A Lean-verified finite-torus proof of Ehrhart's sharp volume bound

Initio Intelligence, Inc.

August 19, 2026

Theorem 1. *Let $n \geq 1$, and let $K \subseteq \mathbb{R}^n$ be a full-dimensional compact convex body whose barycenter is the origin. Suppose that the origin is the only lattice point in the interior of K:*

$$\operatorname{int}(K) \cap \mathbb{Z}^n = \{0\}.$$

Then

$$\operatorname{vol}(K) \leq \frac{(n+1)^n}{n!}.$$

The constant is sharp: equality holds for the centered simplex

$$(n+1)\Delta_n - \mathbf{1},$$

where $\Delta_n = \operatorname{conv}\{0, e_1, \ldots, e_n\}$.

The accompanying Lean development proves Theorem 1 directly for arbitrary compact convex bodies. Its proof preserves the central protected-product and finite-torus mechanism of the original manuscript, but formalization led to a shorter route. The argument works over $\mathbb{F}_p$ from the outset, constructs the required two-flags basis by a direct coordinate-hyperplane induction, uses only an aggregate depth bound in the nilpotence step, proves no-wrap directly from the support of the product, and selects primes along an asymptotically sharp subsequence using only the infinitude of primes.

The proof is organized around the following exact finite obstruction. Let

$$A_k = \{a \in \mathbb{Z}^n : a/k \in \operatorname{int}(K)\}, \qquad N_k = \#A_k.$$

For a suitable prime p at scale k, the formal argument proves

$$(n+1)kN_k - \binom{n+(n+1)k}{n+1} \leq n(p-1). \tag{1}$$

The left side comes from finite-field jet counting; the right side is the nilpotence threshold of the maximal ideal in the group algebra of $(\mathbb{Z}/p\mathbb{Z})^n$. The barycenter condition prevents the protected coefficient from wrapping around modulo p.

Notation. Lebesgue measure on $\mathbb{R}^n$ is normalized so that $\mathbb{Z}^n$ has covolume one. The barycenter of a full-dimensional compact convex body is

$$g(K) = \operatorname{vol}(K)^{-1} \int_K x \, dx.$$

For $a = (a_1, \ldots, a_n) \in \mathbb{Z}^n$, write $z^a = z_1^{a_1} \cdots z_n^{a_n}$. We use the lexicographic order on $\mathbb{Z}^n$; it is a translation-invariant total order and therefore is compatible with addition.

1 Lattice samples of the original body

The formal proof does not pass through rational polytopes. It samples the original body directly. For $k \geq 1$, set

$$A_k = \{a \in \mathbb{Z}^n : a/k \in \operatorname{int}(K)\}, \qquad N_k = \#A_k,$$

$$U_k = \sum_{a \in A_k} a, \qquad b_k = \frac{U_k}{kN_k}, \qquad s_k = kN_k.$$

The hypothesis $\operatorname{int}(K) \cap \mathbb{Z}^n = \{0\}$ includes $0 \in \operatorname{int}(K)$, so $0 \in A_k$ and $N_k \geq 1$ for every $k \geq 1$.

Lemma 2 (Lattice count and first moment)**.** *Let $V = \operatorname{vol}(K)$. Then*

$$\frac{N_k}{k^n} \longrightarrow V, \qquad b_k \longrightarrow 0, \qquad \frac{s_{k+1}}{s_k} \longrightarrow 1, \qquad s_k \longrightarrow \infty.$$

Proof. A compact convex body is Jordan measurable: its boundary has Lebesgue measure zero. Hence the ordinary lattice Riemann-sum theorem gives, for every continuous function f on K,

$$\frac{1}{k^n} \sum_{a \in A_k} f(a/k) \longrightarrow \int_K f(x)\, dx. \tag{2}$$

Applying (2) to $f = 1$ gives $N_k/k^n \to V$. Applying it to each coordinate function gives

$$\frac{1}{k^n} \sum_{a \in A_k} \frac{a}{k} \longrightarrow \int_K x\, dx = V g(K) = 0.$$

