One Engine, Three Counts

Descartes, Sturm and Budan–Fourier through one sign-variation engine in Lean 4

Carles Marín*
Independent researcher
karlesmarin@gmail.com

June 2026

Abstract

Three classical theorems count the real roots of a polynomial in an interval by reading sign variations of a sequence: *Descartes'* rule uses the coefficients, *Budan–Fourier* the derivative tower $p, p', p'', \ldots$, and *Sturm* the signed-remainder chain. That they are facets of one principle is classical (Akritas [5]; Basu–Pollack–Roy [7]), and the deepest unifying invariant, the Cauchy index, is axiomatised through abstract *Sturm chains* by Eisermann [8] and machine-checked, for the Cauchy-index route, in Isabelle/HOL by Li and Paulson [10]. This paper does three things in Lean 4 over Mathlib, all `sorry`-free. (1) It exhibits *one engine*—a sign-variation count, its local constancy off critical points, and a global telescoping over them—and runs all three theorems through it: the first Lean formalizations of Sturm's theorem [13] and the Budan–Fourier theorem [14], and the bridge `fourierVar p 0 = Polynomial.signVariations p` identifying the engine's $V(0)$ with the coefficient sign count of Mathlib's own Descartes' rule, so the third count too is checked against the library and not merely read off in prose. (2) It states their common local-drop law, $V(c^-) = V(c^+) + \mu_c + 2e$, where μ_c is the order to which the counted polynomial vanishes at the critical point c. (3) It locates precisely where the three diverge: Eisermann's Sturm-chain axiom forbids two consecutive members from vanishing together, and the derivative tower *violates* this at every multiple root, so the tower is *not* a Sturm chain—its local law is the block collapse/alternation (`Rseq`/`Lseq`), of which the antipodal single-drop of a genuine Sturm chain is the non-degenerate special case. The unification is classical; the contribution is the shared Lean engine, the two first-in-Lean formalizations it carries, the Descartes bridge to Mathlib's coefficient count, and this exact axiomatic placement of the tower. Every headline theorem depends only on `propext`, `Classical.choice`, `Quot.sound`.

Three theorems, born a century and a half apart, count real roots by the same gesture: reading the signs of a sequence. Descartes (1637) read them off the *coefficients* and bounded the positive roots. Budan (1807) and Fourier (1820s, published posthumously in 1831) read them off the *derivative tower*, extending the bound to any interval and counting with multiplicity; their near-simultaneous discovery set off a priority dispute later disentangled by Akritas [5]. Sturm (1829) closed the gap from bound to *exact* count—but with a third sequence, the signed Euclidean remainders, and only for distinct roots. That these are three faces of one principle emerged only in the twentieth century, through Cauchy's index and its modern axiomatisation as abstract *Sturm chains* by Eisermann [8].

*Formalized with the assistance of an AI system (Claude, Anthropic); the mathematics is classical, every claim, scope statement and limitation is the author's responsibility, and the Lean kernel—not the assistant—certifies the proofs. The boundary between what is classical and what is contributed here is drawn explicitly in Section 5.

This paper makes that fusion concrete in Lean: one sign-variation engine, one local-drop law, three instances run through it, and the exact point where the derivative tower steps outside the Sturm-chain world. The unification is classical; what is new is the machine-checked engine and the axiomatic line it lets us draw between the three.

What you will find here. One engine (Section 1); the local-drop law they share (Section 2); the three instances read off it—Descartes, Sturm, Budan–Fourier (Section 3); the dividing line, where the tower leaves the Sturm-chain world (Section 4); what is classical and what is contributed, without varnish (Section 5); and the questions worth carrying forward (Section 6). The two companion papers [13, 14] carry the full proofs of the Sturm and Budan–Fourier instances; here I assemble them into one picture and draw the line between them.

