly negative factor bound

$$F(1 + U/128) + Gv \le -\frac{17}{162} + \frac{15}{512} < 0.$$

Here

$$U_h = \frac{14}{3}xy\rho + \frac{2}{3}xy(x^2 - y^2), \qquad J = 2,$$

so

$$V = \frac{(\rho^2 + U_h/128)^{128}}{\rho^{255}}.$$

The numerator and denominator degrees are 512 and 510. These deliberately conservative degrees illustrate a verified construction, not practical degree minimization. The general bounds (11)–(12) are sufficient choices; an example may admit much smaller powers, as this one does.

Reproducibility boundary. A short exact rational symbolic calculation checks the displayed v, U, the cancellation in (17), and, writing $A_0 = \rho^J + U_h/m$, the identity

$$m\rho\mathcal{L}_X A_0 - (Jm-1)A_0\mathcal{L}_X\rho = 2\rho^{J+3}\big(F(1+U/m)+Gv\big)$$

for these quintic fields. The dense numerators can also be expanded. These computations support the worked examples only. The general proof relies on the preceding estimates and effective algebraic arguments. We have not implemented the complete algorithm, its precomputed elimination formulas, or its certified quadrature stage as a software package.

10 Scope and further questions

The theorem supplies a single-exponential upper bound in coefficient bit length for fixed field degree. The coarse exponential lower scale follows already from prior work as explained in Section 8. A useful explicit constant, sharper degree and coefficient-length orders, and an implementation that can compete with smaller-degree searches remain open. Improving the normalized angular power or exploiting structure in F, G could reduce degrees without changing the logical certificate class.

The rational representation matters: neither the numerator alone nor a power of it is asserted to be a polynomial Lyapunov function. Multiplying a rational certificate by its denominator changes its Lie derivative. No conclusion is drawn about higher dimensions, general nonhomogeneous dynamics, or arbitrary weak stability. The known planar decision theory and the general rational converse remain antecedents, not new corollaries claimed as separate discoveries.

The literature comparison is bounded to the sources listed below, checked through 24 October 2026, including their stated versions. It does not establish exhaustive priority. In particular, a specialist assessment of the quantitative construction bound remains necessary before assigning its mathematical significance.

AI assistance and review status. The author used OpenAI Codex for exploration, source comparison, proof development, symbolic checks and manuscript preparation. A GPT-6 Astra session configured with effort `xhigh` audited earlier proof notes, including the construction-time extension. A separate fresh conversation reviewed the exact first draft and identified the scope clarification for E incorporated here. The original draft and reports are preserved; assessments must identify the exact artifact they cover. These sessions share filesystem context and are not technically isolated, statistically independent, human, or formal proof reviews. Neither note-level findings nor a draft score is silently transferred to different PDF bytes. This revision has not received journal peer review. Numerical grids, when used during exploration, are not substituted for proofs. No Lean formalization of the theorem is claimed.

Example artifacts. The two original quintic example calculations and their recorded outputs are available in a pinned public repository snapshot. Their finite checks do not constitute a general solver or a formal proof of Theorem 1.

References

[1] A. A. Ahmadi and B. El Khadir, *On Algebraic Proofs of Stability for Homogeneous Vector Fields*, arXiv:1803.01877v4, 2018. https://arxiv.org/abs/1803.01877v4. See also

the author manuscript, Theorem 3.1 and Section 7: https://optimization-online.org/wp-content/uploads/2018/03/6502.pdf.

[2] M. Korda, *Lyapunov stability of polynomial vector fields is undecidable*, arXiv:2609.22058v2, 2026. https://arxiv.org/abs/2609.22058v2.

[3] M. Korda, *Supplement to Lyapunov stability of polynomial vector fields is undecidable*, Part III, especially Theorem 20.3 and Corollary 21.2, 2026. https://homepages.laas.fr/mkorda/arnold_supplement.pdf. The consulted 60-page copy has SHA-256 0b6090d432cb6ae175e883363246a94cc4 dbe3dbeb7d3d8ed2c0578e74eeccf9.

[4] J. Liu and M. Fitzsimmons, *A Globally Asymptotically Stable Planar Homogeneous Polynomial Vector Field With No Polynomial Lyapunov Function*, arXiv:2607.16171v1, 2026. https://arxiv.org/abs/2607.16171v1.

[5] A. A. Ahmadi and P. A. Parrilo, *Stability of Polynomial Differential Equations: Complexity and Converse Lyapunov Questions*, arXiv:1308.6833, 2013. https://arxiv.org/abs/1308.6833.

[6] H. Abdelraouf, E. Feron and J. S. Shamma, *Algebraic Lyapunov Functions for Homogeneous Dynamic Systems*, arXiv:2303.02185v1, 2023. https://arxiv.org/abs/2303.02185v1.

[7] S. Basu, *Algorithms in Real Algebraic Geometry: A Survey*, arXiv:1409.1534, 2014. Author version, especially Theorem 2.18: https://www.math.purdue.edu/~sbasu/raag_survey2011_final.pdf.

[8] Z. Du, V. Sharma and C. K. Yap, *Amortized Bound for Root Isolation via Sturm Sequences*, author manuscript, Theorem 2(i), pp. 4–5. https://cs.nyu.edu/exact/doc/sturmcomplexity.pdf.

[9] S. Basu, R. Pollack and M.-F. Roy, *Algorithms in Real Algebraic Geometry*, second edition, Algorithms and Computation in Mathematics 10, Springer, 2006. Chapters 8–11. https://doi.org/10.1007/3-540-33099-2.