Since $V > 0$,

$$b_k = \frac{k^{-n} \sum_{a \in A_k} a/k}{N_k/k^n} \longrightarrow 0.$$

Moreover

$$\frac{s_k}{k^{n+1}} = \frac{N_k}{k^n} \longrightarrow V > 0.$$

It follows that $s_k \to \infty$, and

$$\frac{s_{k+1}}{s_k} = \frac{s_{k+1}/(k+1)^{n+1}}{s_k/k^{n+1}} \left(\frac{k+1}{k}\right)^{n+1} \longrightarrow 1.$$

$\square$

The following direct radial exclusion is the geometric input to the no-wrap argument.

Lemma 3 (Uniform radial exclusion)**.** *For every $\varepsilon > 0$, for all sufficiently large k,*

$$b_k + tz \notin K$$

for every $z \in \mathbb{Z}^n \setminus \{0\}$ and every $t \geq 1 + \varepsilon$.

Proof. Choose $\rho > 0$ such that the open ball $B(0, \rho)$ is contained in $\operatorname{int}(K)$. By Lemma 2, for all sufficiently large k,

$$\|b_k\| < \varepsilon\rho.$$

Suppose that $x = b_k + tz \in K$ for some $z \neq 0$ and $t \geq 1 + \varepsilon$. Put

$$q = -\frac{b_k}{t-1}.$$

Then $\|q\| < \rho$, so $q \in \mathrm{int}(K)$. Since $t > 1$,

$$z = t^{-1}x + (1 - t^{-1})q.$$

This is a convex combination with strictly positive weight on the interior point q. Convexity therefore gives $z \in \mathrm{int}(K)$, contradicting $\mathrm{int}(K) \cap \mathbb{Z}^n = \{0\}$. □

2 Finite-field jets in the finite torus

Fix $k \geq 1$ and a prime p. Write $N = N_k$, and enumerate

$$A_k = \{a_1 < \cdots < a_N\}$$

in lexicographic order. Let

$$G_p = (\mathbb{Z}/p\mathbb{Z})^n, \qquad R_p = \mathbb{F}_p[G_p]$$

be the group algebra. For $u \in G_p$, denote its basis element by X^u. If e_i is the ith coordinate vector, set

$$Z_i = X^{e_i}, \qquad Y_i = Z_i - 1,$$

and let

$$\mathfrak{m} = (Y_1, \ldots, Y_n) \subseteq R_p.$$

Reducing the exponents a_j modulo p defines a linear map

$$T = T_{k,p} : \mathbb{F}_p^N \longrightarrow R_p, \qquad T(c) = \sum_{j=1}^{N} c_j X^{\overline{a_j}}.$$

For $r \geq 0$, define the descending filtration

$$W_r = T^{-1}(\mathfrak{m}^r).$$

In particular, $W_0 = \mathbb{F}_p^N$.

Lemma 4 (Finite-field jet bound)**.** *For every $r \geq 1$,*

$$\dim_{\mathbb{F}_p} W_r \geq N - \binom{n+r-1}{n}.$$

Consequently, for every $M \geq 1$,

$$MN - \binom{n+M}{n+1} \leq \sum_{r=1}^{M} \dim_{\mathbb{F}_p} W_r. \tag{3}$$

Proof. Choose the standard representatives $\overline{a_{j,i}} \in \{0, \ldots, p-1\}$ of the coordinates of a_j modulo p, and form

$$P_c(y) = \sum_{j=1}^{N} c_j \prod_{i=1}^{n} (1 + y_i)^{\overline{a_{j,i}}} \in \mathbb{F}_p[y_1, \ldots, y_n].$$

