Pilz's Extended 1–2–3 Conjecture over every field

Sparse multiples of weighted integer intervals

23 October 2026

Abstract

We prove Pilz's Extended 1–2–3 Conjecture for every n, in a sharp weighted form valid over every field. For every field K, every $n \geq 1$ and all $c_1, \ldots, c_n \in K^\times$, every nonzero polynomial or Laurent-polynomial multiple of $\sum_{a=1}^{n} c_a \prod_p x_p^{v_p(a)}$ has at least n terms; Pilz's conjecture is the case $K = \mathbb{F}_2$, $c_a = 1$. The proof builds on the framework of Holdridge and Pach and adds support compression and descent in widths and exponent residues, which control cancellation over arbitrary fields, including imperfect ones. It yields a general finite-residue formula for polynomials completed by fresh variables. Further consequences include exact criteria for module coefficients and commuting monoid actions, a coefficient-rank bound, classification of equality at prime indices, and a universal inverse after fewer than n erasures. Every theorem stated here is machine-checked in an accompanying Lean 4 development.

Contents

1 Weighted integer intervals . . . 1
2 Elementary support tools . . . 4
3 Residue bounds . . . 9
4 Intervals with $n \geq 67$ . . . 12
5 Coefficients and consequences . . . 14
A The initial intervals through twenty-four . . . 17
B The middle intervals: 25 through 66 . . . 24
C Arithmetic estimates . . . 34

1 Weighted integer intervals

For each prime p, let x_p be an independent variable, and write

$$X(a) = \prod_p x_p^{v_p(a)} \qquad (a \geq 1).$$

Unique factorization gives $X(ab) = X(a)X(b)$. Put $[n] = \{1, \ldots, n\}$. All polynomials use finitely many variables. Write $\operatorname{wt} Q$ for the number of nonzero monomials of a polynomial Q, with $\operatorname{wt} 0 = 0$, and, for $Q \neq 0$, put

$$d(Q) = \min_{H \neq 0} \operatorname{wt}(QH).$$

Theorem 1.1 (Weighted interval theorem)**.** *For every field K, every $n \geq 1$, and every $c_1, \ldots, c_n \in K^\times$, the polynomial*

$$P_{n,c} = \sum_{a=1}^{n} c_a X(a)$$

satisfies $d(P_{n,c}) = n$. The same bound holds for Laurent polynomial multiples.

Equivalently, every nonzero finitely supported function $f : \mathbb{N}_{>0} \to K$ satisfies

$$(T_c f)(m) = \sum_{\substack{1 \le a \le n \\ a \mid m}} c_a f(m/a), \qquad |\operatorname{supp}(T_c f)| \ge n. \tag{1.1}$$

Indeed, the displayed sum is the coefficient of $X(m)$ in $P_{n,c} \sum_b f(b) X(b)$. A singleton input gives equality.

The original question is the special case $K = \mathbb{F}_2$, $c_a = 1$. Over $\mathbb{F}_2$, the coefficient of $X(m)$ in $P_{n,1} F_A$, where $F_A = \sum_{a \in A} X(a)$, is the parity of the number of representations $m = ab$ with $a \in A$ and $1 \le b \le n$.

Corollary 1.2 (Pilz's Extended 1–2–3 Conjecture)**.** *For every finite nonempty set A of positive integers and every $n \ge 1$,*

$$\left| \bigtriangleup_{a \in A} \{a, 2a, \dots, na\} \right| \ge n.$$

Equivalently, at least n integers have an odd number of ordered representations ab with $a \in A$ and $1 \le b \le n$.

Following [5], we write $A * [n]$ for the set in Corollary 1.2, the integers with an odd number of such representations. In the Lean development the corollary is `WeightedPilz.weighted_symmetric_difference`; see the end of this section.

A small example. With $x = X(2)$ and $y = X(3)$, the unweighted interval polynomial for $n = 4$ is $1 + x + x^2 + y$. Over every field,

$$(1 + x + x^2 + y)(1 - x) = 1 - x^3 + y - xy.$$

Cancellation removes two intermediate powers of x, yet four terms remain, attaining the bound. The nonmonomial cofactor also shows why equality at a composite index can differ from the prime-index rigidity in Corollary 5.7.

Remark 1.3 (Scope of the bound). The interval structure is essential. Over $\mathbb{F}_2$,

$$(1 + x + x^2)(1 + x) = 1 + x^3,$$

so the analogous bound fails for the three-element set $\{1, 2, 4\}$; this example is from [5, §1]. The nonzero-weight condition is also exact: for arbitrary $c_1, \dots, c_n \in K$, the inequality $\operatorname{wt}(P_{n,c} H) \ge n$ holds for every $H \ne 0$ if and only if every c_a is nonzero. Sufficiency is Theorem 1.1; necessity follows by taking $H = 1$, since the monomials $X(a)$ are distinct.

Historical context. The question originates in Pilz's study of the minimal distance of polynomial near-ring codes [1]. Pilz proved the bound for $n \le 6$, proved the general lower bound $\pi(n) + 2$, and reported that a computer search found no counterexample. Huang, Ke and Pilz [2] proved the interval-input case $A = [k]$, known as the 1–2–3 Conjecture, and stated the general problem as the Extended 1–2–3 Conjecture. Pach and Szabó [3] gave the number-theoretic formulation of Pilz's coding question, independently proved the case $A = [k]$, and improved the general lower bound to order $n/(\log n)^\lambda$ for every $\lambda > \lambda_0 \approx 0.2223$. Ke and Meyer [4] proved the conjecture for $|A| \le 3$ and showed that equality holds for arbitrarily large sets A, so the extremal configurations are far from unique. Nagy and Pach [6] proved the analogous statement for additive sumsets. Most recently, Holdridge and Pach [5] proved the conjecture for $n \le 8$ and for all $n \ge 2(3^{80} - 321)$, and proved a lower bound of order $kn/\log k$ when $k = |A|$ is small compared with n. Building on a formula of Ke and Meyer, they also studied the limiting density $h(A) = \lim_n |A * [n]|/n$, proving $h(A) \ge 8/7$ unless $A = \{a\}$ or $A = \{a, 2a\}$. Theorem 1.1 covers every n and extends the binary statement to arbitrary nonzero coefficients over every field.

This paper owes its foundations to Holdridge and Pach [5]. The encoding of integers by monomials in prime variables, the special role of the primes in $(n/2, n]$, slicing by prime valuations, the decomposition into smooth and rough components, and splitting estimates of the kind used in Section 4 and Appendix C all appear in their work, and the overall strategy for large n follows the path they opened.

What is new. The new ingredient is the treatment of multipliers that involve the primes in $(n/2, n]$. Support compression, Frobenius extraction with descent in base widths, and residue capacities (Sections 2 and 3) show that for $n \geq 67$ some minimum multiple has a cofactor that uses only the base variables, or, outside characteristic two, has the affine form $D + ZB$ with D and B in the base variables. After this reduction, component counting in the spirit of [5] closes the argument. These tools control cancellation uniformly in the weights and over every field, and the uniform argument applies from $n \geq 67$, compared with $n \geq 2(3^{80} - 321)$ in [5]; the initial and middle ranges are treated separately in the appendices.

Outline of the proof

A prime in $(n/2, n]$ occurs just once in the interval. Rescaling these variables gives

$$P_{n,c} = C + Z, \qquad Z = z_1 + \cdots + z_r, \qquad r = \pi(n) - \pi(n/2), \quad \operatorname{wt} C = n - r,$$

where $\pi(t)$ counts primes at most t. The variables z_i are fresh: none occurs in the core C. Each fresh variable records a separate copy of a base-only multiplier, so prime factors absent from a multiplier label groups of output terms that cannot cancel one another. For $n \geq 67$ the proof establishes three statements.

(i) *Reduction* (Sections 2–4). Some minimum multiple of $C + Z$ has cofactor $D + ZB$ with D, B in the base variables, and $B = 0$ in characteristic two.

(ii) *Weight formula* (equation (4.2)). Outside characteristic two,

$$\operatorname{wt}\big((C + Z)(D + ZB)\big) = \operatorname{wt}(CD) + r \operatorname{wt}(D + CB) + \binom{r+1}{2} \operatorname{wt} B.$$

(iii) *Base-only bound* (equation (4.1)). For every nonzero D in the base variables,

$$\operatorname{wt}((C + Z)D) = \operatorname{wt}(CD) + r \operatorname{wt} D \geq n. \tag{1.2}$$

For (i), a finite support shift (Lemma 2.5 and Theorem 2.6) combines the fresh variables into Z; the aggregate degree of a multiple is its degree in Z. In positive characteristic p, group these degrees modulo p: a correction divisible by $(C + Z)^p$ can be extracted from each exponent residue class (Lemma 2.7). For a hypothetical counterexample whose cofactor has least total width in the base variables (Lemma 2.8), every nonzero correction class has at least the target number of terms, and bounds on the residue classes of C^j exclude these corrections (Theorem 3.1). This gives a general finite-residue formula (Corollary 3.2). For $n \geq 67$ the fresh-prime estimate $r \geq \lfloor \sqrt{n} \rfloor$ makes it apply uniformly, and a row of aggregate degree three or more would already cost more than n terms.

Given (i) and (ii), endpoint bounds show that $B \neq 0$ already costs at least n terms, leaving (1.2). For (iii), delete terms until no further deletion preserves a counterexample. If the multiplier has u terms, a split at any prime q in its support forces $q < 2(u - 1)$ (Lemma 2.9). Prime factors absent from the multiplier then separate the output into disjoint components, and counting these components (Theorem C.2) excludes such a q.

The binary case. A reader interested only in Pilz's original statement, $K = \mathbb{F}_2$ and $c_a = 1$, can follow a shorter path. For $n \geq 67$ it uses, besides the basic tools of Section 2, Lemma 2.5, Theorem 2.6, Lemmas 2.7 and 2.8, Theorem 3.1 in its characteristic-two form (§3), and Corollary 3.2 with $p = 2$, which gives a base-only cofactor; then (4.1), via Lemma 2.9 and Theorem C.2. The weight formula in (ii) and the endpoint bounds are not needed. For $n \leq 66$ it uses Appendices A and B, specialised to characteristic two.

Section 5 gives the coefficient extensions: commuting monoid endomorphisms have the same sharp support bound precisely when each reflects zero. It also proves the rank bound $n + \rho - 1$, classifies equality at prime indices, and gives recovery after fewer than n erasures.

Range and dependency guide

Range	Main mechanism
$1 \leq n \leq 24$	Initial cores, endpoint and binomial bounds, and special cases (Appendix A).
$25 \leq n \leq 66$	Finite-residue capacities and exceptional cases, with a separate characteristic-two treatment (Appendix B).
$n \geq 67$	Uniform compression and descent, affine reduction, and component counting (Section 4).

The initial and middle ranges are proved uniformly over all fields, nonzero weights, and nonzero multipliers. Their tables certify integer inequalities used in these universal arguments, rather than testing a finite collection of polynomials. The large-range proof uses only the specified initial-case bounds and the independently proved arithmetic estimates of Appendix C; it does not assume the earlier unweighted interval theorem.

Formalisation and availability. This paper, its Lean 4 sources, and reproducible verification instructions are archived on Zenodo [7]. The development uses Lean 4.24.0 and mathlib revision `f897ebcf72cd16f89ab4577d0c826cd14afaafc7`, and depends only on the standard axioms `propext`, `Classical.choice` and `Quot.sound`. Its main declarations are `WeightedPilz.weighted_interval`, `WeightedPilz.weighted_interval_laurent`, `WeightedPilz.weighted_convolution`, and `WeightedPilz.weighted_symmetric_difference`. The last is stated for the set of Corollary 1.2, which is proved equal (`intervalSymmetricDifference_eq_oddProduct`) to the odd product `Pilz.oddProduct` of the earlier formal proof of the binary case. The file `WeightedPilz/PROOF_MAP.md` in the archive records the correspondence between this paper and the formal development. The formal development verifies the mathematical statements represented here, with explicitly documented alternative proofs of some intermediate results; it does not claim a line-by-line translation of the printed proof.
The same archive contains an earlier proof of the binary case $K = \mathbb{F}_2$, $c_a = 1$, which uses a square-root descent specific to characteristic two and has its own Lean 4 formalisation, and a short companion note proving that $h(A) \geq 4/3$ unless $A = \{a\}$ or $A = \{a, 2a\}$, the improvement anticipated by Holdridge and Pach [5, Remark 1.9]; the constant $4/3$ is attained by $A = \{1, 3\}$ [5, Lemma 5.6]. The weighted proof here does not use the earlier binary theorem as an input, although the two formal developments share their arithmetic estimates.

2 Elementary support tools

2.1 Basic operations and widths

Extending the coefficient field does not change $d(Q)$. For fixed finite sets of allowed cofactor and output exponents, the required cancellations form a homogeneous linear system over the original

field. It has a nonzero solution over an extension exactly when it has one over the original field, by equality of matrix ranks. Multiplication by $Q \neq 0$ is injective, so either solution gives a nonzero product.

A common monomial may be removed from a cofactor without changing the weight of its product. Polynomial and Laurent distances therefore agree. Variables absent from Q may also be removed: a nonzero coefficient slice of the cofactor gives a nonzero Q-multiple of no greater weight.

For a finite nonempty exponent set $A \subseteq \mathbb{Z}^a$ and an integer vector v, its width in direction v is $\max_{\alpha\in A} v\cdot\alpha - \min_{\alpha\in A} v\cdot\alpha$. The width of a nonzero polynomial means the width of its support. In particular $\operatorname{width}_{x_i} Q = \deg_{x_i} Q - \operatorname{ord}_{x_i} Q$. The highest and lowest occupied rows of a product are products of the corresponding factor rows. They are nonzero because a polynomial ring over a field is a domain. Consequently

$$\operatorname{width}_v(QH) = \operatorname{width}_v(Q) + \operatorname{width}_v(H). \tag{2.1}$$

Lemma 2.1 (Endpoint and dimension bounds)**.** *Suppose $Q = \sum_{i=0}^{a} Q_i y^i$, where $a > 0$ and $Q_0 Q_a \neq 0$. Then*

$$d(Q) \geq d(Q_0) + d(Q_a).$$

If the support of Q has affine dimension s over $\mathbb{Q}$, every nonzero multiple of Q has at least $s+1$ terms. In particular, a polynomial with a nonzero constant and a positive pure power of each of s variables has distance at least $s+1$.

