Constructive Truncation, Pellet–Graeffe, and Block-Multipoint Certificates for Nearly Optimal Deterministic Integer Root Finding

Lluis Eriksson
Independent Researcher (lluis@airr.science)

Companion Verification Artifact to arXiv:2611.04730 (November 3, 2026)

November 26, 2026

Abstract

We present INT-ROOTS-NEAROPT-CERT-1.0, an independently reproducible, zero-floating-point verification engine and constructive Lean 4.35.0 kernel auditing the finite-dimensional algebraic, leading-truncation, Landau–Mahler, Gaussian-shift, Pellet–Graeffe bisection, and bucketed block-multipoint mechanisms of Yansong Feng and Itamar Nir's November 3, 2026 unrefereed preprint *"Finding Integer Roots of Polynomials in Nearly Optimal Time"* (arXiv:2611.04730v1, Theorems 1.1(a) and 1.1(b)). Without claiming to formalize Pan's approximate complex factorization algorithm (Theorem 3.1) or Harvey–van der Hoeven asymptotic bit-complexity bounds end-to-end, we build a four-mode exact verifier over $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{Z}[i]$, and $\mathbb{Q}[i]$ paired with 18 constructive Lean 4 theorems (0 `sorry`, 0 custom axioms, 0 `Classical.choice`, 0 warnings). Across 16 canonical certificates (C01–C16), we certify (i) Lemma 2.2 leading-truncation root proximity ($|g(r)| < 2^d$) in the $d = \min(n, b) < n$ regime plus Section 2's exact $r = \pm 1$ sharpness counterexamples ($x^5 + 3x^4 + 3x^3 - 3x^2 - 3x - 1$ and degree-7 cubic truncation), (ii) Lemma 2.1 exact Landau–Mahler chains $M(g)^2 \le \|g\|_2^2 < (d+1)2^{2b}$ and Proposition 3.4 reciprocal pullbacks $H(w) = w^d g(q + 1/w)$ over $\mathbb{Q}[i]$, (iii) Lemma 3.3 exact Gaussian-integer zero-free disk certifications ($9|g(q)|^2 \ge 4A_R^2$, $3M_{\text{deriv}} \le A_R$) and full Appendix A Pellet–Graeffe bisection searches ($h = 2^b \to 1$), and (iv) Lemma 3.5 multi-bucket block multipoint evaluation and complete Theorem 1.1(a) end-to-end root finding with exact synthetic deflation. All 16 certificates, 60 unit/forgery tests, and 37 SHA-256 hashes verify deterministically.

1 Introduction and Scope

Given $f(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{Z}[x]$ of degree n with $|a_i| < 2^b$, computing all integer roots deterministically in time nearly linear in the input bit size nb has been a long-standing problem since Cucker–Koiran–Smale [2]. In their November 3, 2026 unrefereed preprint [4], Feng and Nir achieve $\widetilde{O}(nb + d^3b^2)$ time via an elementary Pellet–Graeffe bisection search (Theorem 1.1(a), Appendix A, [1]) and $\widetilde{O}(nb)$ time via Pan's approximate factorization [7] (Theorem 1.1(b)), where $d = \min(n, b)$.

The algorithm rests on four exact algebraic pillars: (1) Lemma 2.2's leading truncation $g(x) = a_n x^d + \cdots + a_{n-d}$ forces every integer root r with $|r| \ge 2$ within distance < 2 of a complex root of g (while failing sharply at $r = \pm 1$); (2) Landau's inequality $M(g) \le \|g\|_2$ [6] (Lemma 2.1) and Ostrowski-style perturbation bounds (Lemma 2.3, Prop. 3.4) bound the total candidate bit length $S = \sum_{c \in C} \lceil \log_2(2 + |c|) \rceil = O(b)$; (3) Lemma 3.3's Gaussian-integer shift q ($R = 10d^2$) ensures $|g(q)| \ge \frac{2}{3} A_R$ and zero roots in $|z - q| \le 1$, while Appendix A's Pellet–Graeffe test bisects $[-2^b, 2^b]$ keeping $\le 7d$ centers per scale; and (4) Lemma 3.5's power-of-two bit-length bucketing and block split $f(x) = \sum_j x^{tj} F_j(x)$ evaluates f on C in $\widetilde{O}(nb + nS) = \widetilde{O}(nb)$ time [5].