Under the substitution $y_i \mapsto Y_i$, the polynomial P_c maps to $T(c)$. Let $J_r(c)$ be the collection of coefficients of P_c in total degree $< r$. There are

$$\binom{n+r-1}{n}$$

such monomials. If $J_r(c) = 0$, then $P_c \in (y_1, \ldots, y_n)^r$, and therefore $T(c) \in \mathfrak{m}^r$. Thus

$$\ker J_r \subseteq W_r.$$

Rank–nullity gives the first assertion. Summing it for $r = 1, \ldots, M$ and using the hockey-stick identity

$$\sum_{r=1}^{M} \binom{n+r-1}{n} = \binom{n+M}{n+1}$$

gives (3). □

This step is already different from the original manuscript. There is no characteristic-zero Laurent-jet space and no comparison of an integer jet matrix before and after reduction modulo p. The filtration is constructed directly inside the finite torus.

3 A terminal basis and a protected product

The formalization needs a basis compatible with two descending flags: the ideal-adic filtration W_r and the terminal coordinate flag determined by the ordered exponent list,

$$F^N = H_0 \supseteq H_1 \supseteq \cdots \supseteq H_N = 0, \qquad H_j = \{x : x_1 = \cdots = x_j = 0\}.$$

The Lean structure records only the data consumed later—reverse-echelon form, membership at assigned filtration depths, and an aggregate depth inequality. The proposition below gives those data by a direct induction on the coordinate flag. As Corollary 6 shows, they in fact force exact adaptation to every filtration level through the chosen cutoff.

Proposition 5 (Terminal two-flags basis)**.** *Let F be a field, and let*

$$F^N = W_0 \supseteq W_1 \supseteq W_2 \supseteq \cdots$$

be a descending filtration, observed through a fixed cutoff M. There are a basis $c_1, \ldots, c_N$ of F^N and integers $d_1, \ldots, d_N \in \{0, \ldots, M\}$ such that:

1. *$c_i \in W_{d_i}$;*
2. *writing $c_i = (c_{i1}, \ldots, c_{iN})$, one has*

$$c_{ij} = 0 \quad (j < i), \qquad c_{ii} = 1;$$

3.

$$\sum_{r=1}^{M} \dim_F W_r \leq \sum_{i=1}^{N} d_i. \tag{4}$$

Proof. We argue by induction on N. The case $N = 0$ is immediate. Let

$$H = \{x \in F^N : x_1 = 0\}.$$

Since $W_0 = F^N$, there is at least one $r \leq M$ for which $W_r \not\subseteq H$. Let d be the largest such r, and choose $c_1 \in W_d$ with first coordinate one. Then $c_1 \in W_r$ for every $r \leq d$, while maximality of d gives $W_r \subseteq H$ for every $d < r \leq M$.

Identify H with F^{N-1} by deleting the first coordinate, and apply the induction hypothesis to the filtration

$$W'_r = W_r \cap H.$$

This gives a terminal basis $c_2, \dots, c_N$ of H, with depths $d_2, \dots, d_N$. Since $c_1 \notin H$, the vectors $c_1, \dots, c_N$ form a basis of F^N and have the required terminal shape.

For $r \leq d$, intersecting W_r with the coordinate hyperplane H loses at most one dimension:

$$\dim W_r \leq 1 + \dim W'_r.$$

For $d < r \leq M$, one has $W_r \subseteq H$, so

$$\dim W_r = \dim W'_r.$$

Therefore

$$\sum_{r=1}^{M} \dim W_r \leq d + \sum_{r=1}^{M} \dim W'_r \leq d + \sum_{i=2}^{N} d_i,$$

which is (4) with $d_1 = d$. □

Corollary 6 (Exact adaptation through the cutoff)**.** *For the basis and depths in Proposition 5, one has, for every $1 \leq r \leq M$,*

$$W_r = \operatorname{span}_F\{c_i : d_i \geq r\}, \qquad \dim_F W_r = \#\{i : d_i \geq r\}. \tag{5}$$

Moreover,

$$\sum_{r=1}^{M} \dim_F W_r = \sum_{i=1}^{N} d_i. \tag{6}$$

If $d_i < M$, then $c_i \in W_{d_i} \setminus W_{d_i+1}$.