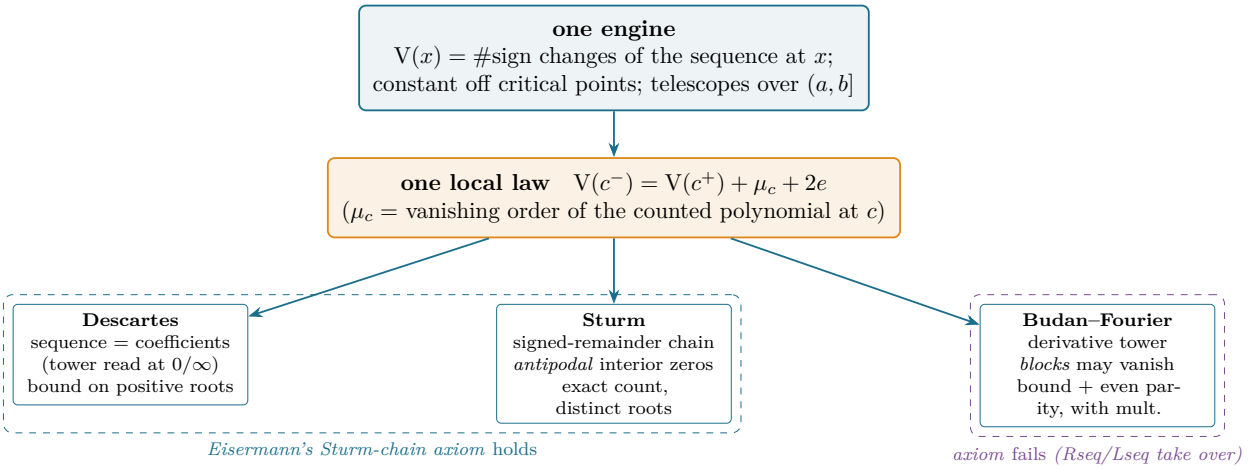


Figure 1: The thesis in one picture. A single sign-variation engine and a single local-drop law carry three classical root counts. Descartes' and Sturm's sequences obey Eisermann's Sturm-chain axiom—no two members vanish together; the derivative tower of Budan–Fourier breaks it at every multiple root and needs the block law `Rseq`/`Lseq`, of which the antipodal case is a degeneration.

1 One engine

Fix a finite sequence of real polynomials $S = (S_0, \dots, S_n)$ and, for a point x that is not a common obstruction, let

$$\mathrm{V}_S(x) \;=\; \#\{\text{sign changes in } (\operatorname{sign} S_0(x), \dots, \operatorname{sign} S_n(x)),\ \text{zeros deleted}\}.$$

In Lean this is one function, `signChanges` on the list of evaluated signs (equivalently `signVarAt` on the polynomials), with one parity engine `wallCount` underneath. Two facts hold for *any* such sequence of continuous functions and are proved once: *(i)* on an interval where no member vanishes, every sign is constant, so V_S is locally constant (`signVarAt_eq_of_no_root`, from the intermediate value theorem); *(ii)* the parity of V_S on a zero-free-ended block depends only on its first and last surviving signs (`wallCount_even_iff_endpoints`). The *critical points*—where some member vanishes—are finite (the roots of $\prod_k S_k$, a nonzero polynomial), so V_S is a staircase: flat between criticals, and the total descent over $(a, b]$ telescopes into a sum of per-critical drops. This spine is shared verbatim by all three theorems; it was written once and used three times.

2 One local law

Everything then reduces to the drop across a single critical point c. Write $\mathrm{V}(c^-), \mathrm{V}(c^+)$ for the locally-constant values just left and right of c, and let μ_c be the order to which the *counted* polynomial (the head $S_0 = p$) vanishes at c. All three theorems are instances of one statement.

$$\mathrm{V}(c^-) \;=\; \mathrm{V}(c^+) \;+\; \mu_c \;+\; 2e \qquad (\exists\, e \in \mathbb{N}).$$

The right side carries no information beyond c (the count just to the right equals the count at c with zeros ignored); the left side adds the head's vanishing order μ_c and an *even* surplus $2e$ from the interior. Summing over the critical points in $(a, b]$ gives the interval statement: the number of roots of p there (with multiplicity $= \sum \mu_c$) is at most $\mathrm{V}(a) - \mathrm{V}(b)$, and differs from it by the even $\sum 2e$. The whole divergence between the three theorems is in *how the interior behaves*—and that is exactly what the next two sections separate.