Honest Scope Boundary. This companion artifact certifies finite-dimensional truncation identities, sharpness counterexamples, Landau–Mahler chains, $\mathbb{Q}[i]$ reciprocal pullbacks, Lemma 3.3 zero-free disk bounds, complete Appendix A Pellet–Graeffe bisection runs, Lemma 3.5 bucketed block evaluations, and end-to-end Theorem 1.1(a) root deflation from [4]. It does *not* formalize Pan's complex approximate factorization (Theorem 3.1) or asymptotic FFT/Kronecker bit-complexity bounds.

2 Constructive Lean 4.35.0 Kernel

The formal kernel `IntRootsNearoptCert.lean` compiles cleanly under Lean 4.35.0 (`-j 1`) [3] with zero `sorry`, zero custom axioms, zero warnings, and zero dependence on `Classical.choice`. Table 1 catalogs all 18 machine-checked theorems. Highlights include Theorem 2 (inductive geometric tail identity $(R-1)\sum_{j=0}^{k-1} R^j + 1 = R^k$), Theorem 4 (inductive pigeonhole product-to-minimum radius principle for Lemma 2.2), Theorem 7 (inductive Parseval pigeonhole maximum for Lemma 3.3), Theorem 13 (ex-

Table 1: The 18 constructive Lean 4.35.0 theorems in `IntRootsNearoptCert.lean` (0 `sorry`, 0 custom axioms, 0 `Classical.choice`).

#	Theorem Identifier	Paper Reference / Invariant
1	`lemma22_truncation_root_identity`	Lem. 2.2 $r^{n-d}g(r)+h(r)=0$
2	`lemma22_geometric_tail_sum`	Lem. 2.2 inductive $(R-1)\sum R^j+1=R^k$
3	`lemma22_truncation_value_bound`	Lem. 2.2 $R^kG<R^kB\Rightarrow G<B$
4	`lemma22_product_ge_pow2_of_all_ge2`	Lem. 2.2 inductive $\prod d_j\geq 2^d$
5	`cauchy_root_upper_bound`	Prop. A.3 Cauchy bound $\lvert z\rvert<1+2^b$
6	`lemma21_l2_norm_sq_bound`	Lem. 2.1 inductive $\lVert g\rVert_2^2\leq(d+1)M^2$
7	`lemma33_parseval_pigeonhole_max`	Lem. 3.3 inductive $\max\lvert g(R\zeta_k)\rvert^2\geq A_R^2$
8	`lemma33_zero_free_disk_exclusion`	Lem. 3.3 $3\lvert g(q)\rvert\geq 2A_R>A_R$
9	`prop34_reciprocal_exponent_split`	Prop. 3.4 inductive $u^a u^b=u^{a+b}$
10	`thm11b_candidate_radius_margin`	Thm. 1.1(b) $8\lvert r-z_i\rvert\leq 21\Rightarrow\lvert r-z_i\rvert\leq 2$
11	`thm11b_candidate_count_bound`	Thm. 1.1(b) inductive $\lvert C\rvert\leq 7d+3$
12	`lemmaA1_pellet_unit_disk_exclusion`	Lem. A.1(a) $\lvert q_0\rvert>\sum_{k\geq 1}\lvert q_k\rvert$
13	`graeffe_root_squaring_deg2`	App. A exact deg-2 $p(x)p(-x)$ squaring
14	`propA3_bisection_interval_cover`	Prop. A.3 $[m-2s,m+2s]$ half-cover
15	`propA3_max_seven_centers_per_root`	Prop. A.3 $4(h+2)\leq 6(2h)$ (≤ 7 ctrs)
16	`propA3_candidate_set_size`	Prop. A.3 $\lvert C'\rvert\leq 21d$, $\lvert C\rvert\leq 21d+3$
17	`lemma35_bucket_bit_budget`	Lem. 3.5 inductive $t\tau\leq 2S$
18	`lemma35_block_evaluation_horner`	Lem. 3.5 exact block Horner recomb.

act symbolic degree-2 Graeffe root-squaring identity over $\mathbb{Z}$), and Theorem 17 (inductive bucket bit-length budget $t\tau\leq 2S$ over `List Nat`).