Proof. For $1 \leq r \leq M$, let $I_r = \{i : d_i \geq r\}$. Since the filtration is descending and $c_i \in W_{d_i}$, the vectors c_i with $i \in I_r$ are linearly independent elements of W_r. Hence

$$\#I_r \leq \dim_F W_r.$$

Summing over r and counting each index i exactly d_i times gives

$$\sum_{i=1}^{N} d_i = \sum_{r=1}^{M} \#I_r \leq \sum_{r=1}^{M} \dim_F W_r \leq \sum_{i=1}^{N} d_i,$$

where the last inequality is Proposition 5. Equality holds throughout. Thus $\#I_r = \dim_F W_r$ for every r, and the independent family $\{c_i : i \in I_r\} \subseteq W_r$ is a basis of W_r, proving (5) and (6).

Finally, if $d_i < M$ and $c_i \in W_{d_i+1}$, then (5) would express c_i as a linear combination of basis vectors c_j with $d_j \geq d_i + 1$, none of which is c_i. This contradicts linear independence of the full basis. □

After the coefficient coordinates are ordered by the chosen translation-invariant exponent order, the terminal zeros and unit diagonal in Proposition 5 give pairwise distinct pivots. Corollary 6 shows that the basis is exactly adapted through the cutoff. Applied to the manuscript's order-of-vanishing filtration, which terminates in zero, one may choose M with $W_{M+1} = 0$; the proposition and corollary then recover the full conclusion of the corrected Lemma 5 for that pivot order. The difference is therefore not a weakening of that lemma: the formalization supplies a second, coordinate-inductive proof and records only the finite-cutoff data needed downstream.

Apply Proposition 5 to the filtration $W_r = T^{-1}(\mathfrak{m}^r)$. For the resulting basis, define Laurent rows

$$f_i(z) = \sum_{j=1}^{N} c_{ij} z^{a_j} = \sum_{j=i}^{N} c_{ij} z^{a_j}.$$

Let

$$U = \sum_{j=1}^{N} a_j, \qquad G(z) = z^{-U} \prod_{i=1}^{N} f_i(z).$$

Lemma 7 (Protected coefficient)**.** *The constant coefficient of G is one. More precisely, the diagonal selection a_i from the ith row is the unique nonzero selection whose exponent sum is U.*

Proof. A term in the expansion of $\prod_i f_i$ is specified by a function $\sigma : \{1, \ldots, N\} \to \{1, \ldots, N\}$ and has coefficient $\prod_i c_{i,\sigma(i)}$. If this coefficient is nonzero, terminality gives

$$\sigma(i) \geq i \qquad \text{for every } i.$$

If σ is not the identity, then at least one inequality is strict. Since the lexicographic order is compatible with addition,

$$\sum_i a_{\sigma(i)} > \sum_i a_i = U.$$

Thus a nonzero selection can have exponent sum U only when $\sigma(i) = i$ for every i. Its coefficient is $\prod_i c_{ii} = 1$. After multiplication by z^{-U}, this becomes the constant coefficient of G. □

Two further consequences will be used. First, if $u \in \operatorname{supp}(G)$, then there is at least one selection σ with nonzero coefficient such that

$$u = \sum_{i=1}^{N} a_{\sigma(i)} - U. \tag{7}$$

Second, since $c_i \in W_{d_i}$,

$$T(c_i) \in \mathfrak{m}^{d_i},$$

and hence

$$\prod_{i=1}^{N} T(c_i) \in \mathfrak{m}^D, \qquad D = \sum_{i=1}^{N} d_i. \tag{8}$$

4 No-wrap and the finite-torus obstruction

Lemma 8 (Finite-torus nilpotence)**.** *In $R_p = \mathbb{F}_p[(\mathbb{Z}/p\mathbb{Z})^n]$,*

$$\mathfrak{m}^{n(p-1)+1} = 0.$$

Proof. For each i, $Z_i^p = 1$. In characteristic p,

$$Y_i^p = (Z_i - 1)^p = Z_i^p - 1 = 0.$$

Every monomial in the Y_i of total degree at least $n(p-1)+1$ has some exponent at least p, and hence vanishes. Therefore every product of $n(p-1)+1$ elements of $\mathfrak{m}$ is zero. $\square$

The protected coefficient survives reduction to R_p provided no other supported exponent of G is congruent to zero modulo p. The next lemma proves this directly from convexity and the empirical center.

