Proof-Carrying Toric Guard Certificates for Positivity of Linear Recurrence Sequences

Luca Blanchi

June 2026

Abstract

We describe a proof-carrying certificate calculus for eventual positivity of real algebraic linear recurrence sequences. After passing to arithmetic progressions, a recurrence is written in dominant torus normal form

$$u_{Mr+s} = \rho_s^r r^{k_s}\big(H_s(z_r, 1/r) + E_s(r)\big), \qquad z_r = \gamma_s^r,$$

where z_r lies in a compact algebraic torus, H_s is a finite asymptotic polynomial, and $E_s(r)$ is exponentially smaller than the dominant part. Positivity is then certified by lower bounds for finitely many toric guard functions along the orbit z_r.

The framework separates three layers. Level A consists of automatic elementary guard modules, including binomial guards, rank-one S-unit guards, selected trinomial guards, products and powers, sums of norms, and dominant amplification. Level B consists of proof-carrying geometric modules, such as finite-zero guards, toric-coset resolved guards, polygon-rigid guards, Lojasiewicz shields, and Gram-positive non-cancellation certificates. Level C records exclusions: arbitrary non-binomial S-unit sums, flexible four-term non-toric zero curves, arbitrary non-cancellation, toric-coset decomposition without proof, and unverified Lojasiewicz constants are not treated as automatic primitives.

The main result is a guarded shield theorem: if a branch carries a finite certificate reducing the leading asymptotic expression to elementary positive terms, certified guard powers, and an error of strictly larger asymptotic weight, then that branch is eventually positive with an effective tail bound. The note should be read as a preliminary certification architecture, not as a solution of the general Positivity Problem. Its boundary deliberately approaches the Skolem barrier and therefore requires explicit proof objects whenever the geometry is not elementary.

Declaration of generative AI and AI-assisted technologies in the writing process

During the preparation of this work, ChatGPT, by OpenAI, was used to assist with mathematical drafting, formalization, review, and editing. This work is shared as a preliminary AI-assisted mathematical note. The mathematical content may have been only partially reviewed and may contain errors; it should not be treated as peer-reviewed or as a fully verified manuscript.

1 Introduction

Let

$$u_n = \sum_{i=1}^{m} P_i(n)\lambda_i^n$$

be a real algebraic linear recurrence sequence, written in exponential-polynomial form over a number field. The Positivity Problem asks whether

$$u_n \geq 0 \qquad \text{for all } n \geq 0.$$

Even deciding eventual positivity becomes delicate when several dominant characteristic roots have equal modulus and non-torsion quotient phases. The hard obstruction is that the orbit of those phases may approach the zero set of a trigonometric polynomial extremely closely; this is also where Skolem-type questions enter.

This note proposes a restricted certification framework. It does not claim to decide positivity in full generality. Instead, it describes a finite proof object which, when present, can be checked mechanically and yields an effective index N such that

$$u_n \geq 0 \qquad (n \geq N).$$

The certificate is built from *toric guards*: algebraic functions on the compact phase torus whose values along the recurrence orbit admit explicit lower bounds except at certified exact hits.

The guiding principle is conservative. Elementary cases are automatic. Geometric cases are accepted only when accompanied by a proof object containing all constants and decompositions needed for verification. Everything else is explicitly outside the automatic calculus.

2 Dominant Torus Normal Form

We begin with the standard decomposition into residue classes and dominant roots.

Definition 2.1 (Dominant branch)**.** *Fix a residue class $n = Mr + s$. A dominant branch consists of data*

$$\rho_s > 0, \qquad k_s \geq 0, \qquad \gamma_s = (\gamma_{s,1}, \ldots, \gamma_{s,d}) \in (S^1)^d$$

and Laurent polynomials $F_{s,j} \in \overline{\mathbb{Q}}[x_1^{\pm 1}, \ldots, x_d^{\pm 1}]$ such that

$$u_{Mr+s} = \rho_s^r r^{k_s} \big(H_s(z_r, 1/r) + E_s(r)\big), \qquad z_r = \gamma_s^r,$$

where

$$H_s(z,t) = F_{s,0}(z) + tF_{s,1}(z) + \cdots + t^{J_s} F_{s,J_s}(z)$$

and

$$|E_s(r)| \leq B_s r^{a_s} \theta_s^r$$

for some effectively given B_s, a_s and $0 < \theta_s < 1$.