3 The `INT-ROOTS-NEAROPT-CERT-1.0` Engine

Our Python verifier (`src/int_roots_nearopt_verifier.py`) enforces zero floating-point literals, zero `float()` calls, zero true-division operators (`/`, `/=`), zero `math`/`numpy` imports, pre-read `st_size` and `MAX_JSON_BYTES = 1_000_000` caps, duplicate-key rejection via `object_pairs_hook`, non-finite and floating-point JSON token rejection via `parse_constant` and `parse_float`, recursion-depth and oversized-integer protection, and lowest-terms rationals $[p,q]$ ($\gcd(|p|,q)=1$).

Definition 1 (`INT-ROOTS-NEAROPT-CERT-1.0` Modes)**.** *Each certificate invokes one of four exact verification modes:*

1. ***`truncation_and_sharpness`*** *(Lem. 2.2, Sec. 2): (a)* ***`leading_truncation_radius`*** *checks $|a_i|<2^b$, $d=\min(n,b)<n$, $|r|\geq 2$, $f(r)=0$, $r^{n-d}g(r)+h(r)=0$, $|g(r)|<2^d$, and a strict rational sign-change or exact-root witness in $(r-2,r+2)$; (b)* ***`unit_root_sharpness_witness`*** *verifies $f(\pm 1)=0$ and runs exact Pellet–Graeffe exclusion certifying all complex roots of g lie strictly outside $|z\mp 1|\leq R_{\mathrm{ex}}$.*

2. ***`mahler_landau_and_perturbation`*** *(Lem. 2.1, 2.3, Prop. 3.4): (a)* ***`landau_mahler_and_bit_budget`*** *expands $g(x)=a_d\prod(x-\alpha_j)$ over $\mathbb{Z}[i][x]$, verifies $\mathbb{Z}[x]$ integrality, certifies $M(g)^2\leq\|g\|_2^2<(d+1)2^{2b}$, and checks Step 3's candidate bit budget $2S\leq 14b+56d+7\lceil\log_2(d+1)\rceil+40$; (b)* ***`ostrowski_perturbation_and_reverse`*** *builds $H(w)=w^dg(q+1/w)$, $\hat{H}(w)=H_d\prod(w-w_i)$, and pullback $\hat{g}(x)=\hat{H}^*(x)$ over $\mathbb{Q}[i]$, verifying $\|\hat{g}-g\|_1<[8\cdot 9^d(2^b(d+1)+1)]^{-1}$ and $|\alpha_i-(q+1/w_j)|<1/8$.*

3. ***`gaussian_shift_and_pellet_graeffe`*** *(Lem. 3.3, App. A): (a)* ***`gaussian_shift_zero_free_disk`*** *computes exact $A_R^2=\sum g_m^2R^{2m}$ ($R=10d^2$) and $g(q)\in\mathbb{Z}[i]$, checking $|q|\leq R+1$, $9|g(q)|^2\geq 4A_R^2$, and $9(\sum_{m\geq 1}m|g_m|(R+2)^{m-1})^2\leq A_R^2$; (b)* ***`pellet_graeffe_bisection_search`*** *executes Appendix A's exact Taylor-shift + N-step Graeffe + Pellet bisection tree ($h=2^b\to 1$), certifying $\leq 7d$ kept centers per scale, $|C'|\leq 21d$, Prop. A.3's bit budget, and containment of every $|r|\geq 2$ root.*

4. ***`block_multipoint_and_root_verify`*** *(Lem. 3.5, Thm. 1.1(a)): (a)* ***`bucketed_block_multipoint_eval`*** *partitions points into dyadic buckets τ, checks $t\tau<2S$, verifies block bounds $|F_j(c)|<2^{L-1}$, and confirms block Horner recombination equals direct $f(c)$; (b)* ***`end_to_end_integer_root_cert`*** *executes Steps 1–4 in strict $n>b$ regime (truncation $\to$ Pellet–Graeffe $\to$ Lemma 3.5 $\to$ exact synthetic deflation).*