Lemma 9 (Geometric no-wrap)**.** *Fix $\varepsilon > 0$. For all sufficiently large k, if p is a prime satisfying*

$$p \geq (1+\varepsilon)s_k = (1+\varepsilon)kN_k,$$

then zero is the only exponent $u \in \operatorname{supp}(G)$ divisible by p coordinatewise. Consequently, the image of G in R_p is nonzero.

Proof. Take k large enough for Lemma 3. Suppose that $u \in \operatorname{supp}(G)$ and $u = pz$ for some $z \in \mathbb{Z}^n$. By (7), choose a selection σ with nonzero coefficient and

$$u = \sum_i a_{\sigma(i)} - U.$$

The selected average

$$x_\sigma = \frac{1}{N}\sum_{i=1}^{N} \frac{a_{\sigma(i)}}{k}$$

belongs to K by convexity. Since $b_k = U/(kN)$,

$$x_\sigma = b_k + \frac{u}{kN} = b_k + \frac{p}{kN}z.$$

If $u \neq 0$, then $z \neq 0$, while $p/(kN) \geq 1+\varepsilon$. This contradicts Lemma 3. Hence $u = 0$.

By Lemma 7, the coefficient of G at zero is one. Reduction modulo p groups Laurent exponents by their residue classes. Since zero is the only supported exponent in the zero residue class, the coefficient of the identity basis element in the image of G is still one. Thus the image of G in R_p is nonzero. $\square$

Proposition 10 (Exact finite obstruction)**.** *Fix $\varepsilon > 0$. For all sufficiently large k, every prime p satisfying $p \geq (1+\varepsilon)kN_k$ obeys*

$$(n+1)kN_k - \binom{n+(n+1)k}{n+1} \leq n(p-1). \tag{9}$$

Proof. Set $M = (n+1)k$, and apply Proposition 5 to the filtration W_r. Combining (3) and (4) gives

$$MN - \binom{n+M}{n+1} \leq D.$$

By (8), the product $\prod_i T(c_i)$ belongs to $\mathfrak{m}^D$. Its product with the unit $X^{-\overline{U}}$ is the image of G, which is nonzero by Lemma 9. Lemma 8 therefore forces

$$D \leq n(p-1).$$

Substituting $M = (n+1)k$ proves (9). $\square$

This proposition contains the proof's algebraic core. A large low-jet filtration forces a product deep into the maximal ideal; the finite torus makes the ideal nilpotent; the protected coefficient and the barycenter prevent the product from vanishing through modular wraparound.

5 Prime crossing without prime-gap estimates

The original manuscript selected a prime in a short multiplicative interval using the prime number theorem. The formal proof instead takes a first crossing of the generally nonmonotone scale $s_k = kN_k$.

Lemma 11 (Prime crossing)**.** *Let (s_k) be a sequence of positive integers such that*

$$s_k \longrightarrow \infty, \qquad \frac{s_{k+1}}{s_k} \longrightarrow 1.$$

Fix an integer $d \geq 1$. There are indices $q_j \to \infty$ and primes p_j such that

$$\frac{d+1}{d} < \frac{p_j}{s_{q_j}} \leq \frac{d+1}{d}\frac{s_{q_j+1}}{s_{q_j}}. \tag{10}$$