The passage to such branches is routine: one separates moduli of characteristic roots, kills torsion in quotient phases by taking arithmetic progressions, and groups conjugate terms so that the resulting expression is real on the orbit. The certificate stores the number field, embeddings, height bounds, and all constants used in the tail estimate.

Remark 2.2. *The exponential error is harmless in the final positivity comparison. The real difficulty is not the non-dominant spectrum, but the possible smallness of the dominant toric expression $H_s(z_r, 1/r)$.*

3 Branches and Spectral Descent

If $F_{s,0}(z_r)$ is bounded below by a positive constant on the orbit closure, the branch is easy. If it vanishes somewhere on the orbit closure, one must descend to the first non-vanishing asymptotic layer. The certificate therefore contains a finite spectral descent tree.

At a node one records:

(i) a toric stratum or certified local chart;

(ii) the active asymptotic polynomial $H(z,t)$;

(iii) a finite set of guards $G_1,\dots,G_q$;

(iv) a shield inequality proving that the active expression is positive away from the guarded exceptional sets;

(v) exact-hit instructions for the cases $G_j(z_r)=0$.

Exact hits are not ignored. They either form finite computable sets, reduce to lower-dimensional branches, or are discharged by a supplied toric-coset certificate. This is the first point at which the framework touches the Skolem boundary: an arbitrary claim that an algebraic torus orbit avoids a hypersurface is not accepted without an explicit proof object.

4 Guards and Shields

Definition 4.1 (Guard)**.** *A guard for a branch is a Laurent polynomial*

$$G \in \overline{\mathbb{Q}}[x_1^{\pm 1},\dots,x_d^{\pm 1}]$$

together with constants $A>0$, $D\ge 0$, and a certified exact-hit set $Z_G\subset\mathbb{N}$, such that for all $r\notin Z_G$,

$$|G(z_r)| \ge A r^{-D}.$$

The exact-hit set may be empty, finite with listed elements, or represented by a lower dimensional recurrence branch. In the last case, verification is delegated to another node of the certificate.

Definition 4.2 (Shield)**.** *A shield for a real-valued asymptotic expression $H(z,t)$ is an inequality on a certified chart of the form*

$$H(z,t) \ge \sum_{\ell=1}^{L} c_\ell t^{p_\ell} \prod_{j=1}^{q} |G_j(z)|^{e_{\ell j}} - Ct^{Q},$$

where $c_\ell>0$, $C\ge 0$, $p_\ell, Q\in\mathbb{Q}_{\ge 0}$, and $e_{\ell j}\in\mathbb{Q}_{\ge 0}$. All coefficients, domains, and constants are part of the proof object.

If $t=1/r$ and each guard satisfies $|G_j(z_r)|\ge A_j r^{-D_j}$, then the ℓ-th positive term is bounded below by

$$c_\ell \prod_j A_j^{e_{\ell j}} r^{-\left(p_\ell+\sum_j e_{\ell j}D_j\right)}.$$

Thus a shield is effective whenever at least one positive term has weight

$$p_\ell + \sum_j e_{\ell j} D_j < Q.$$

5 Soundness

Theorem 5.1 (Guarded shield soundness)**.** *Consider one dominant branch in normal form. Suppose it carries a finite certificate consisting of guard lower bounds, exact-hit resolutions, and a shield inequality whose minimum positive weight is strictly smaller than the negative error weight Q. Then there is an effectively computable R such that*

$$H(z_r, 1/r) + E(r) \geq 0 \qquad (r \geq R)$$

on that branch. Consequently $u_{Mr+s} \geq 0$ for all $r \geq R$.

Proof. For r outside the exact-hit sets, substitute the guard lower bounds into the shield. Let

$$\omega_\ell = p_\ell + \sum_j e_{\ell j} D_j$$

and choose ℓ_0 with $\omega_{\ell_0} < Q$. Then

$$H(z_r, 1/r) \geq C_0 r^{-\omega_{\ell_0}} - C r^{-Q}$$

for an explicit $C_0 > 0$, after discarding the other non-negative shield terms. Since $\omega_{\ell_0} < Q$, the right side is positive for all sufficiently large r. The exponential error $E(r)$ is smaller than any fixed negative power of r beyond an effective threshold, so it is absorbed by halving C_0. Exact hits are handled by the descendant nodes listed in the certificate. The tree is finite, hence the maximum of the branch thresholds is effective. □

6 Level A: Automatic Elementary Guard Modules

Level A contains guard families whose verification uses standard explicit algebraic-number estimates and elementary reductions.