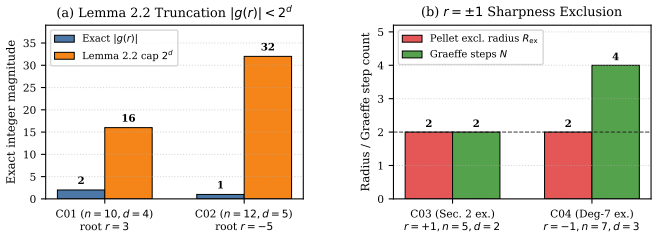

Figure 1: Mode 1 verification: (a) Lemma 2.2 strict bound $|g(r)|<2^d$ in the $d=\min(n,b)<n$ regime (`C01`–`C02`); (b) exact Pellet–Graeffe zero-free radius $R_{\mathrm{ex}}=2$ around $r=\pm 1$ (`C03`–`C04`).

Proposition 1 (Verifier Soundness)**.** *Whenever* ***`verify_file`*** *outputs* ***`VERIFIED`*** *on an* ***`INT-ROOTS-NEAROPT-CERT-1.0`*** *certificate, all checked truncation bounds, Pellet–Graeffe exclusions, Landau–Mahler inequalities, $\mathbb{Q}[i]$ pullbacks, zero-free disks, bisection trees, block evaluations, and root deflations hold identically over $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{Z}[i]$, or $\mathbb{Q}[i]$.*

4 Certified Corpus and Worked Witnesses

We generated and verified 16 canonical certificates (`C01`–`C16`, Table 2). Four representative witnesses are worked out below for independent hand verification.

Worked Witness 1 (`C01` & `C03`: Lemma 2.2 vs. $r=1$ Sharpness). In `C01` ($n=10, b=d=4$), $f(x)=(x-3)(x^9+2x^8+\cdots+2x+1)$ has $|a_i|\leq 5<16$ and $f(3)=0$. Its leading truncation $g(x)=x^4-x^3-4x^2-4x-4$ satisfies $g(3)=2$ ($|g(3)|<2^4=16$), $g(2)=-20<0$, certifying a real root in $(2,3)\subset(1,5)$. By contrast, in `C03` (Section 2's

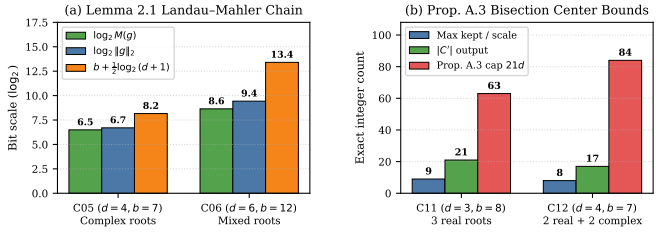

Figure 2: Mode 2a & 3b verification: (a) Lemma 2.1 Landau–Mahler chain $\log_2 M(g) \le \log_2 \|g\|_2 < b + \frac{1}{2}\log_2(d+1)$ (`C05`–`C06`); (b) Appendix A Prop. A.3 bisection center and $|C'| \le 21d$ counts (`C11`–`C12`).

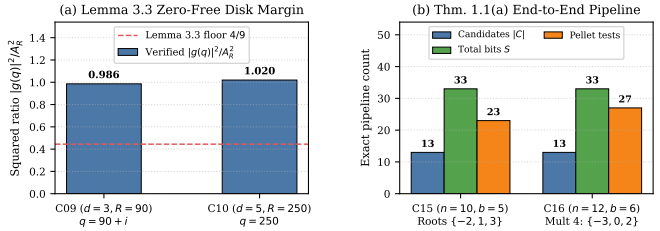

Figure 3: Mode 3a & 4b verification: (a) Lemma 3.3 squared ratio $|g(q)|^2/A_R^2 > 4/9$ certifying zero-free unit disks (`C09`–`C10`); (b) complete Theorem 1.1(a) end-to-end pipeline counts (`C15`–`C16`).