3 Three instances

We read all three off one worked polynomial where they can be compared, $p = x^3 - x = x(x-1)(x+1)$, and then name the feature each one isolates.

Sturm ([13]; Figure 2). The signed-remainder chain $x^3 - x,\ 3x^2 - 1,\ \frac{2}{3}x,\ 1$ is built so that consecutive members are coprime: at a zero of an interior member the two neighbours are *antipodal* (strictly opposite), so deleting that member leaves the count unchanged (the `FlankReduce` relation). Only the head pair (p, p') moves the count, by one, at each root. The drop counts *distinct* roots exactly: $\mathrm{V}(-2) - \mathrm{V}(2) = 3$ on $(-2, 2]$. Here $\mu_c = 1$ at every root and the surplus is 0.

Budan–Fourier ([14]; Figure 2). The derivative tower $p, p', p'', \ldots$ replaces coprimality by a one-step relation—each member is the derivative of the previous—so a vanishing member's sign just off c is fixed by its derivative: it copies it on the right (the block *collapses*, no new change) and negates it on the left (the block *alternates*, one change per member). At a multiple root a whole block vanishes, the left alternation contributes the multiplicity, and interior blocks contribute an even surplus—so the count is a *bound with multiplicity*, even-off from the truth. For $x^3 - x$ (simple roots) it agrees with Sturm; its distinctive face is the double root and the phantom even drop (Figure 2).

Descartes is the shadow at the ends of $(0, \infty)$: since $p^{(k)}(0) = k!\, a_k$, the tower's sign sequence at 0 *is* the coefficient sequence, so $\mathrm{V}(0)$ is the coefficient sign-variation count; and $\mathrm{V}(+\infty) = 0$. The bound on positive roots is $\mathrm{V}(0) - \mathrm{V}(+\infty) = \mathrm{V}(0)$, even-off from the truth. For $x^3 - x$ the coefficients $1, 0, -1, 0$ give one sign change and one positive root, $x = 1$. This last instance is checked against the library, not just asserted: `fourierVar p 0 = Polynomial.signVariations p` (`Descartes.lean`, `sorry`-free), so the engine's $\mathrm{V}(0)$ is *definitionally* Mathlib's own coefficient sign-variation count—the function on which Mathlib's Descartes' rule is stated. The bridge is the two facts above ($p^{(k)}(0) = k!\, a_k$, and $\mathrm{V}(+\infty) = 0$ left to prose) together with reversal-invariance of the sign count, the tower listing the signs low-to-high and Mathlib's coefficient list high-to-low.

4 The dividing line

What separates Sturm from Budan–Fourier is not a matter of taste; it is a precise axiom, and the machine made it precise. Eisermann's abstract *Sturm chain* [8] is required to satisfy one condition (his Def. 3.10): whenever an *interior* member S_k vanishes, its neighbours are strictly opposite there,

	sequence built from $p = x^3 - x$	**one engine** V	*drop counts*
Descartes	coefficients $1, 0, -1, 0$	$\mathrm{V}(0) = 1$	positive roots
Budan–Fourier	tower p, p', p'', p'''	$\mathrm{V}(-2) - \mathrm{V}(2) = 3$	roots w. mult. (+ even gap)
Sturm	remainders $p, p', \frac{2}{3}x, 1$	$\mathrm{V}(-2) - \mathrm{V}(2) = 3$	distinct roots, exact

Figure 2: One polynomial, three sequences, one engine. Each classical count is the *same* sign-variation engine V applied to a different sequence built from $p = x^3 - x$: Descartes' coefficients, the Budan–Fourier derivative tower, Sturm's signed remainders. They read different facets—positive roots, roots with multiplicity, distinct roots—but the count, its local constancy off critical points, and its telescoping over $(a, b]$ are one and the same (boxed). The detailed staircases live in the companion papers [13, 14]; this paper's subject is the boxed column they share.

$$S_k(c) = 0 \implies S_{k-1}(c)\, S_{k+1}(c) < 0 \qquad (0 < k < n),$$

which in particular forbids two consecutive members from vanishing together. Sturm's chain satisfies it (coprimality); Descartes' coefficient reading is degenerate but compatible.