Proof. The lowest and highest occupied y-rows of QH are distinct, and are nonzero multiples of Q_0 and Q_a respectively. This proves the first assertion.

For the second, let L_Q and L_{QH} be the rational spans of the support differences. If an integer vector v annihilates L_{QH}, then $\operatorname{width}_v(QH) = 0$. Equation (2.1) gives $\operatorname{width}_v(Q) = 0$, so v also annihilates L_Q. Ordinary rational linear algebra therefore gives $L_Q \subseteq L_{QH}$: otherwise a rational separating linear functional, multiplied by a common denominator, would contradict this implication. Thus the support of QH has affine dimension at least s and contains at least $s+1$ points. □

Lemma 2.2 (Exponent dilation)**.** *For every integer $q \geq 1$,*

$$d(Q(x_1^q, \ldots, x_a^q)) = d(Q).$$

Proof. Decompose any multiplier uniquely as

$$H(x) = \sum_{0\leq\alpha_i<q} x^\alpha H_\alpha(x_1^q, \ldots, x_a^q).$$

Its product with $Q(x_1^q, \ldots, x_a^q)$ has disjoint exponent residue classes, each nonzero class having the weight of the Q-multiple QH_α. This proves the lower bound. Substituting x_i^q into a multiple attaining $d(Q)$ proves the reverse bound. □

Lemma 2.3 (Power gap)**.** *Let C be nonmonomial and let $\delta = d(C)$. In characteristic zero, $\operatorname{wt}(C^j) \geq \delta + 1$ for every $j \geq 2$. In characteristic $p > 0$, the same conclusion holds whenever $j > 0$ is not a power of p.*

Proof. In characteristic zero, put $D = C$ and $h = j$. In characteristic p, remove a common monomial and the largest common exponent power p^s to write

$$C = x^\mu D(x_1^{p^s}, \ldots, x_a^{p^s}),$$

where two exponents of D differ modulo p. Write $j = p^e h$ with $p \nmid h$. Since j is not a power of p, we have $h \geq 2$. Exponent dilation and Frobenius give $d(D) = \delta$ and $\operatorname{wt}(D^h) = \operatorname{wt}(C^j)$.

In either case, let β be the lexicographically largest exponent of D. There is a coordinate i such that $(E_i - \beta_i)D \neq 0$, where $E_i = x_i\partial/\partial x_i$. Then

$$(E_i - h\beta_i)D^h = hD^{h-1}(E_i - \beta_i)D$$

is a nonzero D-multiple. The operator creates no monomials and deletes the leading term at exponent $h\beta$. Its weight is at least δ and at most $\mathrm{wt}(D^h) - 1$, as required. □

If $j > 0$ and $r \geq 1$, define

$$W_r(j) = \mathrm{wt}((z_1 + \cdots + z_r)^j), \qquad W_r(0) = 1.$$

In characteristic zero,

$$W_r(j) = \binom{r+j-1}{j}.$$

In characteristic p, write $j = \sum_e j_e p^e$, $0 \leq j_e < p$. Frobenius and the unique digit expansion of each exponent give

$$W_r(j) = \prod_e \binom{r+j_e-1}{j_e}. \tag{2.2}$$

In particular $W_r(j) \geq r$ for $j > 0$. If $r \geq 2$, equality occurs only at $j = 1$ in characteristic zero and at powers of p in characteristic p. Every other positive degree costs at least $\binom{r+1}{2}$. Different aggregate degrees have disjoint expanded supports.

2.2 Adding fresh variables

Theorem 2.4 (Sharp completion, including rigidity)**.** *Let $0 \neq C \in K[x]$, $c = \mathrm{wt}\, C$, $\delta = d(C)$, and let $z_1, \ldots, z_r$ be independent fresh variables. Then*

$$d(C + z_1 + \cdots + z_r) \geq \min\{c + r, \delta + 2r\}.$$

If $r > c - \delta$ and $c + r \geq 3$, every minimum multiple is a nonzero scalar monomial times $(C + z_1 + \cdots + z_r)^q$, where $q = 1$ in characteristic zero and q is a characteristic power otherwise.

Proof. For one new variable, remove the lowest power of z from a nonzero multiple G; divisibility survives since $C + z$ and z are coprime. Its constant row $A_0 \neq 0$ is divisible by C, by substituting $z = -C$. If $\mathrm{wt}\, G < \delta + 2$, exactly one positive-degree term remains, say Mz^j with M scalar monomial. Thus

$$G = M(z^j - (-C)^j).$$

The power gap excludes non-Frobenius exponents in this weight range. The remaining expressions have weight $c+1$. A monomial C is the elementary binomial case. Hence $d(C+z) \geq \min(c+1, \delta+2)$, and iteration gives the bound.

At the strict threshold, the polynomial obtained before adjoining the final fresh variable already has distance equal to its weight $c + r - 1 \geq 2$. A minimum multiple after adjoining that variable has weight $(c + r - 1) + 1 < (c + r - 1) + 2$. The one-variable argument gives its stated form, including the removed monomial factor. □

2.3 Combining the fresh variables

Put $Z = z_1 + \cdots + z_r$. We shall show that a sparsest multiple of $C + Z$ can be chosen to depend on the fresh variables only through Z. All weights still count monomials in the individual z_i. The proof moves allowed monomials towards earlier fresh variables until no further move is possible, then extracts a coefficient in the coordinates $z_1, \ldots, z_{r-1}, Z$.

Lemma 2.5 (A two-variable support shift)**.** *Fix $d \geq 0$, write $m_k = X^k Y^{d-k}$, and let $A \subseteq \{0, \ldots, d\}$. Apply the substitution $T_t : Y \mapsto Y + tX$, with X fixed. There is a set B of the same size as A with the following properties.*

1. *If $a_1 > \cdots > a_s$ and $b_1 > \cdots > b_s$ list A and B, then $b_i \geq a_i$ for every i.*
2. *The highest coefficient in t of any nonzero polynomial vector in $T_t\langle m_a : a \in A\rangle$ belongs to $\langle m_b : b \in B\rangle$.*
3. *If $B = A$, the span of the m_a is preserved by T_t.*

Membership in the shifted span is understood over $K(t)$.

Proof. Order the coordinates $m_d, \ldots, m_0$. Let B be the pivot set obtained by row reduction of the vectors $T_1 m_a$. Since

$$T_t m_a = \sum_{k \geq a} \binom{d-a}{k-a} t^{k-a} m_k,$$

a reduced basis $m_b + \sum_{k<b} \lambda_{b,k} m_k$ at $t = 1$ gives the basis

$$f_b(t) = m_b + \sum_{k<b} \lambda_{b,k} t^{k-b} m_k$$

at general t. Every nonpivot coefficient has negative degree in t. In an expansion $F(t) = \sum_b h_b(t) f_b(t)$, the coefficient h_b is exactly the pivot coordinate of F, and is therefore a polynomial when F is. The highest coefficient of F is consequently supported on the pivots. This proves the second assertion.

For each threshold k, the original columns indexed by $a \geq k$ remain independent on the rows indexed by exponents at least k: the submatrix on their original indices is triangular with diagonal 1. Thus there are at least as many pivots above each threshold as there are original indices, proving the first assertion.

Finally suppose $B = A$. Descend through the elements of A. The largest-index vector $T_1 m_a$ can have no term above a, for that would give a larger pivot. After subtracting already available larger monomials in A, the same argument applies to each subsequent vector. Hence T_1 preserves the coordinate span. All coefficients $\binom{d-a}{k-a}$ with $a \in A$ and $k \notin A$ are therefore zero in K, so the displayed formula proves preservation for formal t as well. □

Theorem 2.6 (Scalar support compression)**.** *Let $C \in K[x_1, \ldots, x_a]$, let $Z = z_1 + \cdots + z_r$ with $r \geq 1$, and put $P = C + Z$. Every nonzero P-multiple G has a nonzero replacement $F \in K[x, Z]$ divisible by P, with $\operatorname{wt} F \leq \operatorname{wt} G$. No base monomial occurring in F is new. In particular,*

$$\operatorname{width}_{x_i}(F) \leq \operatorname{width}_{x_i}(G) \qquad (1 \leq i \leq a).$$

Proof. The case $r = 1$ is immediate. A *profile* records a base exponent and a total fresh degree. Fill out the finitely many profiles occurring in G with all possible fresh monomials. Among the coordinate sets S having the same number of monomials in each profile as G, and whose span contains a nonzero P-multiple, choose one maximizing

$$\Phi(S) = \sum_{x^\gamma z^\beta \in S} \sum_{i=1}^{r} (r-i)\beta_i.$$

This is a maximum over a nonempty finite collection. Write V for the coordinate span of S, and choose $0 \neq G_0 \in V \cap (P)$.

Fix $i < j$. Partition S into blocks with the same base exponent, the same fresh exponents outside i, j, and the same sum of the ith and jth exponents. Apply Lemma 2.5 to the substitution $T_t : z_j \mapsto z_j + t z_i$ in every block. The resulting coordinate set S' has the same profile counts. It is still admissible: if D_t scales z_i by $1 - t$, then

$$T_t D_t(P) = P,$$

and $T_t D_t(G_0)$ is a nonzero polynomial in t, is divisible by P, and belongs to $T_t(V)$ over $K(t)$. Its highest coefficient in t is therefore a nonzero P-multiple in the span of S'.

The pivot comparison gives $\Phi(S') \geq \Phi(S)$, strictly if any block changes, because moving one exponent from z_j to z_i increases its weight by $j - i$. Maximality forces every block to remain unchanged. The final assertion of the lemma shows that V is preserved by every upper substitution $z_j \mapsto z_j + tz_i$. It is also preserved by diagonal scalings.

Now use the coordinates $u_i = z_i$ for $i < r$, together with Z. The substitution

$$u_i \mapsto \lambda_i u_i, \qquad Z \mapsto Z$$

is a composition of the preceding substitutions and scalings: in the original coordinates it sends z_i to $\lambda_i z_i$ for $i < r$, and sends z_r to $z_r + \sum_{i<r}(1 - \lambda_i)z_i$. It preserves both V and (P). Expand

$$G_0 = \sum_{\alpha} u^{\alpha} F_{\alpha}(x, Z).$$

Taking a nonzero coefficient of the independent parameters λ_i shows that $u^{\alpha} F_{\alpha} \in V \cap (P)$ for some $F_{\alpha} \neq 0$. Substitution $Z = -C$ and cancellation of u^{α} in the polynomial domain give $F_{\alpha}(x, -C) = 0$. Monic division then shows that P divides F_{α}. Removing the monomial u^{α} preserves weight and changes no base exponent, so $F = F_{\alpha}$ has all the required properties. □

2.4 Frobenius extraction and descent

In characteristic p, taking a pth power dilates every exponent by p. The next lemma reverses this operation on a residue class without requiring roots of arbitrary coefficients.

Lemma 2.7 (Frobenius extraction)**.** *Let K have characteristic $p > 0$, and let q be a power of p. Let P, E be polynomials over K in any finite set of variables. Suppose $0 \neq U = P^q E$ and every exponent of U is congruent to α modulo q, with $0 \leq \alpha_i < q$. Then there are polynomials J and $F = PJ \neq 0$ over K such that*

$$\alpha + q \operatorname{supp} F \subseteq \operatorname{supp} U, \qquad \alpha + q \operatorname{supp} J \subseteq \operatorname{supp} E.$$

In particular $\operatorname{wt} F \leq \operatorname{wt} U$ *and* $\operatorname{width}_{x_i} F \leq \operatorname{width}_{x_i} U/q$.

Proof. Multiplication by P^q preserves exponent residues and is injective, so every exponent of E has the same residue α. The subfield $K^q = \{a^q : a \in K\}$ acts on the finite-dimensional space spanned by the coefficients of E. All coefficients of U lie in that space. Choose a K^q-linear functional to K^q that is nonzero on one coefficient of U, and apply it coefficientwise. Since the coefficients of P^q lie in K^q, the resulting nonzero polynomial is still P^q times the image of E, and has support contained in $\operatorname{supp} U$. The image of E is $x^{\alpha} J^q$ for some J over K: its coefficients lie in K^q and its exponents have residue α. Thus the image of U is $x^{\alpha}(PJ)^q$. Take $F = PJ$. □

Lemma 2.8 (Descent in base widths)**.** *Let K have characteristic $p > 0$, let $0 \neq C \in K[x]$, and put*

$$c = \operatorname{wt} C, \qquad Z = z_1 + \cdots + z_r, \qquad P = C + Z, \qquad r \geq 1.$$

Fix an integer $1 \leq N \leq c + r$. If a nonzero P-multiple with fewer than N terms exists, choose $G = PH$ among them minimizing

$$b(H) = \sum_i \operatorname{width}_{x_i} H.$$

Then $b(H) > 0$, and G may be chosen in $K[x, Z]$. For this choice, let $0 \neq U \in (P^p)$ satisfy, for every base variable,

$$\operatorname{ord}_{x_i} U \geq \operatorname{ord}_{x_i} G, \qquad \deg_{x_i} U \leq \deg_{x_i} G + (p-1)\deg_{x_i} C. \tag{2.3}$$

Every nonzero full exponent-residue class of U modulo p then has at least N terms.

Proof. Compression does not increase the weight or any base width of G. By width additivity it does not increase any base width of H either, so it preserves the minimum defining $b(H)$.

If $b(H) = 0$, remove its base monomial to make H depend only on the fresh variables. Let c_0 be the constant coefficient of C, and put $\epsilon = 1$ if $c_0 \neq 0$, and 0 otherwise. The disjoint base rows give

$$\operatorname{wt}(PH) = (c - \epsilon) \operatorname{wt} H + \operatorname{wt}((c_0 + Z)H) \geq (c - \epsilon) + (r + \epsilon) = c + r \geq N,$$

a contradiction. Here $c_0 + Z$ has distance $r + \epsilon$ by its weight and the dimension bound in Lemma 2.1.