6.1 Binomial Guards

For

$$G(z) = az^\mu - bz^\nu$$

with $a, b \in \overline{\mathbb{Q}}^\times$, the guard inequality follows from lower bounds for a non-zero linear form in logarithms unless the ratio a/b is exactly attained by $\gamma^{r(\nu-\mu)}$. Torsion cases are separated by the residue-class modulus M, and exact hits are listed or passed to a lower-dimensional branch.

6.2 Rank-One S-Unit Guards

When all phases are powers of one algebraic unit phase, a guard becomes a one-variable S-unit expression. The automatic module accepts only the cases with a supplied factorization into binomial and monomial factors, or with a univariate root-separation certificate proving the required lower bound along the orbit.

6.3 Trinomial Guards

Selected trinomials are automatic when their Newton polygon and coefficient data imply a rigid separation from zero along the orbit, or when they reduce to a certified univariate problem. A typical model is

$$G(z, w) = 1 + z + w.$$

The module accepts the guard if the certificate proves that exact solutions of

$$1 + \gamma_1^r + \gamma_2^r = 0$$

are exhausted and that the remaining values have an explicit inverse-polynomial lower bound.

6.4 Products, Powers, and Sums of Norms

If G_i are guards, then products and powers give new guards with additive exponents. Also, if

$$N(z) = \sum_{i=1}^{q} |G_i(z)|^2,$$

then $N(z_r)$ is guarded whenever at least one $G_i(z_r)$ is guarded away from zero on the active chart. This module is useful for Gram-positive non-cancellation certificates.

6.5 Dominant Amplification

If a positive term dominates all uncertain terms by a certified power gap, the branch closes automatically. This is the common case in which the recurrence has a unique positive real dominant root, or a positive definite dominant envelope.

7 Level B: Proof-Carrying Geometric Modules

Level B modules are not automatic theorems invoked by name. They are formats for checkable proof objects.

7.1 Finite-Zero Guards

A finite-zero guard contains an ideal or resultant computation proving that the intersection of the orbit closure with $G = 0$ consists of finitely many torsion cosets, plus a list of the residue classes producing exact hits. The checker verifies the algebraic decomposition and then delegates each exact-hit class.

7.2 Toric-Coset Resolved Guards

For a hypersurface in a torus, a toric-coset resolved guard supplies a decomposition into torsion cosets and residual components, with explicit equations. The certificate is accepted only if the decomposition is independently checkable and if each residual component carries a lower-bound proof or is irrelevant to the orbit closure.

7.3 Polygon-Rigid Guards

Some sparse Laurent polynomials have Newton polygons forcing rigidity of possible small values along a one-parameter torus orbit. A polygon-rigid certificate records the polygon, the active faces, the excluded balancing relations, and the resulting lower-bound constants.

7.4 Lojasiewicz Shields

A Lojasiewicz shield gives a local inequality comparing a non-negative analytic expression to powers of defining equations for its zero set. The exponent and constant must be part of the certificate, together with a cover of the relevant compact chart. The framework does not infer these constants automatically.

7.5 Gram-Positive Non-Cancellation

When the leading expression can be written as

$$v(z)^* A(z) v(z)$$

with a positive semidefinite Gram matrix on the active chart, the certificate records the Gram factorization and the residual kernel conditions. Positivity is accepted only after all possible kernel intersections are resolved by guards or descendant nodes.

8 Level C: Exclusions and External Modules

The following are deliberately excluded from the automatic calculus:

(i) arbitrary non-binomial S-unit sums;

(ii) flexible four-term non-toric zero curves;

(iii) arbitrary non-cancellation among dominant phases;

(iv) toric-coset decomposition without a proof object;

(v) unverified Lojasiewicz constants;

(vi) any step equivalent to deciding a general Skolem instance.

Such inputs may still appear as *external modules*, but then the certificate must contain a separately checkable proof or a trusted reference implementation with reproducible output. The distinction is important: the framework is a checker of supplied certificates, not an oracle for all toric orbit intersections.