In particular,

$$\frac{p_j}{s_{q_j}} \longrightarrow \frac{d+1}{d}.$$

Proof. For each $j \geq 1$, choose a prime p_j so large that

$$p_j > (d+1) \max_{1 \leq i \leq j} s_i;$$

only the infinitude of primes is used here. Since $s_k \to \infty$, there is some r for which

$$dp_j \leq (d+1)s_r.$$

Let r_j be the first such index and put $q_j = r_j - 1$. The choice of p_j implies $r_j > j$, so $q_j \geq j$ and $q_j \to \infty$. Minimality gives

$$(d+1)s_{q_j} < dp_j \leq (d+1)s_{q_j+1}.$$

Dividing by ds_{q_j} yields (10). The conclusion follows from $s_{q_j+1}/s_{q_j} \to 1$. □

6 Proof of the volume bound

Proof of Theorem 1. Let $V = \mathrm{vol}(K)$ and fix $d \geq 1$. Apply Lemma 11 to $s_k = kN_k$, using Lemma 2. We obtain $q_j \to \infty$ and primes p_j such that

$$\frac{p_j}{q_jN_{q_j}} \longrightarrow \frac{d+1}{d} \quad \text{and} \quad p_j > \left(1 + \frac{1}{d}\right) q_jN_{q_j}.$$

For all sufficiently large j, Proposition 10, with $\varepsilon = 1/d$, gives

$$(n+1)q_jN_{q_j} - \binom{n + (n+1)q_j}{n+1} \leq n(p_j - 1).$$

Divide by q_j^{n+1}. Lemma 2 gives

$$\frac{N_{q_j}}{q_j^n} \longrightarrow V, \qquad \frac{q_jN_{q_j}}{q_j^{n+1}} \longrightarrow V.$$

The binomial term has the elementary asymptotic

$$\frac{\binom{n+(n+1)q_j}{n+1}}{q_j^{n+1}} \longrightarrow \frac{(n+1)^{n+1}}{(n+1)!} = \frac{(n+1)^n}{n!}.$$

Finally,

$$\frac{p_j - 1}{q_j^{n+1}} = \frac{p_j}{q_j N_{q_j}} \frac{q_j N_{q_j}}{q_j^{n+1}} - \frac{1}{q_j^{n+1}} \longrightarrow \frac{d+1}{d} V.$$

Passing to the limit yields

$$(n+1)V - \frac{(n+1)^n}{n!} \le n \frac{d+1}{d} V.$$

Equivalently,

$$V - \frac{(n+1)^n}{n!} \le \frac{nV}{d}. \tag{11}$$

Since (11) holds for every $d \ge 1$, letting $d \to \infty$ gives

$$V \le \frac{(n+1)^n}{n!}.$$

□

7 Sharpness

Let

$$S = (n+1)\Delta_n - \mathbf{1}.$$

Then

$$\operatorname{vol}(S) = (n+1)^n \operatorname{vol}(\Delta_n) = \frac{(n+1)^n}{n!}.$$

The barycenter of Δ_n is $\mathbf{1}/(n+1)$, so the barycenter of S is zero. Finally, if $x \in \operatorname{int}(S) \cap \mathbb{Z}^n$, then

$$x_i > -1 \quad \text{for every } i, \qquad \sum_{i=1}^{n} (x_i + 1) < n + 1.$$

The integers $y_i = x_i + 1$ are all at least one. Their sum is at least n and is an integer strictly less than $n+1$, so it equals n; hence every $y_i = 1$ and $x = 0$. Conversely, $0 \in \operatorname{int}(S)$, since all its coordinates are greater than -1 and $\sum_{i=1}^{n}(0+1) = n < n+1$. Thus $\operatorname{int}(S) \cap \mathbb{Z}^n = \{0\}$, and S satisfies the hypotheses and attains the bound.

The Lean development proves this example independently. It constructs the centered simplex as an explicit image of the standard simplex, proves compactness, convexity, nonempty interior, the exact interior lattice-point description, the volume formula, and barycenter zero, and then packages these facts into the formal structure used by the upper-bound theorem.