Proposition 1 (the derivative tower is not a Sturm chain)**.** *The derivative tower fails Eisermann's axiom at every multiple root. Concretely, for* $p_A = (x-1)^2(x+1)$ *with tower* $[p_A, p'_A, p''_A, p'''_A]$*, the interior member* p'_A *vanishes at* $x = 1$*, yet*

$$p_A(1) \cdot p''_A(1) = 0 \cdot 4 = 0 \not< 0,$$

because p_A *and* p'_A *vanish there* at once*. Hence the tower is not a Sturm chain in the sense of [8], and the antipodal interior-deletion that proves Sturm's theorem cannot apply.*

This is the whole point of the block law. Where a Sturm chain deletes one sandwiched interior member at a time (`FlankReduce`), the tower must resolve an entire vanishing block at once (`Rseq`/`Lseq`: copy the derivative's sign on the right, negate it on the left). The two are not rival techniques; the antipodal single-deletion is the *non-degenerate special case* of the block law, the case where every block has length one. Figure 3 sets the two local geometries side by side.

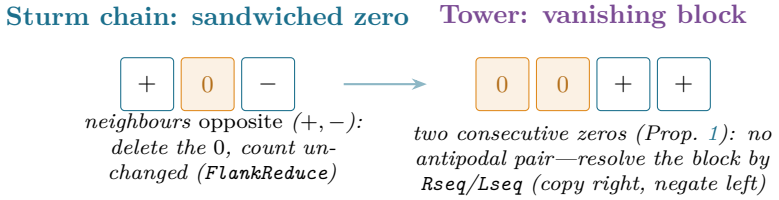


Figure 3: Two local geometries. Left: a Sturm chain's interior zero sits between opposite signs and is deleted without trace. Right: the tower's consecutive zeros have no such sandwich; the block is resolved by collapse (right) and alternation (left). The first is the length-one special case of the second.

5 What is classical, and what is contributed

Without varnish. *Classical, not ours*: that Descartes, Budan–Fourier and Sturm are facets of one sign-variation principle (Akritas [5]; Basu–Pollack–Roy [7]); the Cauchy index as the deep unifying invariant (Cauchy; Eisermann [8]); and the abstract Sturm-chain axiomatisation itself [8]. *Already machine-checked elsewhere*: the Cauchy-index route, in Isabelle/HOL, by Li and Paulson [10]; and the Budan–Fourier theorem, in Isabelle/HOL, by Li [9]. *Contributed here*: the explicit *shared* sign-variation engine in Lean 4 over Mathlib; the first Lean formalizations of Sturm's theorem [13] and of Budan–Fourier [14] running through it; the bridge `fourierVar p 0 = Polynomial.signVariations p` (`Descartes.lean`), which identifies the engine's V(0) with the coefficient sign count on which Mathlib's own Descartes' rule is stated—so the third count is checked against the library, not merely read off in prose; and Proposition 1, the precise placement of the derivative tower *outside* the classical Sturm-chain axiom, with `Rseq`/`Lseq` identified as the local law of that wider regime. Everything is over $\mathbb{R}$; the multiplicity step uses characteristic zero essentially. No root is ever computed; no certificate is produced; no isolator is built.

6 Questions worth carrying forward

1. *The weakest axiom.* Proposition 1 shows the tower escapes Eisermann's condition. What is the *weakest* hypothesis on an abstract sequence under which the local law $\mathrm{V}(c^-) = \mathrm{V}(c^+) + \mu_c + 2e$ still holds—one that has the antipodal Sturm-chain axiom and the derivative tower as its two leading instances? A Lean structure carrying exactly that hypothesis would hold the local lemma once instead of three times. The engine of Section 1 is already that structure minus the local law; the law is what wants axiomatising.