9 Guarded Shield Theorem

Theorem 9.1 (Eventual positivity from proof-carrying guards)**.** *Let u_n be a real algebraic linear recurrence sequence. Suppose that after passing to finitely many residue classes, every dominant branch admits a finite proof-carrying toric guard certificate whose shields have a strict positive weight gap over all negative and error terms. Then u_n is eventually positive. Moreover, the certificate determines an explicit N such that*

$$u_n \geq 0 \qquad (n \geq N).$$

Proof. Apply the guarded shield soundness theorem to each residue class s. Let R_s be the resulting bound for r. Then

$$N = \max_s (MR_s + s)$$

is effective. Since the prefactor $\rho_s^r r^{k_s}$ is positive, the sign is controlled by the certified branch expression. □

10 Automatic Closure Theorem

Theorem 10.1 (Level A closure)**.** *If every guard and every shield in the branch certificate is built using only Level A modules and all exact-hit sets are finite and listed, then the certificate is checkable by algebraic-number arithmetic, root separation, finite residue-class enumeration, and explicit linear-form lower bounds.*

Proof. Level A operations are closed under multiplication, powers, finite sums of squared norms, and finite branching. Binomial and rank-one lower bounds reduce to standard algebraic-number separation and linear forms in logarithms. Listed exact hits are checked by direct substitution. Therefore the verifier needs no geometric decomposition beyond the data stored in the certificate. □

11 Bounded Proof-Carrying Verification

A practical verifier need only implement the following checks:

(1) validate the recurrence-to-branch normal form and the exponential tail bound;

(2) verify each guard lower bound and exact-hit resolver;

(3) verify each shield inequality on its declared compact chart;

(4) compute the asymptotic weights and check the strict gap;

(5) recursively discharge descendant branches;

(6) combine the finite branch thresholds into a global tail bound.

The checker is therefore small compared with the mathematics used to discover a certificate. Discovery may use symbolic computation, numerical experimentation, tropical geometry, or external theorem proving. Verification should remain deterministic and auditable.

12 Worked Example: A Trinomial Guard

Consider a branch whose leading obstruction is

$$G(z, w) = 1 + z + w, \qquad z = \alpha^r, \quad w = \beta^r,$$

with α, β algebraic unit phases. Suppose the certificate proves:

(i) the exact solutions of $1 + \alpha^r + \beta^r = 0$ occur only in a listed finite set Z;

(ii) for $r \notin Z$,

$$|1 + \alpha^r + \beta^r| \geq A r^{-D};$$

(iii) the active asymptotic expression satisfies

$$H(z, w, t) \geq c|1 + z + w|^2 - Ct^Q$$

on the relevant chart.

Then outside Z,

$$H(\alpha^r, \beta^r, 1/r) \geq cA^2 r^{-2D} - Cr^{-Q}.$$

If $2D < Q$, this branch is eventually non-negative. The exact-hit values in Z are checked directly or sent to descendant branches. This example illustrates the preferred style of certificate: the difficult Diophantine statement is isolated as a guard, and the positivity argument is a transparent weight comparison.

13 Applications

13.1 Unbounded-Order Families

The calculus applies naturally to families of unbounded recurrence order when the dominant phase geometry remains sparse. For instance, products of independent binomial guards may certify families with many conjugate dominant roots, provided the shield has a uniform weight gap.

13.2 Sums of Norms

Expressions of the form

$$H(z, t) = \sum_i c_i(t)|G_i(z)|^2 + \text{higher-order terms}$$

are well suited to the framework. Once the common zero set of the G_i is resolved, positivity follows from norm guards and the higher-order comparison.

13.3 Toric-Coset Resolved Examples

Some non-binomial examples become tractable after resolving the zero set into toric cosets. The certificate records the decomposition and assigns to each coset either a lower-dimensional branch or a proof that the orbit misses it with an explicit lower bound.

13.4 Hybrid Cone Certificates

The toric guard calculus can be combined with contracted cone certificates. A cone certificate may prove that an iterate enters a positive invariant cone, while toric guards certify the finitely many boundary modes that prevent uniform contraction.

14 Robust Negative Certificates

The same branch normal form can certify eventual negativity or infinitely many negative values in restricted settings. If a shield proves

$$H(z_r, 1/r) \leq -cr^{-\omega} + Cr^{-Q}$$

with $\omega < Q$, then the branch is eventually negative. More subtly, if the orbit is dense in a toric component on which the leading term is negative on a certified open set, then negative values occur infinitely often. This latter statement requires effective recurrence to the open set and is therefore treated as an external module unless the torus dynamics are elementary.