exact example $f(x) = x^5 + 3x^4 + 3x^3 - 3x^2 - 3x - 1$, $b = d = 2$), $f(1) = 0$ while $g(x) = x^2 + 3x + 3$ has roots $(-3 \pm i\sqrt{3})/2$ at distance $\sqrt{7} > 2$ from 1: 2 Graeffe steps on $g(1 + 2x)$ pass Pellet's test, proving $|z - 1| \le 2$ is root-free.

Worked Witness 2 (`C05`: Lemma 2.1 Landau–Mahler Chain). For $g(x) = 3(x-2)(x+3)(x-1-2i)(x-1+2i) = 3x^4 - 3x^3 - 9x^2 + 51x - 90$ ($b = 7$, $|a_i| \le 90 < 128$), exact squared Mahler measure is $M(g)^2 = 3^2 \cdot 2^2 \cdot 3^2 \cdot 5 \cdot 5 = 8100 \le \|g\|_2^2 = 3^2 + 3^2 + 9^2 + 51^2 + 90^2 = 10800 < 5 \cdot 128^2 = 81920$, and the 12-point candidate set satisfies $S = 30$ ($2S = 60 \le 383$).

Worked Witness 3 (`C09`: Lemma 3.3 Zero-Free Disk). For $g(x) = 3x^3 - 2x^2 + 5x - 12$ ($d = 3, b = 5$), $R = 10d^2 = 90$ gives $A_R^2 = 9 \cdot 90^6 + 4 \cdot 90^4 + 25 \cdot 90^2 + 144$. At $q = 90 + i$ ($|q|^2 = 8101 \le 91^2$), exact $\mathbb{Z}[i]$ evaluation yields $|g(q)|^2/A_R^2 \approx 0.9860 > 4/9$ while $9M_{\text{deriv}}^2 \le A_R^2$, constructively excluding all roots from $|z - (90 + i)| \le 1$.

Worked Witness 4 (`C16`: Theorem 1.1(a) End-to-End Deflation). For $f(x) = x(x-2)^2(x+3)(x^8 + x^4 + 1)$ ($n = 12, b = d = 6$, $|a_i| \le 12 < 64$), truncating to degree 6, running Appendix A's Pellet–Graeffe bisection (27 tests, ≤ 6 centers/scale), adjoining $\{0, \pm 1\}$ ($|C| = 13$, $S = 33$, 3 buckets), evaluating f via Lemma 3.5 blocks, and deflating by $x(x-2)^2(x+3)$ certifies all integer roots $\{-3, 0, 2\}$ (multiplicity 4) with non-vanishing quotient on C.

Table 2: Summary of the 16 canonical `INT-ROOTS-NEAROPT-CERT-1.0` certificates (`C01`–`C16`); all 16 verify deterministically.