Write $U = P^p E$. Multiplication by P^p preserves full exponent residues, so a nonzero class U_α equals $P^p E_\alpha$. Lemma 2.7 gives a nonzero multiple PJ with $\operatorname{wt}(PJ) \leq \operatorname{wt} U_\alpha$ and base widths at most $1/p$ times those of U_α. Set $d_i = \deg_{x_i} C$. The fresh summand ensures $\operatorname{ord}_{x_i} P = 0$ and $\operatorname{width}_{x_i} P = d_i$. Thus

$$d_i + \operatorname{width}_{x_i} J \leq \frac{\operatorname{width}_{x_i} G + (p-1)d_i}{p} = d_i + \frac{\operatorname{width}_{x_i} H}{p}.$$

Consequently $b(J) \leq b(H)/p < b(H)$. Minimality gives $\operatorname{wt}(PJ) \geq N$, and hence $\operatorname{wt} U_\alpha \geq N$. □

2.5 A cut at a support prime

Normalize a multiplier D by removing its common monomial. Its *support primes* are the variables on which its exponents vary. A counterexample is *deletion minimal* if none of its nonzero proper subpolynomials remains a counterexample.

Lemma 2.9 (Directed cut)**.** *Let $u = \operatorname{wt} D$, and suppose every nonzero proper subpolynomial of D has product with $P_{n,c}$ of weight at least n. For any support prime q,*

$$\operatorname{wt}(P_{n,c}D) \geq 2n - 2(u-1)\left\lfloor \frac{n}{q} \right\rfloor.$$

In particular, a deletion-minimal counterexample satisfies $q < 2(u-1)$.

Proof. Write $D = L + H$, where L has zero q-valuation and H has q-valuation at least $b > 0$. Both products have weight at least n. If $u_0 = \operatorname{wt} L$, at most $u_0\lfloor n/q^b \rfloor$ positions of $P_{n,c}L$ can meet $P_{n,c}H$: only kernel terms divisible by q^b can reach that part. Therefore

$$\operatorname{wt}(P_{n,c}D) \geq 2n - 2u_0\lfloor n/q^b \rfloor.$$

Since $u_0 \leq u - 1$ and $q^b \geq q$, this proves the bound. A strict counterexample forces $q^b < 2u_0 \leq 2(u-1)$. □

3 Residue bounds

Group aggregate degrees modulo p. The governing estimate is simple: if a correction has at least N terms and the comparison polynomial has b terms in that class, the corrected class has at least $N - b$ terms and its weight changes by at least $N - 2b$. Lemma 2.8 supplies the lower bound N for every nonzero Frobenius correction. All weights below count monomials in the individual fresh variables.

Let K have characteristic $p > 0$, let $0 \neq C \in K[x_1, \ldots, x_a]$, and put

$$c = \operatorname{wt} C, \qquad Z = z_1 + \cdots + z_r, \qquad P = C + Z, \qquad r \geq 1.$$

For a base polynomial B, let $\sigma_p(B)$ be the largest number of its support exponents congruent coordinatewise modulo p, with $\sigma_p(0) = 0$. Put $w_j = \binom{r+j-1}{j}$ for $0 \leq j < p$. An expanded coefficient monomial multiplied by Z^j costs w_j fresh monomials. Replacing only this factor Z^j by $(-C)^j$, while holding all fresh pth powers fixed, contributes at most $\sigma_p(C^j)$ positions to any fixed exponent class. These are the cost and the possible cancellation that the reduction compares.

A residue-correction example. Over any field of characteristic two, take

$$C = 1 + x, \qquad Z = z_1 + z_2, \qquad T = Z^2 = z_1^2 + z_2^2, \qquad P = C + Z.$$

The multiple

$$G = P(P + T) = 1 + x^2 + xT + ZT = A_0 + ZA_1, \qquad A_0 = 1 + x^2 + xT, \quad A_1 = T,$$

has its aggregate degrees grouped modulo two. Replacing only the explicit factor Z by $-C = C$, while keeping the fresh square block T fixed, gives

$$U = A_0 + CA_1 = 1 + x^2 + T = P^2, \qquad V = G - U = PT.$$

Since $ZT = z_1^3 + z_1^2 z_2 + z_1 z_2^2 + z_2^3$, expansion in the individual fresh variables gives $\operatorname{wt} G = \operatorname{wt} V = 8$ and $\operatorname{wt} U = 4$. Aggregate degree modulo two is distinct from the full parity class $(a, b_1, b_2) \bmod 2$ of a monomial $x^a z_1^{b_1} z_2^{b_2}$. In the full zero class, V contributes T, whereas U contributes $1 + x^2 + T$; their sum is $1 + x^2$. Thus, with $b = 2$, the corrected class has exactly $\operatorname{wt} U - b = 2$ terms, and its weight changes by $\operatorname{wt} U - 2b = 0$. Extracting the square $U = P^2$ also returns P, whose cofactor has base width zero, compared with base width one for the cofactor $P + T$ of G. These identities illustrate the bookkeeping; the minimality assumption below supplies the general lower bound N for a nonzero correction class.

Theorem 3.1 (Residue capacities)**.** *Fix an integer $1 \le N \le c + r$. If a nonzero P-multiple with fewer than N terms exists, choose $G = PH$ as in Lemma 2.8 and write*

$$G = \sum_{j=0}^{p-1} Z^j A_j(x, Z^p), \qquad m = \operatorname{wt} G < N.$$

Define

$$u_j = \operatorname{wt} A_j, \qquad R = \sum_{j=1}^{p-1} w_j u_j, \qquad M = \sum_{j=1}^{p-1} \sigma_p(C^j) u_j,$$

$$U = \sum_{j=0}^{p-1} (-C)^j A_j, \qquad V = G - U.$$

Then $m = u_0 + R$, both U and V are P-multiples, and $U = P^p E$ with $E \in K[x, Z^p]$. Every nonzero full exponent-residue class of U has at least N terms.

If h is the number of nonzero correction classes of U, then

$$m \ge \operatorname{wt} V + h(N - 2M), \qquad h(N - M) \le m - R. \tag{3.1}$$

More precisely, if b_α is the weight in class α of the fresh-residue-zero part of V, then $b_\alpha \le M$ and

$$m \ge \operatorname{wt} V + \sum_{\alpha:\, U_\alpha \ne 0} (N - 2b_\alpha), \qquad \sum_{\alpha:\, U_\alpha \ne 0} (N - b_\alpha) \le m - R.$$

In particular, every class with $b_\alpha \le R$ has zero correction.

If $\kappa \le d(C)$ and $r\kappa \ge N$, the degree-zero aggregate row of G is nonzero, $u_0 \ge \kappa$, and

$$R \le N - 1 - \kappa. \tag{3.2}$$

Proof. Every fresh exponent of A_j is divisible by p. For $j < p$, the monomials of Z^j have exponents below p and nonzero multinomial coefficients. They occupy distinct fresh-residue sectors, also distinct for different j. Hence $m = u_0 + R$.

The polynomial

$$V = \sum_{j=1}^{p-1} (Z^j - (-C)^j) A_j$$

is divisible by P. Also U uses only fresh pth powers. Evaluating G at $Z = -C$, and writing $T = Z^p$, gives $U(x, -C^p) = 0$. Monic division in $K[x, T]$ yields

$$U = (T + C^p)E = P^p E, \qquad E \in K[x, Z^p].$$

Every base exponent in A_j occurs in G. Therefore, if $U \neq 0$,

$$\operatorname{ord}_{x_i} U \geq \operatorname{ord}_{x_i} G, \qquad \deg_{x_i} U \leq \deg_{x_i} G + (p-1) \deg_{x_i} C.$$

Lemma 2.8 now gives at least N terms in each nonzero residue class U_α.

The part of V with zero fresh residues is

$$B = -\sum_{j=1}^{p-1} (-C)^j A_j.$$

Each monomial of A_j contributes at most $\sigma_p(C^j)$ terms to a fixed full residue class, so $b_\alpha = \operatorname{wt} B_\alpha \leq M$. Adding a nonzero U_α leaves at least $N - b_\alpha$ terms and changes weight by at least $N - 2b_\alpha$. These classes are disjoint and lie in A_0, proving the capacity inequalities. If $b_\alpha \leq R$, a nonzero correction would force $u_0 \geq N - b_\alpha \geq N - R > m - R = u_0$. Thus that class is protected.

Finally, write $G = \sum_{j \geq k} g_j Z^j$ with $g_k \neq 0$. Evaluation at $Z = -C$ and cancellation of $(-C)^k$ give $g_k + \sum_{j>k} g_j (-C)^{j-k} = 0$, so $C \mid g_k$. If $k > 0$, its row has at least $W_r(k) \operatorname{wt} g_k \geq r\kappa \geq N$ terms. Hence $k = 0$ and $u_0 \geq \operatorname{wt} g_0 \geq \kappa$, proving (3.2). □

Three consequences will be used repeatedly. If $M \leq R$, then every correction class is protected and $U = 0$: a nonzero correction would leave at least $N - M$ terms in the zero fresh-residue part, in addition to the R terms already present elsewhere. If $\operatorname{wt} V \geq N$ and $2M \leq N$, equation (3.1) excludes a counterexample. If at most one correction class can occur and $\operatorname{wt} V \geq \max\{N, 2M\}$, it also excludes a counterexample.

3.1 The characteristic-two form

For $p = 2$, write $D = A_1$. Then

$$G = A_0 + ZD, \qquad U = A_0 + CD = P^2 E, \qquad V = PD, \qquad m = \operatorname{wt} A_0 + r \operatorname{wt} D. \tag{3.3}$$

Here $A_0, D \in K[x, Z^2]$. The polynomial D is nonzero: otherwise $G = U$, and one of its nonzero correction classes would already have at least N terms. If $r\kappa \geq N$, then

$$1 \leq u := \operatorname{wt} D \leq \left\lfloor \frac{N - 1 - \kappa}{r} \right\rfloor. \tag{3.4}$$

The capacities can be sharpened using the parity distribution. Let s_β count the support of C in base-parity class β, and let t_γ count the expanded terms of D in base-parity class γ. Then

$$b_\alpha \leq \sum_\gamma t_\gamma s_{\alpha - \gamma}.$$

If the positive t_γ form the decreasing partition $\lambda_1 \geq \lambda_2 \geq \cdots$ and the s_β are sorted decreasingly as $s_1 \geq s_2 \geq \cdots$, rearrangement gives the uniform bound $b_\alpha \leq \sum_i \lambda_i s_i$. Thus one may replace M by $\sum_i \lambda_i s_i$ in every capacity inequality.

If protection forces $U = 0$, decompose $D = \sum_\beta z^{2\beta} D_\beta(x)$. The products $z^{2\beta} P D_\beta$ have disjoint supports because the fresh exponents of P are zero or one. Thus a short PD would supply a short base-only multiple.

3.2 Finite-residue reduction

Corollary 3.2 (Uniform finite-residue formula)**.** *If*

$$\sigma_p(C^j) \le \binom{r+j-1}{j} \qquad (1 \le j < p),$$

then

$$d(P) = \min\left\{ \sum_{j=0}^{p-1} w_j \operatorname{wt} B_j : B_j \in K[x],\ (B_0,\dots,B_{p-1}) \neq 0, \sum_{j=0}^{p-1} (-C)^j B_j = 0 \right\}.$$

In particular, a minimum multiple can be chosen with aggregate output degree at most $p-1$ and cofactor degree at most $p-2$. For $p=2$ and $r \ge \sigma_2(C)$ this becomes

$$d(C+Z) = \min_{D\neq 0}\bigl(\operatorname{wt}(CD) + r \operatorname{wt} D\bigr).$$

Proof. The stated inequalities give $M \le R$, so $U = 0$ in Theorem 3.1. Expand each A_j in individual fresh-pth-power monomials. For each such monomial, its coefficient in $U = 0$ says $\sum_j (-C)^j B_j = 0$. Thus $\sum_j Z^j B_j$ is a P-multiple of aggregate degree at most $p-1$. These slices have disjoint expanded supports, so one is no heavier than the original G. To obtain the minimum formula, if $d(P) < c + r$ use the theorem with $N = d(P) + 1$. If $d(P) = c + r$, the polynomial P already attains the minimum in the claimed form. □

4 Intervals with $n \ge 67$

Theorem 4.1. *Theorem 1.1 holds for every $n \ge 67$ and every field.*

Throughout, remove the fresh primes in $(n/2, n]$ and rescale their variables, writing

$$P_{n,c} = C + Z, \qquad r = \pi(n) - \pi(n/2), \qquad \operatorname{wt} C = n - r,$$

and put $d_0 = 1 + \pi(n/2)$ and $R = r(r+1)/2$.

4.1 Multipliers in the base variables

For every nonzero D in the base variables,

$$\operatorname{wt}(CD) + r \operatorname{wt} D \ge n. \tag{4.1}$$

Otherwise delete dispensable terms and normalize D; by the slice argument of Section 2, a deletion-minimal D uses no variable absent from C. It cannot be monomial, which would give exactly n terms. Its largest support prime $q \le n/2$ satisfies $q < 2(\operatorname{wt} D - 1)$ by Lemma 2.9, contradicting the localized estimate (Theorem C.2).

4.2 A uniform affine reduction

Lemma C.9 gives $r \ge s := \lfloor \sqrt{n} \rfloor \ge 8$ for every $n \ge 67$. In characteristic $p > 0$, support indices of C^j are at most n^j. A full exponent class modulo p consists of integers ab^p with fixed pth-power-free part a, so

$$\sigma_p(C^j) \le \lfloor n^{j/p} \rfloor \qquad (1 \le j < p).$$

For $j = 1$ this is at most $s \le r$. For $j = 2 < p$,

$$n^{2/p} \le n^{2/3} < (s+1)^{4/3} \le s(s+1)/2 \le R,$$

where the middle inequality follows from $s^3 \geq 8(s+1)$. For $3 \leq j < p$,

$$\sigma_p(C^j) < n < (s+1)^2 < \binom{s+2}{3} \leq \binom{r+j-1}{j}.$$

Corollary 3.2 therefore gives a minimum multiple of aggregate degree at most $p-1$. Since P itself has n terms, a row of degree at least three would already cost more than n terms, so its degree is at most two. In characteristic two it is at most one. In characteristic zero, scalar compression and the same degree-three cost give degree at most two directly. Monic division by $C+Z$ now shows that a minimum multiple can be chosen with a base-only cofactor in characteristic two and an affine cofactor $D+ZB$ otherwise. Characteristic two is settled by (4.1).