2. *Through the Cauchy index.* Li and Paulson formalised the Cauchy index in Isabelle [10]; Mathlib has no such development. Does the engine here factor through a Lean Cauchy index, recovering Sturm and Budan–Fourier as winding-number computations in the sense of [8]—and would the derivative tower then appear as a non-generic boundary case there too?

3. *From bound to certificate.* The even surplus measures how far Budan–Fourier overshoots. Can bisecting until it vanishes be turned into a verified, certificate-producing root isolator over Mathlib, the multiplicity-aware analogue of the Vincent–Collins–Akritas methods [6]?

The pattern across all three is one reflection: the theorem is now a fixed point a kernel defends, so the live direction is not to reprove it but to find the *one* hypothesis of which the three counts—and perhaps the Cauchy index above them—are instances, and to learn exactly how much of it the derivative tower's blocks force us to weaken.

Reproducing

```
git clone https://github.com/karlesmarin/godsil-gutman-lean
cd godsil-gutman-lean && lake exe cache get
lake env lean Sturm.lean          # the shared engine + Sturm instance
lake env lean BudanFourier.lean   # the Budan-Fourier instance (imports Sturm)
lake env lean Descartes.lean      # the Descartes bridge: V(0) = signVariations
```

Lean `v4.30.0-rc2`, Mathlib pin `701fb6e9`. All headline theorems are `sorry`-free and `#print axioms` reports only `propext`, `Classical.choice`, `Quot.sound`. The worked signs of every figure

are re-derived in exact arithmetic before the figure is drawn (`figures/`).

References

[1] R. Descartes, *La Géométrie* (1637).

[2] F. D. Budan de Boislaurent, *Nouvelle méthode pour la résolution des équations numériques*, Paris (1807).

[3] J. Fourier, *Analyse des équations déterminées*, Firmin Didot, Paris (posthumous, 1831).

[4] C. Sturm, Mémoire sur la résolution des équations numériques, *Mém. présentés par divers savants à l'Acad. Royale des Sci.* **6** (1835) 271–318.

[5] A. G. Akritas, Reflections on a pair of theorems by Budan and Fourier, *Math. Magazine* **55** (1982) 292–298.

[6] G. E. Collins, A. G. Akritas, Polynomial real root isolation using Descartes' rule of signs, in *Proc. SYMSAC '76*, ACM, 1976, 272–275.

[7] S. Basu, R. Pollack, M.-F. Roy, *Algorithms in Real Algebraic Geometry*, 2nd ed., Springer, 2006 (sign-variation theory, Ch. 2).

[8] M. Eisermann, The fundamental theorem of algebra made effective: an elementary real-algebraic proof via Sturm chains, *Amer. Math. Monthly* **119** (2012), no. 9, 715–752; `arXiv:0808.0097`.

[9] W. Li, L. C. Paulson, Counting polynomial roots in Isabelle/HOL: a formal proof of the Budan–Fourier theorem, in *CPP 2019*, ACM, 2019, 52–64; `arXiv:1811.11093`.

[10] W. Li, L. C. Paulson, Evaluating winding numbers and counting complex roots through Cauchy indices in Isabelle/HOL, *J. Automated Reasoning* **64** (2020), no. 2, 331–360; `arXiv:1804.03922`.

[11] The mathlib Community, The Lean mathematical library, in *CPP 2020*, ACM, 2020, 367–381.

[12] L. de Moura, S. Ullrich, The Lean 4 theorem prover and programming language, in *CADE 28*, LNCS **12699**, Springer, 2021, 625–635.

[13] C. Marín, *The Staircase of Signs: Sturm's Root-Counting Theorem, Machine-Checked in Lean 4*, Zenodo, 2026, `doi:10.5281/zenodo.20707348`.

[14] C. Marín, *Counting with the Derivative Tower: The Budan–Fourier Theorem, Machine-Checked in Lean 4*, Zenodo, 2026, `doi:10.5281/zenodo.20736143` (companion paper).