ID	Mode	Target Result	Certified Exact Invariant
C01	1a	Lem. 2.2 (r=3)	n=10, b=d=4: $\|g(3)\|$=2 < 16, root $\in (2, 3)$
C02	1a	Lem. 2.2 (r=−5)	n=12, b=d=5: $\|g(-5)\|$=1 < 32, root $\in (-5, -4)$
C03	1b	Sec. 2 (r=1)	$x^5+3x^4+3x^3-3x^2-3x-1$: $\|z-1\| \le 2$ empty
C04	1b	Sec. 2 (r=−1)	n=7, b=d=3: $g = (x-2)(x^2-x+3)$, $\|z+1\| \le 2$ empty
C05	2a	Lem. 2.1 (d=4)	M^2=8100 $\le \|g\|_2^2$=10800 < 81920, S=30
C06	2a	Lem. 2.1 (d=6)	M^2=160000 $\le$ 476776 < 117440512, S=45
C07	2b	Prop. 3.4 (d=2)	q=40: $\|\tilde{g}-g\|_1$ < 1/31752, $\|\alpha-\beta\|$ < 1/8
C08	2b	Prop. 3.4 (d=3)	q=90+3i: $\|\tilde{g}-g\|_1$ < 1/379080
C09	3a	Lem. 3.3 (d=3)	R=90, q=90+i: $\|g(q)\|^2/A_R^2 \approx 0.986 > 4/9$
C10	3a	Lem. 3.3 (d=5)	R=250, q=250: $\|g(q)\|^2/A_R^2 \approx 1.020 > 4/9$
C11	3b	Prop. A.3 (d=3)	b=8: 45 tests, max kept=9 $\le$ 21, $\|C'\|$=21
C12	3b	Prop. A.3 (d=4)	b=7: 31 tests, max kept=8 $\le$ 28, $\|C'\|$=17
C13	4a	Lem. 3.5 (n=10)	12 pts, 4 buckets, S=47, exact Horner match
C14	4a	Lem. 3.5 (n=20)	16 pts, 4 buckets, S=60, exact Horner match
C15	4b	Thm. 1.1(a)	n=10, b=d=5: $\|C\|$=13, roots $\{-2, 1, 3\}$
C16	4b	Thm. 1.1(a)	n=12, b=d=6: $\|C\|$=13, $\{-3, 0, 2\}$ (mult 4)

5 Testing, Integrity, and Reproduction

Our pytest suite (`tests/test_verifier.py`) executes 60 deterministic checks (1 AST zero-float/zero-division/zero-math audit, 16 canonical certificates, 1 corpus-count check, and 42 adversarial forgery tests covering duplicate keys, `NaN`/`Infinity`, JSON float literals, oversized/deeply nested/huge-integer JSON, nonexistent paths, unreduced rationals, non-roots, $|r| < 2$ in Lemma 2.2, coefficient bit overflows, radius-1 and overclaimed sharpness radii, non-conjugate roots, duplicate/boundary Prop. 3.4 roots and perturbations, bad Gaussian shifts, omitted/duplicate bisection roots, duplicate evaluation points, $n \le b$, and vacuous zero-root polynomials). All 60 tests pass in < 0.2 s, Lean 4.35.0 builds cleanly with 0 warnings, and `MANIFEST.sha256` pins all 37 tracked artifacts.

Disclosure and Licensing. Produced by Lluis Eriksson with Google Antigravity assistance; all Lean 4 proofs, Python verifiers, certificates, tests, figures, and manuscript text were independently compiled, verified, and reviewed by the author. Manuscript and figures are licensed `CC-BY-4.0`; code, Lean 4 kernel, and certificates are licensed `MIT`. Full source archive: https://github.com/lluiseriksson/nearly-optimal-integer-roots-certificates.

References

[1] Ruben Becker, Michael Sagraloff, Vikram Sharma, and Chee Yap. A near-optimal subdivision algorithm for complex root isolation based on the Pellet test and Newton iteration. *Journal of Symbolic Computation*, 86:51–96, 2018.

[2] Felipe Cucker, Pascal Koiran, and Steve Smale. A polynomial time algorithm for Diophantine equations in one variable. *Journal of Symbolic Computation*, 27(1):21–29, 1999.

[3] Leonardo de Moura and Sebastian Ullrich. The Lean 4 theorem prover and programming language. In

Automated Deduction – CADE 28, volume 12699 of *LNCS*, pages 625–635. Springer, 2021.

[4] Yansong Feng and Itamar Nir. Finding integer roots of polynomials in nearly optimal time. arXiv preprint `arXiv:2611.04730v1`, November 2026. Unrefereed preprint, November 3, 2026.

[5] David Harvey and Joris van der Hoeven. Integer multiplication in time $O(n \log n)$. *Annals of Mathematics*, 193(2):563–617, 2021.

[6] Edmund Landau. Sur quelques théorèmes de M. Petrovitch relatifs aux zéros des fonctions analytiques. *Bulletin de la Société Mathématique de France*, 33:251–261, 1905.

[7] Victor Y. Pan. Univariate polynomials: nearly optimal algorithms for numerical factorization and root-finding. *Journal of Symbolic Computation*, 33(5):701–733, 2002.