In characteristic zero or odd characteristic, the exact expanded weight of the affine product is

$$m = \operatorname{wt}(CD) + r\operatorname{wt}(D+CB) + R\operatorname{wt}B. \tag{4.2}$$

If $B=0$, use (4.1). If $D=0$, the left side is $r\operatorname{wt}(CB)+R\operatorname{wt}B$, which is at least $\operatorname{wt}(CB)+r\operatorname{wt}B \geq n$. Otherwise $\operatorname{wt}(CD) \geq d_0$ by Lemma 2.1. For $n \geq 229$, we have $d_0 + R \geq n$. Indeed the thirteen blocks in Appendix C.3 prove this through 1799. For $1800 \leq n \leq 32768$, Lemma C.9 gives $R > n^2/1800 \geq n$; for $n \geq 32768$ it gives $R > 18n$. Thus the affine weight is already at least n throughout this range.

4.3 Endpoint bounds for $67 \leq n \leq 228$

Put

$$\kappa = 1 + \pi(\sqrt{n}) + \sum_{\substack{\sqrt{n}<q\leq n/2 \\ q \text{ prime}}} \left\lfloor \frac{n}{q} \right\rfloor, \qquad h = \pi(n/2) - \pi(\sqrt{n}).$$

The core has the decomposition

$$C = A + \sum_{\substack{\sqrt{n}<q\leq n/2 \\ q \text{ prime}}} x_q B_q,$$

where A is supported on the $\sqrt{n}$-smooth integers through n and B_q is a weighted interval of length $k_q = \lfloor n/q \rfloor \leq 15$. No two of the displayed large prime variables occur together. The initial-interval theorem gives $d(B_q) = k_q$, while the constant and pure-prime vertices give $d(A) \geq 1 + \pi(\sqrt{n})$. Repeated endpoint slicing therefore gives

$$d(C) \geq \kappa.$$

In characteristic different from two, the zero-large-variable row and the pure x_q^2-rows of C^2 are A^2 and B_q^2. They are disjoint. All these factors are nonmonomial, so the power-gap lemma gives

$$\operatorname{wt}(C^2) \geq d(A) + 1 + \sum_q (d(B_q)+1) \geq \kappa + h + 1. \tag{4.3}$$

The endpoint table in Appendix C.3 proves

$$\kappa + R + r \geq n, \qquad \kappa + R + h + 1 \geq n. \tag{4.4}$$

Suppose the affine weight in (4.2) were less than n, with $B, D \neq 0$. Since $R \geq r$, the first inequality forces B to be monomial and then forces $D + CB = 0$. The weight is consequently $\operatorname{wt}(C^2) + R$, which is at least n by (4.3) and the second inequality.

This completes the proof of Theorem 4.1.

Proof of Theorem 1.1. Theorem A.1 proves the result for $1 \leq n \leq 24$. Theorem B.1 covers $25 \leq n \leq 66$. Theorem 4.1 proves all $n \geq 67$. A nonzero scalar monomial multiplier has exactly n output terms, proving sharpness. Laurentization preserves support cardinality by Section 2. □

5 Coefficients and consequences

The field theorem says that erasing fewer than n outputs preserves injectivity. Over the ring of universal invertible weights, this gives a left inverse. The same inverse proves the support bound for every module, so erasure recovery and change of coefficients have a common algebraic source.

5.1 Erasure recovery

Fix a finite nonempty input support $S \subset \mathbb{N}_{>0}$, let $B = [n]S = \{ab : 1 \le a \le n,\ b \in S\}$, and erase $E \subseteq B$ with $|E| < n$. Over $A = \mathbb{Z}[t_1^{\pm 1}, \dots, t_n^{\pm 1}]$, form the matrix Q with rows $B \setminus E$, columns S, and entries

$$Q_{m,b} = \begin{cases} t_{m/b}, & b \mid m \text{ and } 1 \le m/b \le n, \\ 0, & \text{otherwise.} \end{cases}$$

Proposition 5.1 (Universal erasure inverse)**.** *There is a matrix L over A with $LQ = I_{|S|}$. It remains a left inverse when the t_a are specialized to units in any commutative ring.*

Proof. Modulo every maximal ideal, Q has full column rank by Theorem 1.1: a nonzero kernel vector would have at most $|E| < n$ outputs. In particular Q has at least $|S|$ rows. Thus the ideal of maximal minors lies in no maximal ideal and equals A. Choose $a_I \in A$ with $\sum_I a_I \det Q_I = 1$, where $Q_I = E_I Q$ and E_I selects $|S|$ rows. Then

$$L = \sum_I a_I \operatorname{adj}(Q_I) E_I \quad \text{satisfies} \quad LQ = I_{|S|}.$$

□

Remark 5.2 (Errors and erasures). The support bound also gives the standard unique-decoding criterion. Suppose the output of weighted interval convolution is received with at most t corrupted coordinates outside a known set of s erased coordinates. The finitely supported input is uniquely determined whenever $2t + s < n$. This holds over a field with nonzero weights and, by Theorem 5.3, for module-valued inputs when every weight acts injectively. Indeed, two compatible inputs f, g have outputs differing on at most $2t + s$ coordinates, whereas $f \neq g$ implies $|\operatorname{supp}(T_c(f - g))| \ge n$. This is a uniqueness statement; it does not assert an efficient decoding algorithm.

5.2 Modules and commuting actions

Theorem 5.3 (Module coefficients)**.** *Let $M \neq 0$ be a unital module over a commutative ring R, and let $c_1, \dots, c_n \in R$, where $n \ge 1$. Every nonzero finitely supported $f : \mathbb{N}_{>0} \to M$ satisfies $|\operatorname{supp}(T_c f)| \ge n$ if and only if each c_a acts injectively on M. The bound is sharp.*

Proof. Suppose first that the weights are units. If a nonzero input f had fewer than n outputs, put $S = \operatorname{supp} f$ and $E = \operatorname{supp}(T_c f)$. In Proposition 5.1, specialize $t_a = c_a$. The surviving-output matrix Q then acts on M^S and annihilates the vector of input values. Its left inverse gives $f = 0$, a contradiction.

For injective weight actions, localize at the multiplicative set U generated by the c_a. The map $M \to U^{-1}M$ is injective: an element maps to zero only if some $u \in U$ kills it. Input and output supports are unchanged, and all weights become units.

If some c_a kills $m \neq 0$, the singleton input $f(1) = m$ has at most $n - 1$ nonzero outputs. When all weight actions are injective, every nonzero singleton input has exactly n outputs. □

Corollary 5.4 (Commuting group actions)**.** *Let $G \neq 0$ be an abelian group and let $\varphi_1, \dots, \varphi_n$ be commuting endomorphisms. Then*

$$(T_\varphi f)(m) = \sum_{\substack{1 \le a \le n \\ a \mid m}} \varphi_a(f(m/a))$$

has at least n nonzero values for every nonzero finitely supported input if and only if every φ_a is injective.

Proof. Apply Theorem 5.3 to the commutative subring of $\mathrm{End}_{\mathbb{Z}}(G)$ generated by the identity and the φ_a. □

5.3 Commutative monoids

An endomorphism φ of an additive monoid *reflects zero* if $\varphi(m) = 0$ implies $m = 0$. On a group this is injectivity; on a monoid it is weaker, as $(x, y) \mapsto (x + y, 0)$ on $\mathbb{N}^2$ shows.

Theorem 5.5 (Monoid coefficients)**.** *Let $M \neq 0$ be a commutative additive monoid and let $\varphi_1, \ldots, \varphi_n$, $n \geq 1$, be commuting endomorphisms. Every nonzero finitely supported input satisfies $|\operatorname{supp}(T_\varphi f)| \geq n$ if and only if each φ_a reflects zero. The bound is sharp.*

Proof. Let $M^\times$ be the group of additively invertible elements of M, and suppose each weight reflects zero. Every endomorphism preserves $M^\times$, and its restriction to this group is injective. Put $\psi = \varphi_1 \cdots \varphi_n$; this map also reflects zero.

If $\psi(f(b)) \notin M^\times$ for some b, then $\varphi_a(f(b)) \notin M^\times$ for every a: applying the remaining endomorphisms to a unit would give a unit. Each output at ab, $1 \leq a \leq n$, therefore contains a nonunit summand and is nonzero, since a summand of a zero sum has an additive inverse.

Otherwise $h = \psi \circ f$ is a nonzero input with values in $M^\times$. Apply Corollary 5.4 to the restrictions of the weights to this group. Commutativity gives $T_\varphi h = \psi \circ T_\varphi f$, and the zero-reflecting property of ψ makes these two outputs have identical supports. Thus the required bound follows in this case as well.

A weight that kills a nonzero element gives a singleton input with fewer than n outputs. Zero-reflecting weights give exactly n outputs on every nonzero singleton input. □

The theorem also applies to semimodules over commutative semirings. Commutativity of the weight actions is essential. On $\mathbb{Q}^2$, put

$$B = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \qquad C = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Since $B^2 = C^2 = I$ and $BC + CB = 0$,

$$(I + Bx + Cy + \tfrac{1}{2}Ix^2)(I - Bx - Cy + \tfrac{1}{2}Ix^2) = I + \tfrac{1}{4}Ix^4 - Iy^2.$$

With $x = X(2)$ and $y = X(3)$, applying this identity to a nonzero vector gives four invertible interval weights and only three outputs.

5.4 Rank and equality

Theorem 5.6 (Coefficient rank)**.** *Let $n \geq 1$, let V be a vector space over K, let $c_1, \ldots, c_n \in K^\times$, and let $f : \mathbb{N}_{>0} \to V$ be nonzero and finitely supported. If $\rho = \dim_K \operatorname{span}\{f(b) : b \geq 1\}$, then*

$$|\operatorname{supp}(T_c f)| \geq n + \rho - 1.$$

Proof. The input values and the output values $g = T_c f$ span the same space. One inclusion is immediate; the other follows by induction on b from

$$c_1 f(b) = g(b) - \sum_{\substack{2 \leq a \leq n \\ a \mid b}} c_a f(b/a).$$

Choose $\rho - 1$ independent output values and a nonzero linear functional on $\operatorname{span}\{f(b) : b \geq 1\}$ vanishing on them. The projected input is nonzero, so Theorem 1.1 leaves at least n output positions. At least $\rho - 1$ original positions were removed. □

Corollary 5.7 (Equality at a prime index)**.** *Let V be a vector space over K, let $\ell \geq 3$ be prime, let $c_1, \ldots, c_\ell \in K^\times$, and put $P = P_{\ell,c}$. Every vector-valued Laurent multiple $G = PH$ with exactly ℓ nonzero coefficients has the form*

$$G = vMP^q, \qquad H = vMP^{q-1},$$

where $v \in V \setminus \{0\}$, M is a Laurent monomial, and $q = 1$ in characteristic zero or a power of the characteristic otherwise. If G is a polynomial, M has nonnegative exponents.

Proof. A monomial translation makes H polynomial. The rank bound forces its coefficients to span a line, so $H = vh$ for a scalar polynomial h. By Theorem 1.1, $d(P_{\ell-1,c}) = \operatorname{wt} P_{\ell-1,c} = \ell - 1$. Set $z = c_\ell x_\ell$, a fresh variable. The strict case of Theorem 2.4 gives $Ph = aMP^q$; absorb a into v and undo the initial monomial translation. Finally, P^q has nonzero constant term, so MP^q is polynomial only when M has no negative exponent. □

5.5 Consequences for the original Pilz conjecture

For a finite nonempty set $A \subset \mathbb{N}_{>0}$, write

$$S_n(A) = \bigtriangleup_{a \in A} \{a, 2a, \ldots, na\}, \qquad F_A = \sum_{a \in A} X(a) \in \mathbb{F}_2[\mathbf{x}], \qquad P_n = \sum_{a=1}^{n} X(a).$$

Corollary 5.8 (All equality cases at prime indices)**.** *Let $\ell \geq 3$ be prime. Then $|S_\ell(A)| = \ell$ if and only if there exist $b \geq 1$ and $e \geq 0$ such that*

$$F_A = X(b)P_\ell^{2^e-1}.$$

For these same b, e, the output is exactly

$$S_\ell(A) = \{ba^{2^e} : 1 \leq a \leq \ell\}.$$

Proof. Apply Corollary 5.7 over $\mathbb{F}_2$ to $P_\ell F_A$. Its nonzero scalar is 1, so $F_A = MP_\ell^{2^e-1}$ for a monomial M with nonnegative exponents. The constant term of $P_\ell^{2^e-1}$ is 1, including when $e = 0$. Thus M occurs in F_A, and $M = X(b)$ for some $b \in A$. Conversely, the displayed form gives

$$P_\ell F_A = X(b)P_\ell^{2^e} = \sum_{a=1}^{\ell} X(ba^{2^e})$$

by Frobenius. These ℓ monomials are distinct, proving equality and the claimed output set. □

The case $e = 0$ gives the singleton inputs $A = \{b\}$. The case $e = 1$ gives $A = b[\ell]$ and output $\{ba^2 : 1 \leq a \leq \ell\}$; higher e give the remaining equality families through the same polynomial formula.

Corollary 5.9 (Sharp parity refinement)**.** *For every $n \geq 1$,*

$$|S_n(A)| \equiv n|A| \pmod 2.$$

Consequently, if n is odd and $|A|$ is even, then $|S_n(A)| \geq n + 1$. This bound is sharp for every odd n.

Proof. Counting the $n|A|$ multiplicative representations modulo two gives the parity identity, also recorded in Holdridge–Pach [5]. Theorem 1.1 gives $|S_n(A)| \geq n$; an even integer at least the odd integer n is at least $n + 1$. For $A = \{1, 2\}$, the intersection $[n] \cap 2[n]$ has $\lfloor n/2 \rfloor$ elements, so

$$|S_n(\{1, 2\})| = 2n - 2\lfloor n/2 \rfloor = n + 1 \qquad (n \text{ odd}).$$ □

A The initial intervals through twenty-four

Theorem A.1. *For every field K, every $1 \le n \le 24$, and every choice $c_a \in K^\times$, the polynomial*

$$P = \sum_{a=1}^{n} c_a X(a)$$

satisfies $d(P) = n$.

Throughout this section, all coefficients in a displayed support are nonzero. Different occurrences of that support may have different coefficients. A dense polynomial of degree e has all $e+1$ coefficients nonzero. We use $x = x_2$, $y = x_3$, $z = x_5$, $w = x_7$, and $v = x_{11}$. Coefficients of fresh variables are absorbed by rescaling. An exponent is *distinguished* if it is 1 in characteristic zero or a power of the characteristic otherwise. Distinguished powers preserve weight.