8 Relation with the original manuscript proof

The proof above is not a line-by-line transcription of the original manuscript. It is a related proof discovered and stabilized during formalization. The differences are mathematically substantive.

The argument works directly with K. The original manuscript first shrinks and approximates K by centered rational polytopes. The Lean route uses lattice Riemann sums for the interior of the original convex body, so the rational-polytope reduction disappears entirely. The only asymptotics required are $N_k/k^n \to \mathrm{vol}(K)$ and $b_k \to 0$; no $O(k^{n-1})$ error term is needed.

The jet filtration begins in characteristic p. The original proof defines an exact order-of-vanishing filtration in characteristic zero, derives a nonlinear lower bound for its total layer sum, and then shows that reduction modulo p cannot decrease the layer dimensions. The Lean proof instead defines the ideal-adic filtration $W_r = T^{-1}(\mathfrak{m}^r)$ directly over $\mathbb{F}_p$. Rank–nullity for the finite low-jet map immediately gives the necessary dimension bound. Thus the integer jet matrix and the characteristic-zero-to-characteristic-p rank comparison are removed.

The terminal-basis construction gives a second proof of the corrected basis lemma. The manuscript's corrected Lemma 5 is correct and states the global, untruncated basis theorem: the basis is adapted to every order-of-vanishing level and has pairwise distinct pivots. The formalization reaches the same two-flags phenomenon by a different proof. After ordering the exponent coordinates by a translation-invariant total order, Proposition 5 constructs a reverse-echelon basis by induction on a coordinate hyperplane. The Lean theorem records membership at assigned depths and the aggregate inequality (4), the data used by the nilpotence argument. Corollary 6 shows mathematically that those data already force exact adaptation through the cutoff, while the terminal zeros and unit diagonal give pairwise distinct pivots. Applied to the manuscript's terminating order filtration and taking M with $W_{M+1} = 0$, this recovers the corrected lemma in full. Thus the formal route neither weakens nor supersedes corrected Lemma 5; it gives a second proof by coordinate-hyperplane induction and retains in Lean only the consequences used later. The exact-adaptation corollary is not separately recorded as a Lean declaration, since the later formal argument does not require it.

The protected coefficient is the common invariant. Both proofs build one row for each sampled exponent, multiply all rows, and center by the sum of the sample exponents. In both arguments, triangularity and a translation-invariant total order on exponents make the diagonal selection unique. This protects a nonzero constant coefficient from cancellation. The formal route uses lexicographic order rather than a generic real linear functional, but the mathematical mechanism is the same.

The formal route bypasses the Newton-polytope radius. The original manuscript packages the support in a Newton polytope, proves that zero is an exposed vertex, and bounds a lattice radius of that polytope. This gives a useful geometric description of the protected term. The Lean route needs only the support-level identity (7): every supported exponent comes from an actual choice of one sampled point per row, so its normalized value is the difference between a point of K and the empirical center. Lemma 3 then rules out nonzero multiples of p directly. Thus the protected coefficient remains essential, while the Newton-polytope radius is replaced by its concrete no-wrap consequence.

Prime crossing replaces the prime number theorem. The original proof chooses a prime in a short multiplicative interval for every sufficiently large k. The Lean proof needs the finite obstruction only along a subsequence. First crossing supplies primes with asymptotic ratio $(d+1)/d$ using only infinitude of primes and $s_{k+1}/s_k \to 1$. A final limit $d \to \infty$ removes the fixed inflation.

The final asymptotic inequality is linear. The original proof optimizes the characteristic-zero jet sum at a cutoff depending on N_k and obtains a nonlinear lower bound involving $(n!\,\mathrm{vol}(K))^{1/n}$. The formal route fixes the simple cutoff $M = (n+1)k$. After normalization, the exact binomial term already produces the sharp constant, and the crossing argument gives the linear slack estimate (11). Letting $d \to \infty$ completes the proof.