15 Relation to Prior Work

The framework is inspired by known reductions of positivity and ultimate positivity for linear recurrence sequences to the geometry of dominant phases and by certificate-based approaches to proving positivity. It also borrows the philosophy of separating discovery from verification: a difficult algebraic or Diophantine computation may be used to find a certificate, but the final proof object should expose only checkable claims.

Linear forms in logarithms provide the model for binomial guards. S-unit results explain why arbitrary sparse sums quickly become hard. Toric geometry enters through orbit closures, torsion cosets, and sparse polynomial zero sets. Contracted cone methods offer a complementary route when positivity can be made invariant under a linear action.

16 Limitations

This note does not solve the Positivity Problem for general linear recurrence sequences. It also does not provide an automatic algorithm for arbitrary toric orbit-hypersurface intersections. In particular, the following remain outside the present automatic scope:

general Skolem instances, arbitrary S-unit cancellations, and unstructured non-cancellation.

The intended claim is narrower: when the relevant small-value phenomena can be expressed by certified guards and shields with explicit constants, eventual positivity follows by a short and checkable argument.

17 Conclusion

Proof-carrying toric guards give a modular way to certify positivity of linear recurrence sequences near the natural Skolem boundary. The calculus is useful precisely because it is explicit about what it can check automatically and what must be supplied as proof data. In favorable sparse or geometrically rigid cases, the certificate reduces eventual positivity to finite algebraic verification and a final asymptotic weight comparison.

A Relative Guard Certificates

A relative guard may depend on another guard. For example, one may prove

$$|G_2(z_r)| \geq Ar^{-D}$$

only on the region where $G_1(z_r) \neq 0$ and $|G_1(z_r)| \leq r^{-B}$. Such guards are accepted if the certificate records the region, the implication, and the exact-hit resolver for G_1. This allows local desingularization without requiring one global lower bound for every function.

B Perturbation Stability

If a branch has a strict shield gap, then sufficiently small algebraic perturbations of lower-order coefficients preserve eventual positivity after possibly increasing the tail bound. The certificate can record explicit perturbation radii by reducing the shield constant c_ℓ and increasing the error constant C. This is useful for families rather than isolated recurrences.

C Conjectural Extensions

One may hope for broader automatic modules for sparse four-term guards, effective toric stratification, and certified Lojasiewicz exponents. Any such extension should preserve the proof-carrying discipline: the checker should verify explicit constants and decompositions, not rely on an unbounded geometric search hidden inside a black box.

References

[1] A. Baker and G. Wuestholz. *Logarithmic Forms and Diophantine Geometry.* Cambridge University Press, 2007.

[2] P. Bacik. Positivity certificates for linear recurrences. Preprint, 2023.

[3] T. Bogart, A. N. Jensen, D. Speyer, B. Sturmfels, and R. R. Thomas. Computing tropical varieties. *Journal of Symbolic Computation* 42 (2007), 54–73.

[4] D. Eisenbud and B. Sturmfels. Binomial ideals. *Duke Mathematical Journal* 84 (1996), 1–45.

[5] G. Everest, A. van der Poorten, I. Shparlinski, and T. Ward. *Recurrence Sequences.* American Mathematical Society, 2003.

[6] J.-H. Evertse, H. P. Schlickewei, and W. M. Schmidt. Linear equations in variables which lie in a multiplicative group. *Annals of Mathematics* 155 (2002), 807–836.

[7] Y. Ibrahim and B. Salvy. Positivity proofs for linear recurrences through contracted cones. Preprint, 2024.

[8] M. Mignotte, T. N. Shorey, and R. Tijdeman. The distance between terms of an algebraic recurrence sequence. *Journal fur die reine und angewandte Mathematik* 349 (1984), 63–76.

[9] J. Ouaknine and J. Worrell. Positivity problems for low-order linear recurrence sequences. In *Proceedings of SODA 2014*, 366–379.

[10] J. Ouaknine and J. Worrell. Ultimate positivity is decidable for simple linear recurrence sequences. In *Proceedings of ICALP 2014*, 330–341.

[11] N. K. Vereshchagin. Occurrence of zero in a linear recursive sequence. *Mathematical Notes* 38 (1985), 609–615.