A.1 Three elementary estimates

The endpoint bound says that if the lowest and highest coefficients in one variable are A and B, every nonzero multiple has at least $d(A) + d(B)$ terms. Each additional occupied row contributes at least one more term. We also use that a nonmonomial polynomial has no monomial multiple.

Lemma A.2 (A quadratic obstruction)**.** *Let $A, B, D \in K[x]$ be nonzero. If*

$$\frac{B^2}{AD}$$

is nonconstant, every nonzero multiple of $A + By + Dy^2$ has at least three occupied y-rows.

Proof. Suppose there were at most two occupied rows. After removing the lowest power of y, the quadratic would divide $U + Vy^k$ over $K(x)$, where $UV \neq 0$ and $k \ge 1$. Put

$$s = \frac{AD}{B^2}, \qquad y = -\frac{B}{D}t.$$

The quadratic becomes a nonzero scalar multiple of $t^2 - t + s$. Modulo this monic quadratic, write

$$t^k = a_k(s)t + b_k(s).$$

The coefficients are polynomials in s over the prime field, with $a_1 = a_2 = 1$ and $a_{k+1} = a_k - sa_{k-1}$. In particular every a_k has constant coefficient 1, so none is the zero polynomial. The binomial divisibility would force $a_k(s) = 0$. A nonconstant rational function in x is transcendental over K, so this is impossible. Indeed, after writing such a function as a reduced fraction, clearing denominators in a polynomial relation first forces its denominator to be constant, and then comparison of degrees forces its numerator to be constant as well. □

Lemma A.3 (Two rows and a binomial coefficient)**.** *Let $R \in K[x, \mathbf{y}]$ and let $D = d_0 + d_1 x$, with $d_0 d_1 \neq 0$. Suppose $\gcd(R, D) = 1$. If $R + Dt$ divides $U + Vt^k$, where $U, V \in K[x, \mathbf{y}]$, $UV \neq 0$, and $k \ge 1$, then, up to signs,*

$$U = R^k M, \qquad V = D^k M$$

for the same polynomial $M \in K[x, \mathbf{y}]$. If $\mathrm{wt}(V) \le 3$, then M is a monomial in $\mathbf{y}$ times a univariate polynomial in x.

In particular, if $d(R) \ge a$ and

$$\mathrm{wt}\big(R^k M_0(x)\big) > a \quad \text{for all } k \ge 1 \text{ and } 0 \neq M_0 \in K[x],$$

then $d(R + Dt) \ge a + 3$.

Proof. Substitution $t = -R/D$ and unique factorization give the first assertion. Each occupied $\mathbf{y}$-row of $D^k M$ is divisible by the nonmonomial D^k, so it has at least two terms. A polynomial of weight at most three can therefore have only one such row.

For the last assertion, endpoints give $a + 2$. A multiple with at most $a + 2$ terms must have exactly two t-rows, with a binomial upper row and a lower row of weight at most a. Extraction makes the lower row a monomial times $R^k M_0(x)$, contrary to the assumed bound. □

Lemma A.4 (Power estimates)**.** *Every positive power of a dense univariate polynomial of degree at least two has at least three terms. Consider also*

$$A = Q(x) + B(x)y + D(x)y^2,$$

where Q is dense of degree at least three and B is dense of degree at least one. In either of the following situations,

$$\mathrm{wt}(A^k M(x)) \geq 6 \qquad (k \geq 1,\ M \neq 0) :$$

1. *D is a nonzero constant;*
2. *D is a binomial with nonzero constant and linear coefficients.*

In the first situation $\mathrm{wt}(A^k) \geq \deg(B) + 5$; in the second, $\mathrm{wt}(A^k) \geq 7$.

Let $L = l_0 + l_1 x + l_2 y$ and $T = t_0 + t_1 x + t_2 x^2 + t_3 y$, with all coefficients nonzero. Then

$$d(L) = 3, \qquad d(T) = 4, \qquad \mathrm{wt}(L^k) \geq 3, \qquad \mathrm{wt}(T^k) \geq 4.$$

If $M(x)$ is nonmonomial, both $L^k M$ and $T^k M$ have at least four terms. A nondistinguished power of L has at least six terms, and a nondistinguished power of a binomial has at least three.

Proof. First let the exponent h be nonzero in the field. For a dense univariate polynomial of degree $e \geq 2$, the constant, linear, and leading coefficients of its hth power are nonzero, at the distinct degrees $0, 1, eh$.

The y-rows of $A^h M$ at degrees $2h, 2h-1, 0$ are

$$D^h M, \qquad hD^{h-1} BM, \qquad Q^h M.$$

If D is constant and M is nonmonomial, each row has at least two terms. If M is a monomial, their weights are at least $1, \deg(B) + 1, 3$. If D is a binomial, all three rows have at least two terms; when M is a monomial, the bottom one has at least three.

In characteristic p, write $k = qh$ with q a power of p and $p \nmid h$. Split $A^{qh} M$ into the residue classes of the x-exponent modulo q. Applying Lemma 2.7 to any nonzero class gives a support-contained polynomial $x^i (A^h M_i(x))^q$ with $M_i \neq 0$. The bounds just proved for h therefore imply the bound six for arbitrary k and M. For monomial M, the sharper power estimates follow directly from Frobenius. The univariate assertion follows the same way, or simply by applying Frobenius to the reduced power.

The distance of L follows from endpoints. The distance of T follows from sharp completion, Theorem 2.4, applied to a dense quadratic in x: $\min(3 + 1, 2 + 2) = 4$. The asserted bounds with nonmonomial M follow from the two y-endpoints, each of which has at least two terms. The bound for T^k follows from its monomial top row and the three-term bound for the bottom dense-quadratic power. Finally, the ordinary multinomial formula and its base-p digit version give at least six terms for a nondistinguished power of L, and at least three for a nondistinguished binomial power. □

A.2 A common test for adjoining fresh variables

Two support observations will supply the geometric part of the test. First, if a support meets at least b lines in every nonzero direction, a binomial multiple has at least $2b$ terms: the two endpoints on every occupied line survive. This remains true after translation or Frobenius dilation.

Second, consider

$$C = A(x, y) + \sum_{i=1}^{s} z_i B_i(x, y). \tag{A.1}$$

Its projection to the z_i-coordinates is the simplex $\{0, e_1, \ldots, e_s\}$. A translate of this simplex and a translate of its q-dilate, $q \geq 2$, meet in at most one point: two intersections would equate a nonzero vector with coordinates in $\{-1, 0, 1\}$ to q times another such vector. Thus two translated unequal distinguished powers of C overlap in at most one projected row. An A-to-A intersection has at most as many points as the largest exponent class of A modulo q; any other intersection has at most the smaller coefficient support's size.

Write $W_r(j) = \mathrm{wt}((u_1 + \cdots + u_r)^j)$. The digit formula gives $W_r(j) \geq r$ for $j > 0$. For $r \geq 2$, equality occurs exactly at distinguished degrees. For $r = 2, 3, 4$, every nondistinguished degree costs at least $3, 6, 10$, respectively. For $r = 2, 3$, equality in this lower bound occurs only in characteristic zero or odd characteristic, at twice a distinguished degree.

Lemma A.5 (A short fresh-row test)**.** *Let $P = C + Z$, where Z is a sum of $r \geq 2$ fresh variables. Put $c = \mathrm{wt}\, C$, $N = c + r$, and suppose $d(C) \geq \kappa$, $N \leq r(\kappa + 1)$ and $N - 1 - \kappa \leq 2r$. To prove $d(P) = N$, it suffices to check:*

1. *$\mathrm{wt}(C^j) + W_r(j) \geq N$ for every nondistinguished degree j with $W_r(j) \leq N - 1 - \kappa$;*
2. *every binomial multiple of a distinguished power of C has at least $N - 2r$ terms;*
3. *every nonzero sum of monomial translates of two unequal distinguished powers of C has at least $N - 2r$ terms.*

For $r = 2$ the same conclusion holds when $N - 1 - \kappa = 5$, provided one also checks

$$\mathrm{wt}(MC^q + LC^{2q'}) \geq N - 5$$

for nonzero scalar monomials M, L and distinguished q, q' in characteristic zero or odd characteristic.

Proof. Compress a hypothetical multiple of weight at most $N - 1$ and write it as $\sum_j A_j Z^j$. The coefficient of its lowest occupied Z-degree is divisible by C. If that degree were positive, the row would cost at least $r\kappa$. There must be another occupied row, since a single nonzero row cannot vanish at $Z = -C$; it costs at least r. This contradicts $N \leq r(\kappa + 1)$.

Thus $A_0 \neq 0$, $\mathrm{wt}\, A_0 \geq \kappa$, and the positive rows cost at most $2r$. Every such row costs at least r, and a nondistinguished degree costs strictly more than r. There are only three possibilities: a single monomial coefficient, a single binomial coefficient at a distinguished degree, or two monomial coefficients at distinct distinguished degrees. Evaluation at $Z = -C$ gives exactly the three conditions in the statement. A single distinguished monomial row already costs $c + r = N$.

If $r = 2$ and the budget is five, the only extra possibility is two monomial rows of costs two and three. A cost of three is possible only in characteristic zero or odd characteristic, at a degree $2q'$ with q' distinguished. The additional condition excludes it. □

A.3 The intervals through eight

The cases $n = 1, 2, 3$ are, respectively, a monomial, a binomial, and a three-term affine simplex; their distances are $1, 2, 3$. At $n = 4$, the polynomial is a dense quadratic in x plus a fresh variable. Sharp completion gives $\min(3 + 1, 2 + 2) = 4$. Adding the prime-5 variable gives $n = 5$.

For $n = 6$ and $n = 7$, remove the one or two fresh prime terms. The remaining five-term core is

$$Q_2(x) + D(x)y,$$

where Q_2 is dense quadratic and D is a nondegenerate binomial. Its two endpoint rows each have distance at least two, so its distance is at least four. Completion gives $\min(5 + r, 4 + 2r) = 5 + r$ for $r = 1, 2$. At $n = 8$, replace Q_2 by a dense cubic. The core now has six terms and still has distance at least four; the two fresh variables give $\min(6 + 2, 4 + 4) = 8$.

A.4 Five quadratic bases

The core estimates all start from the following polynomials:

$$A_\nu = Q_a(x) + B_b(x)y + D(x)y^2.$$

Here Q_a, B_b are dense of the indicated degrees, and D is either a nonzero constant or a nondegenerate binomial.

ν	a	b	D	$\mathrm{wt}(A_\nu)$	$d(A_\nu) \geq$	$\mathrm{wt}(A_\nu^k) \geq$
9	3	1	constant	7	4	6
12	3	2	constant	8	4	7
16	4	2	constant	9	4	7
18	4	2	binomial	10	5	7
24	4	3	binomial	11	5	7

For all five bases, Lemma A.4 gives $\mathrm{wt}(A_\nu^k M(x)) \geq 6$ whenever $k \geq 1$ and $M \neq 0$. Except at $\nu = 16$, the numerator and denominator of $B_b^2/(Q_a D)$ have different degrees. Lemma A.2 therefore forces three y-rows. Their endpoint costs give the distance entries. In particular,

$$d(A_9) \geq 4, \qquad \mathrm{wt}(A_9^k) \geq 6, \tag{A.2}$$

$$d(A_{12}) \geq 4, \qquad \mathrm{wt}(A_{12}^k M) \geq 6, \qquad \mathrm{wt}(A_{12}^k) \geq 7, \tag{A.3}$$

$$d(A_\nu) \geq 5, \qquad \mathrm{wt}(A_\nu^k M) \geq 6, \qquad \mathrm{wt}(A_\nu^k) \geq 7 \quad (\nu = 18, 24). \tag{A.4}$$

At $\nu = 16$, only the case in which $B_2^2/(Q_4 D)$ is constant needs attention. Write $D = g$ and $Q_4 = \lambda B_2^2$, with $g\lambda \neq 0$. A three-term multiple would have two y-rows: a binomial lower row $U(x)$ and a monomial upper row $V(x)y^k$. Substitute $y = B_2 t$ and reduce modulo $\lambda + t + gt^2$. In this two-dimensional quotient t is a unit, so the remainder $a + bt$ of t^k is nonzero. Divisibility forces $b = 0$, hence $a \neq 0$ and $U = -aVB_2^k$. Lemma A.4 gives at least three terms in B_2^k, a contradiction. Thus $d(A_{16}) \geq 4$ as well.

A.5 The core extensions

Let $L = l_0 + l_1 x + l_2 y$, let $T = t_0 + t_1 x + t_2 x^2 + t_3 y$, and let D_i denote nondegenerate binomials in x. The following table describes the cores obtained by removing the primes in $(n/2, n]$ from the indicated intervals. The last column is a lower bound for their distance.

n	C_n	$\mathrm{wt}(C_n)$	κ
9	A_9	7	4
12	$A_{12} + D_1 z$	10	7
14	$A_{12} + D_1 z + D_2 w$	12	10
15	$A_{12} + Lz + D_2 w$	13	10
16	$A_{16} + Lz + D_2 w$	14	10
18	$A_{18} + Lz + D_2 w$	15	11
20	$A_{18} + Tz + D_2 w$	16	12
21	$A_{18} + Tz + Lw$	17	12
22	$A_{18} + Tz + Lw + D_3 v$	19	15
24	$A_{24} + Tz + Lw + D_3 v$	20	15

We prove the entries by three applications of the same endpoint argument.

First, put $E = A_{12} + D_1 z$. The constant y^2 coefficient gives $\gcd(A_{12}, D_1) = 1$. Lemma A.3, followed by the power endpoint bounds, gives

$$d(E) \geq 7, \qquad \mathrm{wt}(E^k M(x)) \geq 8, \qquad \mathrm{wt}(E^k) \geq 9. \tag{A.5}$$

A second binomial extension therefore has distance at least 10, proving the entries for C_{12} and C_{14}.