The conceptual spine is nevertheless the same:

$$\begin{aligned} \text{many low-jet constraints} &\Longrightarrow \text{a product deep in a local ideal} \\ &\Longrightarrow \text{a finite-torus nilpotence obstruction,} \end{aligned}$$

while the barycenter condition supplies the geometric no-wrap statement that keeps the protected coefficient nonzero. The formalization therefore does not indicate that the original manuscript, or its corrected Lemma 5, is incorrect. It isolates a second proof in which several intermediate constructions can be replaced by more direct finite-field and support-level arguments.

9 The formal Lean development

The formal statement uses

$$\texttt{Space n} = \mathrm{Fin}(n) \to \mathbb{R}, \qquad \texttt{Lattice n} = \mathrm{Fin}(n) \to \mathbb{Z}.$$

The structure `CenteredBody n` contains a carrier together with proofs of convexity, compactness, nonempty interior, barycenter zero, and

$$\{z \in \mathbb{Z}^n : \iota(z) \in \mathrm{int}(K)\} = \{0\},$$

where $\iota : \mathbb{Z}^n \hookrightarrow \mathbb{R}^n$ is the coordinatewise lattice embedding. The definition `normalizedVolume` is ordinary Lebesgue measure on this coordinate Euclidean space, converted from the extended nonnegative reals to $\mathbb{R}$. Thus the public theorem

`Ehrhart.manuscript_ehrhart_volume_inequality`

has exactly the hypotheses and conclusion of Theorem 1. The public sharpness theorem

`Ehrhart.manuscript_ehrhart_bound_is_sharp`

states existential attainment; its proof invokes the internally explicit centered-simplex construction.

The principal mathematical correspondences are listed below.

Mathematical step	Lean declaration or module
Lattice count $N_k/k^n \to \mathrm{vol}(K)$	`monomial_count_div_pow_tendsto_volume` in `Ehrhart/Core.lean`
Empirical center $b_k \to 0$	`empiricalCenter_tendsto_zero` in `Ehrhart/LatticeMoments.lean`
Uniform radial exclusion	`eventually_no_large_multiple` in `Ehrhart/LatticeRadius.lean`
Terminal two-flags basis (aggregate form)	`TerminalFlagBasisExists` in `Ehrhart/TerminalFlagBasis.lean`
Protected product coefficient	`TerminalProductLemma` and `coeff_centeredLaurentProduct_zero_ne_zero`
Finite-field jet dimension bound	`finiteTorus_jet_finrank_lower_bound` in `Ehrhart/FiniteTorusJet.lean`
Finite-torus nilpotence	`torusMaximalIdeal_pow_eq_bot` in `Ehrhart/FiniteTorusAlgebra.lean`

Mathematical step	Lean declaration or module
Geometric no-wrap	`no_wrap_of_prime_large` in `Ehrhart/GeometricNoWrap.lean`
Exact finite obstruction	`obstruction_at_scale` in `Ehrhart/GeometricFiniteObstruction.lean`
Prime crossing	`primeRatio_tendsto_inflation` in `Ehrhart/PrimeCrossing.lean`
Final slack and upper bound	`volume_sub_sharp_le_slack` and `ehrhart_volume_inequality`
Explicit equality case	`exists_centeredBody_sharp` in `Ehrhart/SharpnessSynthesis.lean`

The project targets Lean 4.32.0 and mathlib 4.32.0. The accompanying `verification.log` records a successful build of all 8,682 jobs. The final upper-bound theorem, the sharpness theorem, the terminal-basis theorem, the protected-coefficient theorem, and the finite-torus obstruction have no `sorryAx` dependency. Their reported axiom dependencies are only

`propext`, `Classical.choice`, `Quot.sound`,

the standard foundations used by classical mathlib developments. The source also includes static checks against local `sorry`, `admit`, and nonstandard axiom declarations.

10 AI-assisted work

This work—research, mathematical development, formal verification, writing, and review—was produced with extensive use of AI systems, including large language models.