Next put $F_\nu = A_\nu + Lz$ for $\nu = 12, 16, 18, 24$. Endpoints give $d(F_\nu) \geq d(A_\nu) + 3$, and

$$\mathrm{wt}(F_\nu^k M(x)) \geq 10 \qquad (k \geq 1, M \neq 0). \tag{A.6}$$

Indeed, for nonmonomial M the two endpoint costs are at least $6 + 4$; for monomial M they are at least $7 + 3$. In particular,

$$d(F_\nu) \geq 8, \qquad \mathrm{wt}(F_\nu^k M(x)) \geq 10 \quad (\nu = 18, 24). \tag{A.7}$$

The coefficient of yz in F_ν is a nonzero constant, so $\gcd(F_\nu, D_2) = 1$. A binomial extension raises the stated distance bound by three, giving the entries for C_{15}, C_{16}, C_{18}. For C_{15} and C_{16} we also need a bare-power bound:

$$\mathrm{wt}(C_n^k) \geq 16 \qquad (n = 15, 16; k \text{ nondistinguished}).$$

Remove the characteristic-power factor of k, leaving $h \geq 2$ nonzero in the field. The z-endpoints of F_ν^h cost at least $7 + 6 = 13$, and the binomial w-endpoint of C_n^h costs at least three. Frobenius preserves this bound.

Finally, for $\nu = 18, 24$ put $E_\nu = A_\nu + Tz$ and $H_\nu = E_\nu + Lw$. Endpoints give

$$d(E_\nu) \geq 9, \qquad \mathrm{wt}(E_\nu^k M(x)) \geq 10, \qquad \mathrm{wt}(E_\nu^k) \geq 11. \tag{A.8}$$

Here the power costs are $6 + 4$ for nonmonomial M and $7 + 4$ for monomial M. Consequently $d(H_\nu) \geq 12$, and

$$\mathrm{wt}(H_\nu^k M(x)) \geq 14. \tag{A.9}$$

The latter costs are $10+4$ or $11+3$, according as M is nonmonomial or monomial. The coefficients of yz in E_ν and of yw in H_ν ensure coprimality with every D_i. Lemma A.3 now gives distance at least 12 for $E_{18} + D_2 w$, and at least 15 for $H_\nu + D_3 v$. This proves the remaining entries.

A.6 The mixed power at sixteen

Only one additional mixed-power estimate is needed. Write $C_{16} = A_{16} + Lz + Dw$, as in the core table. In characteristic different from two, its square has six distinct (z, w)-rows, with coefficients

$$A_{16}^2, \quad 2A_{16}L, \quad 2A_{16}D, \quad L^2, \quad 2LD, \quad D^2.$$

Their weights are at least $4, 4, 4, 4, 4, 3$, respectively. The first three bounds follow from $d(A_{16}) \geq 4$. The power gap gives $\mathrm{wt}(L^2) \geq 4$; the two y-endpoints of LD each cost two; and a nondegenerate binomial square has three terms.

For distinguished q, q', these six rows remain distinct in $C_{16}^{2q'}$, while a monomial translate of C_{16}^q occupies only three (z, w)-rows. At least three square rows are untouched. Thus, for nonzero scalar monomials M, N,

$$\mathrm{wt}(MC_{16}^q + NC_{16}^{2q'}) \geq 4 + 4 + 3 = 11. \tag{A.10}$$

A.7 Applying the fresh-row test

We now collect the estimates needed in Lemma A.5. In the table, b is a lower bound for the number of parallel lines in any direction, and o bounds the overlap of two translated unequal distinguished dilates of the core support.

n	c	r	κ	b	o	relevant nondistinguished powers
9	7	2	4	3	3	weight at least 6
12	10	2	7	4	3	weight at least 9
15	13	2	10	6	3	weight at least 16
16	14	2	10	6	4	weight at least 16; mixed bound 11
18	15	3	11	6	4	weight at least 12
21	17	4	12	7	4	none fit the budget
22	19	3	15	8	4	weight at least 16
24	20	4	15	8	4	none fit the budget

Here is a uniform verification of the geometric columns. Each base A_ν requires at least three lines: a horizontal direction sees three y-levels, and any other direction separates its four or five x-axis points. Each L- or T-slice needs at least two lines, and each D_i-slice at least one. Adding these counts gives b for directions in the xy-plane. A direction outside that plane separates all the points of A_ν, giving at least the same bound.

For overlaps, use (A.1). Every exponent class of a cubic base modulo $q \geq 2$ has at most three points, and every class of a quartic base has at most four. For $q = 2$, the largest possible quartic class is $\{1, x^2, x^4, y^2\}$; for $q \geq 3$, there are at most two points in a class. The other coefficient slices have at most three terms in the cubic cases and four in the quartic cases. This proves the column o, including the unsliced base C_9.

In every row, $n \leq r(\kappa + 1)$ and the positive-row budget $n - 1 - \kappa$ is at most $2r$, except at $n = 16$, where it is five. The binomial and unequal-dilate conditions follow from

$$2b \geq n - 2r, \qquad 2c - 2o \geq n - 2r.$$

The power estimates prove the remaining condition. At $n = 18, 22$, the power gap gives weights at least $\kappa + 1 = 12, 16$, respectively; adding the fresh-row cost of at least six gives n. At $n = 21, 24$, every nondistinguished degree costs at least ten, exceeding the budget eight. At $n = 16$, use (A.10) as well. Thus all eight rows follow from Lemma A.5.

The two cores omitted from this last table follow directly from sharp completion:

$$d(P_{14}) \geq \min(12 + 2, 10 + 4) = 14, \qquad d(P_{20}) \geq \min(16 + 4, 12 + 8) = 20.$$

Finally, adjoining the fresh prime variable gives the cases $13, 17, 19, 23$ from $12, 16, 18, 22$, respectively. Together with the cases through eight, this leaves only $10, 11$.

A.8 The tenth and eleventh intervals

Let $C = A_9$, let $D = d_0 + d_1 x$, and set

$$E = C + Dz, \qquad P = E + w.$$

The support of P is the tenth interval. We first establish the following statements about its nine-term core E:

$$d(E) \geq 7, \tag{A.11}$$

every E-multiple of weight at most seven has three z-rows of weights $(4, 1, 2)$; (A.12)

$$\mathrm{wt}(E^j) \geq 9 \quad (j \geq 1), \tag{A.13}$$

$$\mathrm{wt}(HE^j) \geq 8 \quad \text{if } H \text{ is a binomial.} \tag{A.14}$$

The strengthened core estimate

$$\mathrm{wt}(C^j M(x)) \geq 6 \qquad (M \neq 0)$$

is Lemma A.4. Endpoints first give $d(E) \geq 6$. A multiple of weight at most seven with exactly two z-rows has lower row of weight at least four and upper row of weight at most three. Since

the coefficient of y^2 in C is a nonzero constant, $\gcd(C, D) = 1$. Lemma A.3 makes the lower row a monomial times $C^j M(x)$, costing at least six, and the upper row costs at least two. This is impossible. There are therefore at least three rows. Their endpoint costs are four and two, which proves (A.11) and the forced shape (A.12).

Distinguished powers of E have nine terms. For any other exponent, remove its largest characteristic-power factor and use a reduced exponent $h \geq 2$ that is nonzero in the field. The z-rows of E^h at degrees $h, h-1, 0$ are

$$D^h, \qquad hD^{h-1}C, \qquad C^h.$$

Their weights are at least $2, 4, 6$, giving at least twelve terms and proving (A.13).

For (A.14), write $j = qh$, with q distinguished and h nonzero in the field; in characteristic zero take $q = 1$. The support of E^j contains the three x-axis points at exponents $0, q, 3j$. Its support also contains the four affinely independent endpoint points $(0,0,0), (3j,0,0), (0,2j,0), (0,0,j)$, so it has affine dimension three. In a direction not parallel to the x-axis these three points lie on different parallel lines. If those were the only occupied lines, the support would lie in the plane generated by that direction and the x-axis, a contradiction. In the x-direction, four nonzero rows have (y, z)-coordinates

$$(0,0), \quad (2j,0), \quad (2j-q,0), \quad (0,j).$$

They come from the bottom, top, next-to-top, and final endpoint rows described above. Thus every direction meets at least four lines, and a binomial product has at least eight terms.

We need one last consequence of the forced shape:

$$\mathrm{wt}(ME^i + NE^j) > 7 \quad (1 \leq i < j) \tag{A.15}$$

for any nonzero scalar monomials M, N, provided the sum is nonzero. Suppose otherwise. Write $M = z^a M_0(x,y)$ and $N = z^b N_0(x,y)$. If $a \neq b$, the lowest z-row is a monomial times a power of C, which costs at least six, contradicting its forced weight four. Thus $a = b$, and we remove this common z-power. The resulting constant row is nonzero: its vanishing would make the positive power C^{j-i} a scalar Laurent monomial, impossible for a nonmonomial C. The top row is $N_0 D^j$ and has exactly two terms. Hence j is distinguished. Characteristic zero is impossible because $j > i \geq 1$. In characteristic p, E^j has just the two z-rows of degrees zero and j. Every positive z-row of $M_0 E^i$ below degree j survives unchanged. Exactly three rows in the sum force E^i to have only two rows, so the binomial digit formula forces i to be distinguished as well. The middle row is then $M_0 D^i$, of weight two, contradicting its forced weight one. This proves (A.15).

Now suppose a P-multiple has at most nine terms. Remove its lowest w-power, an operation that preserves both weight and divisibility, and write it as

$$U + \sum_{j>0} A_j w^j, \qquad U \neq 0.$$

Substitution $w = -E$ shows $E \mid U$, so $\mathrm{wt}(U) \geq 7$. At most two terms remain at positive w-degrees. If these form one monomial row, (A.13) gives total weight at least $9 + 1 = 10$. If they form one binomial row, (A.14) gives at least $8 + 2 = 10$. If they form two monomial rows, (A.15) excludes the required constant row of weight at most seven. This proves $n = 10$. Adding the fresh prime-11 variable and applying Theorem 2.4 proves $n = 11$. This completes the proof of Theorem A.1.

B The middle intervals: 25 through 66

Theorem B.1 (The middle intervals)**.** *For every field K, every $25 \le n \le 66$, and every choice $c_a \in K^\times$, the polynomial*

$$P = P_{n,c} = \sum_{a=1}^{n} c_a X(a)$$

satisfies $d(P) = n$.

The constant multiplier gives $d(P) \le n$. For the lower bound we first control small multipliers, then use residue descent to reduce the remaining cases to them.

After rescaling the variables belonging to primes in $(n/2, n]$, write

$$P = C + Z, \qquad Z = z_1 + \cdots + z_r, \qquad r = \pi(n) - \pi(\lfloor n/2 \rfloor), \quad c = \mathrm{wt}(C) = n - r, \quad R = \binom{r+1}{2}. \tag{B.1}$$

The remaining variables are the base variables.

B.1 Small multipliers

First put

$$d_0 = 1 + \pi(\lfloor \sqrt{n} \rfloor) + \sum_{\substack{\sqrt{n} < q \le n/2 \\ q \text{ prime}}} \left\lfloor \frac{n}{q} \right\rfloor. \tag{B.2}$$

Then $d(C) \ge d_0$. Indeed, each prime variable x_q with $\sqrt{n} < q \le n/2$ occurs linearly, and two such variables never occur together. Its coefficient is a weighted interval of length $\lfloor n/q \rfloor \le 6$, whose distance is that length by the initial theorem. Repeated endpoint slicing adds these distances to the lower bound $1 + \pi(\lfloor \sqrt{n} \rfloor)$ for the remaining smooth core. That lower bound follows from its constant and pure-prime vertices.

Lemma B.2 (Six input terms)**.** *For $25 \le n \le 66$, over every field and with arbitrary nonzero weights,* $\mathrm{wt}(PD) \ge n$ *whenever* $1 \le \mathrm{wt}(D) \le 6$.

Proof. A monomial input gives exactly n terms. Otherwise choose a counterexample minimal under term deletion and normalize it. If it has u terms and largest support prime q, the directed cut gives $q < 2(u-1) \le 10$. Thus $q \in \{2, 3, 5, 7\}$, and the respective minimum possible values of u are $3, 3, 4, 5$.

Let $C_q(t)$ count integers through t with no prime factor at most q. Split the output by its q-rough part, using the component bounds of Lemma C.1.

For $q = 2$, every component costs at least two, so the output has at least $2C_2(n) = 2\lceil n/2 \rceil \ge n$ terms. For $q = 3$, the lower bound is

$$3C_3(n) + C_3(n/2) - C_3(n/3).$$

The residues $1, 5$ modulo six give $3C_3(n) \ge n - 1$. Their successive gaps are at most four, while $(n/3, n/2]$ has length greater than four. The remaining difference is therefore at least one.

For $q = 5$, every component costs at least four. Write $n = 30h + s$, $0 \le s < 30$, and let $R(s)$ count the members of $\{1, 7, 11, 13, 17, 19, 23, 29\}$ not exceeding s. The eight gaps give $4R(s) - s \ge -2$. Thus

$$4C_5(n) - n = 2h + 4R(s) - s \ge 0 \qquad (n \ge 30).$$

For $25 \le n \le 29$, the same residue list gives $4C_5(n) \ge n$.

For $q = 7$, the successive component costs are $5, 4, 6, 6, 8, 8, 5, 5, \ldots$. Their sum is

$$H(n) = 5C_7(n) - C_7(n/2) + 2C_7(n/3) + 2C_7(n/5) - 3C_7(n/7).$$

Here are six short intervals on which monotonicity proves $H(n) \geq n$. For $a \leq n \leq b$, evaluate $C_7(n/d)$ at a/d in terms with positive coefficients and at b/d in terms with negative coefficients. The resulting lower bound is B:

a	b	$C_7(a)$	$C_7(b/2)$	$C_7(a/3)$	$C_7(a/5)$	$C_7(b/7)$	B
25	28	6	3	1	1	1	28
29	33	7	3	1	1	1	33
34	38	8	5	2	1	1	38
39	45	9	5	3	1	1	45
46	54	11	6	3	1	1	54
55	66	13	8	4	2	1	66

The 7-rough integers through 66 are

$$1, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61,$$

obtained by removing multiples of seven from the eight residues modulo thirty. In every row $B = b$. □

The two minimum columns in the finite budget table (B.7) give

$$d_0 + 7r \geq n, \qquad rd_0 > n. \tag{B.3}$$

If D uses only base variables, then

$$\operatorname{wt}(PD) = \operatorname{wt}(CD) + r \operatorname{wt}(D) \geq n.$$

For at most six terms this is Lemma B.2; for at least seven it follows from (B.3). We shall call this the base-variable bound.

B.2 Unique products and the odd-characteristic affine bound

In this subsection assume $\operatorname{char} K \neq 2$. Let A be the integer support of C, and define

$$S = \{ab : a, b \in A\},$$
$$U = \{m \in S : \#\{(a, b) \in A^2 : a \leq b,\ ab = m\} = 1\}.$$

Put $g = |U|$. At each position in U, the square coefficient is c_a^2 or $2c_ac_b$, hence nonzero. Thus $\operatorname{wt}(C^2B) \geq g$ for every monomial B.

Lemma B.3 (Lines parallel to a binomial)**.** *Let F be a nonzero polynomial and let B have exactly two terms. If the exponent support of F occupies h affine lines parallel to the difference of the two exponents of B, then* $\operatorname{wt}(FB) \geq 2h$.

Proof. On each occupied line, the two extreme terms of the product have unique contributing pairs and nonzero coefficients. Different lines remain disjoint after multiplication by either term of B. □

We use two elementary observations about the number of occupied lines. A support of affine dimension d occupies at least d lines in any fixed nonzero direction. If it contains four distinct collinear points, and the chosen direction is not parallel to that line, it occupies at least $d+2$ lines. Indeed, projection along the direction has affine dimension at least $d-1$. The four points give four distinct collinear images; at least $d-2$ further points are needed to obtain that dimension.

Lemma B.4 (Four small square bounds)**.** *Assume* $\operatorname{char} K \neq 2$*, and let C be the weighted core in* (B.1)*. For every binomial B, including one involving additional variables,*

$$\operatorname{wt}(C^2B) \geq \begin{cases} 16, & n = 26, \\ 44, & n = 27, 28, \\ 20, & n = 40. \end{cases}$$

Proof. Write $x = x_2$. First consider $n = 26$ or 40. The support of C^2 has affine dimension $d = 6$ or 8, respectively: its constant term and its extreme pure powers in the d prime variables are nonzero. The pure-x part of C is a dense polynomial of degree $e = 4$ or 5. Its square has nonzero terms at exponents $0, 1, 2e-1, 2e$. Thus, in every direction other than the x-direction, it occupies at least $d+2$ lines. In the x-direction the following odd integer positions already give $d+2$ distinct occupied lines:

$$\begin{array}{c|l} n = 26 & 1, 3, 5, 7, 11, 13, 49, 121, \\ n = 40 & 1, 3, 5, 7, 11, 13, 17, 19, 49, 121. \end{array}$$

These square coefficients cannot vanish: the prime positions have unique products $1 \cdot p$, and $49 = 7^2$ and $121 = 11^2$ have unique products in the core. Lemma B.3 proves the bounds 16 and 20.

Now let $n = 27$ or 28. Put $u = x_{11}$ and $v = x_{13}$. Then

$$C = A + uL + vM,$$

where A uses only x_2, x_3, x_5, x_7 and L, M are nondegenerate binomials in x. The six (u, v)-slices of C^2 are

$$A^2, \qquad 2AL, \qquad 2AM, \qquad L^2, \qquad 2LM, \qquad M^2.$$

We show that their union occupies at least 22 lines in every direction.

First, A^2 has at least 22 terms. To see this, set $x = 0$, and write $y = x_3, z = x_5, w = x_7$. The resulting polynomial is

$$A_{\text{odd}} = Q(y) + zR(y) + az^2 + wS(y),$$

where Q is a dense cubic, R, S are nondegenerate binomials, and $a \neq 0$. In its square, the lower bounds for the z-row weights at successive w-degrees are

w-degree	z-row lower bounds	total
0	$(4, 2, 1, 2, 1)$	10
1	$(2, 2, 2)$	6
2	(3)	3.

Here Q^2 has nonzero endpoint and adjacent-endpoint coefficients; $R^2 + 2aQ$ has a nonzero cubic coefficient; all other bounds follow from endpoints. Hence $\mathrm{wt}(A_{\text{odd}}^2) \geq 19$. The additional pure-$x$ square positions $2, 128, 256$ are nonzero, giving $\mathrm{wt}(A^2) \geq 22$.

If the direction has a nonzero component outside the four variables of A, the terms of A^2 already lie on distinct parallel lines. Otherwise the direction lies in those four variables, so the six (u, v)-slices remain separate.

In the x-direction, AL and AM each occupy nine lines, indexed by the nine odd parts

$$1, 3, 5, 7, 9, 15, 21, 25, 27.$$

Each such row survives multiplication by the nonzero polynomial L or M. The other four slices each occupy at least one line, so there are at least $9 + 9 + 4 = 22$ lines in total.

In a direction not parallel to x, the support of A^2 has affine dimension four and contains four pure-x points, so occupies at least six lines. Both AL and AM have affine dimension four and occupy at least four lines each. Finally, L^2, M^2 each have three pure-x terms, and LM has at least two. These give distinct lines in the chosen direction. The total is at least

$$6 + 4 + 4 + 3 + 2 + 3 = 22.$$

Lemma B.3 now gives $\mathrm{wt}(C^2 B) \geq 44$. □

Lemma B.5 (Two missing products)**.** *For $n = 27, 28$, every positive rational translate of the core support A covers at most $c - 2$ unique-product positions:*

$$|U \cap tA| \leq c - 2 \qquad (t > 0).$$

Proof. Write $t = a/b$ in lowest terms. If $b \geq 2$, an integer output requires an input divisible by b, so there are at most $\lfloor n/2 \rfloor \leq c-2$ such outputs. Assume henceforth that t is an integer.

If $t > n$, the inputs $n, n-1 \in A$ both give outputs outside A^2. Indeed, $tn > n^2$. For $t \geq n+2$ also $t(n-1) > n^2$; for $t = n+1$ this output is $n^2 - 1$, strictly between the largest two possible products $n(n-1)$ and n^2.

If $1 \leq t \leq n$ but $t \notin A$, it is a removed prime larger than $n/2$ and divides no product in A^2. For $t \in A$ it remains to exhibit two inputs giving nonunique products. At $t = 1$ use $4, 6$; at $t = 2$ use $2, 3$. Both 4 and 6 have two factorizations. For $3 \leq t \leq n/2$, use the inputs $2, 4$ and the distinct pairs

$$2t = 1 \cdot (2t) = 2 \cdot t, \qquad 4t = 2 \cdot (2t) = 4 \cdot t.$$

Finally, if $n/2 < t \leq n$ and $t \in A$, then t is composite. Write $t = ps$ with p its smallest prime factor. Here $p \leq 5$, $s \geq 4$, and $p, s, 2p \in A$. The inputs $1, 2$ give the distinct pairs

$$t = 1 \cdot t = p \cdot s, \qquad 2t = 2 \cdot t = (2p) \cdot s.$$

In every case at least two inputs fail to give unique products. □

For a monomial B and any polynomial E, the two-missing-products lemma gives

$$\operatorname{wt}(C^2B - CE) \geq g - (c-2)\operatorname{wt}(E) \qquad (n = 27, 28). \tag{B.4}$$

Indeed each monomial translate of C can cover at most $c-2$ of the g uniquely represented square positions. A translate involving an incompatible extra variable covers none.

Lemma B.6 (All affine cofactors)**.** *For $25 \leq n \leq 66$ and $\operatorname{char} K \neq 2$, every nonzero multiple $(C+Z)(D+ZB)$ with D, B in the base polynomial ring has weight at least n.*

Proof. The exact weight is

$$m = \operatorname{wt}(CD) + r\operatorname{wt}(D + CB) + R\operatorname{wt}(B). \tag{B.5}$$

The cases $B = 0$ and $D = 0$ follow from the base-variable bound; for the latter use $r \geq 1$ and $R \geq r$. Otherwise a strict counterexample would give

$$t = \operatorname{wt}(B) \leq \left\lfloor \frac{n-1-d_0}{R} \right\rfloor \leq 2, \qquad \operatorname{wt}(D+CB) \leq K_t := \left\lfloor \frac{n-1-d_0-Rt}{r} \right\rfloor.$$

Writing $E = D + CB$, and using $CD = CE - C^2B$, gives

$$m \geq \operatorname{wt}(C^2B) - (n-2r)K_t + Rt. \tag{B.6}$$

For the case $t = 1$, it is enough to show

$$g \geq T_n := n + (n-2r)K_1 - R.$$

Let A_k be $[k]$ with the primes in $(k/2, k]$ removed, and put

$$f_k(m) = \#\{d \mid m : d \leq \sqrt{m},\ d \in A_k,\ m/d \in A_k\}.$$

The sets A_k increase with k: composites stay included, and a prime already at most $k/2$ stays included. For $a \leq n \leq b$, a product represented in A_a^2 and uniquely represented in A_b^2 remains uniquely represented in A_n^2. Consequently

$$g \geq \ell(a,b) := \sum_{m=1}^{a^2} \mathbf{1}_{\{f_a(m)>0,\ f_b(m)=1\}}.$$

In the following table all minima and maxima are over $a \le n \le b$. The prime counts, (B.2), and the displayed divisor formula determine its entries by integer divisions.

$[a,b]$	$\min(d_0+7r-n)$	$\min(rd_0-n)$	$\max\left\lfloor\frac{n-1-d_0}{R}\right\rfloor$	$\max T_n$	$\ell(a,b)$
$[25,26]$	6	7	2	60	61
$[27,27]$	5	6	2	84	85
$[28,28]$	5	8	2	88	88
$[29,33]$	10	18	1	42	64
$[34,37]$	8	26	1	82	104
$[38,50]$	7	34	2	94	94
$[51,66]$	8	63	1	129	134

(B.7)

The final two columns prove $g \ge T_n$. For a singleton interval, $\ell(n,n) = g$; thus $g = 85, 88$ at $n = 27, 28$.

Only $n = 26, 27, 28, 40$ permit $t = 2$. Apply Lemma B.4 to (B.6):

n	square–binomial bound	K_2	R	output bound
26	16	0	6	28
27	44	1	6	35
28	44	1	6	34
40	20	0	10	40

Every final entry is at least n. □

In characteristic three the lemma remains valid when D and B also use the fresh cubes z_i^3. Decompose them by those fresh-cube exponent vectors. Output aggregate degrees zero, one, and two occupy disjoint fresh residue classes, so the nonzero slices are ordinary affine multiples and their weights add.

B.3 Residue reduction and the higher-degree exceptions

In characteristic three, an exponent class has integer representatives ab^3 with a fixed cube-free part a. Hence $\sigma_3(C) \le \lfloor n^{1/3} \rfloor \le r$ for $25 \le n \le 66$. Similarly $\sigma_3(C^2) \le \lfloor n^{2/3} \rfloor \le R$ except possibly at $n = 26, 27, 28, 38, 39, 40$, as follows by comparing n^2 with $(R+1)^3$.

At $n = 26$, a nonzero cube-residue class has $a \ge 2$ and at most $\lfloor (26^2/2)^{1/3} \rfloor = 6$ terms. The zero class consists of cubes b^3 with $b \le 8$; neither 7^3 nor 8^3 is a product of two integers at most 26, so it also has at most six terms. At $38 \le n \le 40$, nonzero classes have at most $\lfloor (40^2/2)^{1/3} \rfloor = 9$ terms. The zero class has $b \le 11$ and excludes $7^3, 11^3$, again giving at most nine, hence at most $R = 10$. The cubes $7^3, 8^3, 11^3$ have most balanced factor pairs $(7, 49), (16, 32), (11, 121)$, respectively. Thus $\sigma_3(C^2) \le R$ except at $27, 28$. Corollary 3.2 reduces every other characteristic-three case to an affine cofactor, already handled by Lemma B.6.

For characteristic $p \ge 5$, put $w_j = \binom{r+j-1}{j}$ and let J be the least positive index with $w_J \ge n$. The prime counts give $r = 3$ only at $n = 26, 27, 28$, and $r \ge 4$ otherwise. For the two bounds $(r, n) = (3, 28)$ and $(4, 66)$, the values of $w_1, \dots, w_6$ are

$$(3, 6, 10, 15, 21, 28), \qquad (4, 10, 20, 35, 56, 84).$$

Direct integer comparisons therefore give $J \le 6$ and, for every $1 \le j < J$,

$$n^j \le w_j^{p_0}, \qquad p_0 = \begin{cases} 5, & j \le 4, \\ 7, & j = 5. \end{cases} \tag{B.8}$$

For $j < p$, a fixed exponent class modulo p in the support of C^j contains at most $\lfloor n^{j/p} \rfloor$ points: its integer representatives have the form $ab^p \le n^j$. Thus (B.8) gives $\sigma_p(C^j) \le w_j$ for $j < J$, while

$J \le j < p$ gives $\sigma_p(C^j) < n \le w_j$. The residue theorem applies for every $p \ge 5$. In characteristic zero use scalar compression directly, with the same increasing aggregate costs w_j.

The coefficient of the least aggregate row of any P-multiple is a nonzero C-multiple: evaluate at $Z = -C$, divide by its least power of $-C$, and reduce modulo C. By $rd_0 > n$, a short output has a nonzero constant row, costing at least d_0. The inequality $d_0 + w_j < n$ leaves only $(n, j) = (26, 3), (27, 3), (27, 4), (28, 3), (28, 4), (40, 3)$. After the constant and top rows, the respective remaining budgets are $4, 5, 0, 5, 0, 0$, giving the following possibilities:

n	Top degree	Remaining possible rows
$26, 27, 28$	3	Top row monomial, degree-two row absent, degree-one row has at most one term.
$27, 28$	4	Top row monomial, all intermediate rows absent.
40	3	Top row monomial, all intermediate rows absent.

These cases occur only in characteristic zero or $p \ge 5$.

At $n = 26, 27, 28$, set all base variables except those of primes $5, 7, 11, 13$ equal to zero. The remaining core is $Q = A(x) + y_1 + y_2 + y_3$, after rescaling, where $A = a + bx + cx^2$ and $abc \ne 0$. In these characteristics A^2 has nonzero coefficients in degrees $0, 1, 3, 4$, while A^3 has nonzero coefficients in degrees $0, 1, 5, 6$. Therefore

$$\mathrm{wt}(C^3) \ge \mathrm{wt}(Q^3) \ge 4 + 3 \cdot 4 + 6 \cdot 3 + 10 = 44. \tag{B.9}$$

For a cubic output the constant row is a translate of C^3 possibly modified by one translate of C. Including the possible linear row and the top fresh row gives the lower bounds $44 - c + 3 + 10 = 34, 33, 32$, respectively. If the linear row is absent the bound is stronger. In the quartic cases the degree-four part in y_1, y_2, y_3 alone has fifteen terms; the top fresh row costs another fifteen, giving $30 > n$. At $n = 40$, retaining primes $7, 11, 13, 17, 19$ gives a weighted six-term affine simplex. Its cube has $\binom{8}{3} = 56$ terms, and the top fresh row adds twenty. These cases are also impossible.

B.4 The two exceptional cube-residue cases

It remains to handle $n = 27, 28$ in characteristic three. Here $r = 3$, $R = 6$, $d_0 = 11, 12$, and $\sigma_3(C^2) \le 7$. Indeed, nonzero classes have at most $\lfloor (28^2/2)^{1/3} \rfloor = 7$ terms; the zero class has $b \le 9$ and excludes $7^3, 8^3$. We handle these two cases directly.

Choose a short multiple of least total base cofactor width and compress. Theorem 3.1 gives

$$G = A_0 + ZA_1 + Z^2A_2, \qquad A_j \in K[x, Z^3].$$

With expanded weights $u_j = \mathrm{wt}(A_j)$, put

$$F = 3u_1 + 6u_2, \qquad M = 3u_1 + 7u_2 = F + u_2.$$

Then $m = \mathrm{wt}(G) = u_0 + F < n$ and $u_0 \ge d_0$. Hence $u_2 \le 2$; if $u_2 = 1$ then $u_1 \le 3$, and if $u_2 = 2$ then $u_1 \le 1$. The comparison and correction are

$$\begin{aligned} V &= P(A_1 - CA_2 + ZA_2) = CA_1 - C^2A_2 + ZA_1 + Z^2A_2, \\ U &= G - V = A_0 - CA_1 + C^2A_2 = P^3E. \end{aligned}$$

Every nonzero correction class of U has at least n terms by the width descent. Its intersection with the comparison part is at most M. There can be at most one such class, since

$$2(n - M) - (m - F) \ge n + 1 - F - 2u_2 \ge d_0 + 2 - 2u_2 > 0.$$

If $u_2 = 0$, then $M = F$ and all classes are protected, so $U = 0$. If $U = 0$ in any case, Lemma B.6, applied to fresh-cube slices, is already a contradiction. Otherwise $u_2 = 1$ or 2 and exactly one correction class is nonzero.

The comparison V has at least n terms. It also has at least $2M$. If $u_2 = 1$, use (B.4):

$$\mathrm{wt}(V) \geq g - (c-5)u_1 + 6 \geq 34, \qquad 2M \leq 2(3 \cdot 3 + 7) = 32.$$

The two endpoint calculations are $85 - 19 \cdot 3 + 6 = 34$ and $88 - 20 \cdot 3 + 6 = 34$. If $u_2 = 2$, Lemma B.4 gives $\mathrm{wt}(C^2 A_2) \geq 44$. If the two monomials have different fresh-cube exponents, their contributions are disjoint and the bound is stronger. Since $u_1 \leq 1$,

$$\mathrm{wt}(V) \geq 44 - (c-3)u_1 + 12 \geq 34, \qquad 2M \leq 2(3 + 14) = 34.$$

Thus one correction class changes support by at least $n - 2M$, giving $m \geq \mathrm{wt}(V) + n - 2M \geq n$. We have proved

Proposition B.7. *Theorem B.1 holds in characteristic zero and every odd characteristic.*

B.5 Characteristic two: stronger smooth-core bounds

For the rest of this section, $\operatorname{char} K = 2$. A stronger smooth-core bound will sharpen d_0. If $Q(t) = q_0 + \cdots + q_e t^e$ has $e > 0$ and $q_0 q_e \neq 0$, endpoints give $d(Q) \geq d(q_0) + d(q_e)$. If Q cannot divide a two-row polynomial over the fraction field of its coefficient ring, then every multiple has a third occupied row and

$$d(Q) \geq d(q_0) + d(q_e) + 1. \tag{B.10}$$

A useful obstruction to a two-row multiple is

$$\frac{q_{e-1}^2}{q_e q_{e-2}} \text{ is nonconstant,} \tag{B.11}$$

when the three coefficients are nonzero. Indeed, in a splitting field the roots of a binomial are ρ times roots of unity, with their multiplicities. A divisor therefore has $q_{e-j}/q_e = \rho^j a_j$, where each a_j is algebraic over K. The displayed ratio would be algebraic over K. A rational function algebraic over K is constant: choose any variable on which it depends and apply the one-variable argument in Lemma A.2. Thus a nonconstant ratio excludes a two-row multiple.

Let

$$T_{d,e}(x, y) = A_d(x) + yB_e(x) + cy^2, \qquad (d, e) \in \{(3,1), (3,2), (4,2)\},$$

where A_d, B_e are dense polynomials of the indicated degrees and all displayed coefficients are nonzero. Each $T_{d,e}$ has distance at least four. Its bottom row costs two, its top row one, and the ratio $B_e^2/(cA_d)$ is nonconstant. For the first two pairs the degrees $2e, d$ differ; for $(4,2)$ the numerator has no odd exponent while the denominator does. Equation (B.10) supplies the fourth term.

Let B_n denote the part of C supported on integers with all prime factors at most $\sqrt{n}$. We claim

$$d(B_n) \geq b(n), \qquad b(n) = \begin{cases} 7, & n = 25, 26, \\ 6, & 27 \leq n \leq 48, \\ 8, & 49 \leq n \leq 66. \end{cases} \tag{B.12}$$

As before, each support below carries arbitrary nonzero coefficients.

For $n = 25, 26$, slice in $y = x_3$, with $x = x_2$ and $z = x_5$. The bottom row is $T_{4,2}(x, z)$, of distance at least four; the top row is a dense binomial in x, of distance two. The middle row has support $1 + x + x^2 + x^3 + z$. Its square has no odd z-exponent, whereas the product of the bottom and top rows has a nonzero z-linear coefficient. The quadratic ratio is nonconstant. Thus $d(B_n) \geq 4 + 2 + 1 = 7$.

For $27 \leq n \leq 66$, slice in x_2 and put $y = x_3, z = x_5, w = x_7$. The last three row supports, in increasing degree, are

n	Last three x_2-row supports
27–31, 48–55	$(1+y+z,\ 1+y,\ 1)$
32–39, 64–66	$(1+y,\ 1,\ 1)$
40–47	$(1+y+z,\ 1,\ 1)$
56–63	$(1+y+z+w,\ 1+y,\ 1)$

In each row of the table, the square of the middle coefficient has only even exponents, while the product of the other two coefficients has an odd exponent. Thus (B.11) forces a third occupied row.

For $27 \le n \le 48$, the bottom coefficient is $T_{3,1}(y,z)$ through $n = 44$ and $T_{3,2}(y,z)$ thereafter, of distance at least four. The top coefficient is monomial, so $d(B_n) \ge 4+1+1 = 6$.

For $49 \le n \le 66$, the bottom row is

$$T = T_{3,2}(y,z) + wH(y,z) + cw^2,$$

where H has support $1+y+z$ through $n = 62$ and $1+y+y^2+z$ thereafter. Since H^2 has only even exponents and $T_{3,2}$ has nonzero odd exponents, the quadratic invariant is nonconstant. Therefore $d(T) \ge 4+1+1 = 6$. The top x_2-row is monomial. The same odd-exponent obstruction in the preceding table gives a third row, hence $d(B_n) \ge 6+1+1 = 8$. This proves (B.12). Adding the prime rows above $\sqrt{n}$ by endpoints, exactly as for d_0, now gives

$$d(C) \ge \kappa(n) := b(n) + \sum_{\substack{\sqrt{n} < q \le n/2 \\ q \text{ prime}}} \left\lfloor \frac{n}{q} \right\rfloor. \tag{B.13}$$

B.6 Comparison bounds from four rough counts

For a normalized u-term multiplier with largest support prime q, summing the bounds of Lemma C.1 gives:

$$\begin{aligned}
H_{2,u}(n) &= uC_2(n) + (2-u)C_2(n/2),\\
H_{3,u}(n) &= uC_3(n) + (4-u)C_3(n/2) - C_3(n/3),\\
H_{5,u}(n) &= uC_5(n) + (4-u)C_5(n/2) + 2C_5(n/3) - 2C_5(n/5),\\
H_{7,u}(n) &= uC_7(n) + (4-u)C_7(n/2) + 2C_7(n/3) + 2C_7(n/5) - 3C_7(n/7).
\end{aligned}$$

These expressions follow from (C.2). At $q = 5$, for example, the successive costs are $u, 4, 6, 4$ on indices 1, 2, 3–4, and 5 onwards.

For $27 \le n \le 48$, the component with rough part one at $q = 5$ is exactly the smooth core B_n. Its distance is at least six, whereas $H_{5,u}$ charged four. We may therefore add two to $H_{5,u}$ throughout this range. Denote the improved expression by $H^+_{5,u}$, and use $H^+_{5,u} = H_{5,u}$ outside this range.

For $u \in \{3,4,5\}$, if a u-term multiplier uses a prime at least q_0, the least prime at least $2u-1$, the directed cut gives

$$\mathrm{wt}(PD) \ge 2n - 2(u-1)\lfloor n/q_0 \rfloor. \tag{B.14}$$

Indeed each proper piece has at most $u-1 \le 4$ terms and satisfies Lemma B.2. Otherwise its largest support prime is one of $2, 3, 5, 7$, and the corresponding bound above applies.

The resulting bounds are listed below. Each entry holds throughout its row, and the last column is the minimum of the preceding entries.

n	u	Cut	$H_{2,u}$	$H_{3,u}$	$H^+_{5,u}$	$H_{7,u}$	Bound
25	3	30	33	28	—	—	28
27,28	4	32	42	33	32	—	32
34,35	4	40	50	40	40	—	40
36	4	42	54	44	40	—	40
38	4	46	56	48	44	—	44
39,40	4	48	60	47	46	—	46
49–51	4	56	74	62	60	—	56
58	5	76	100	78	73	69	69

The entries follow from

$$C_2(t) = \lfloor t \rfloor - \lfloor t/2 \rfloor, \qquad C_3(t) = \lfloor t \rfloor - \lfloor t/2 \rfloor - \lfloor t/3 \rfloor + \lfloor t/6 \rfloor,$$

the residue formula (C.5), and

$$C_7(t) = C_5(t) - C_5(t/7).$$

For example, at $n = 36$ the improved $q = 5$ bound is $4C_5(36) + 2C_5(12) - 2C_5(36/5) + 2 = 36 + 6 - 4 + 2 = 40$.

B.7 The only remaining four-term pattern

Lemma B.8 (Parity pairing)**.** *In characteristic two, suppose a four-term Laurent multiplier has three terms in one full exponent-parity class and its fourth term in a different class. Its weighted interval product has at least* $36, 36, 44$ *terms at* $n = 27, 28, 36$*, respectively.*

Proof. For a weighted interval kernel Q_k of length k and a three-term multiplier F, the initial theorem gives

$$\mathrm{wt}(Q_k F) \geq a(k), \qquad (a(0), a(1), \ldots, a(6)) = (0, 3, 2, 3, 4, 6, 6).$$

Only $a(5) = 6$ needs explanation. The strict case of sharp completion applied to the dense quadratic core of Q_5 says that a five-term multiple is a scalar monomial times Q_5^q, with q a power of two. Its cofactor is monomial if $q = 1$; if $q \geq 2$, its cofactor is a nonzero Q_5-multiple and has at least five terms. It cannot have three terms.

After removing a Laurent monomial, write $D = F^2 + X(v)M^2$ over a coefficient field in which the needed square roots exist. Here F has three terms, M is monomial, and $v > 1$ is squarefree. For squarefree integers set $s \oplus v = sv/\gcd(s, v)^2$. The kernel splits into its parity classes:

$$P = \sum_{s \text{ squarefree}} X(s) Q_s^2, \qquad k_s := \mathrm{wt}(Q_s) = \lfloor \sqrt{n/s} \rfloor,$$

where Q_s is a weighted interval of length k_s, and $k_s = 0$ when $s > n$. In parity class s, a square root of the output is $Q_s F$ plus a monomial translate of $Q_{s \oplus v} M$. For a pair with sizes $k, l > 0$ the two classes consequently contribute at least

$$\max\{a(k) - l, 0\} + \max\{a(l) - k, 0\}.$$

If just one class is occupied, the contribution is $a(k) + k \geq 4$.

If $v \neq 2$, choose an odd prime divisor p of v. Every occupied pair has exactly one member divisible by p. The squarefree counts through $27, 28, 36$ are $17, 17, 23$, respectively. At most $4, 4, 6$ of those squarefree integers can be divisible by a fixed odd prime: for $p = 3$ the lists are $3, 6, 15, 21$ and, at 36, also $30, 33$; for $p = 5$ the respective counts are $3, 3, 5$; for $p \geq 7$ use $\lfloor n/7 \rfloor$. Hence there are at least $9, 9, 11$ unpaired occupied classes, giving $36, 36, 44$ output terms.

For $v = 2$, pair each odd squarefree s with $2s$:

n	Pair-size multiset	Lower bound
27	$(3,5), (2,3), (1,2), 3(1,1), 5(0,1)$	38
28	$(3,5), (2,3), 2(1,2), 2(1,1), 5(0,1)$	36
36	$(4,6), (2,3), 2(1,2), 4(1,1), 7(0,1)$	51

Here $j(k,l)$ means j copies; each bound is sufficient. □

B.8 Two largest parity classes suffice

Suppose a short multiple exists. Choose one with least total base cofactor width and apply residue descent:

$$G = A_0 + ZD, \qquad U = A_0 + CD = P^2E, \qquad V = PD, \qquad m = \mathrm{wt}(G) = \mathrm{wt}(A_0) + ru < n.$$

Here $u = \mathrm{wt}(D) \geq 1$, and every nonzero parity class of U has at least n terms.

In $25 \leq n \leq 36$ one has $r \geq 3, \kappa \geq 12$; in $37 \leq n \leq 66$ one has $r \geq 4, \kappa \geq 18$. Thus $r\kappa \geq n$. The residue theorem gives

$$u \leq \left\lfloor \frac{n-1-\kappa}{r} \right\rfloor. \tag{B.15}$$

Using (B.13) gives the following table. Its last column lists those n for which both $\kappa + 4r < n$ and $2(3\lfloor\sqrt{n}\rfloor + \lfloor\sqrt{n/2}\rfloor) > n$ hold.

Range	$\min(\kappa + 5r - n)$	Possible four-term exceptions
25–26	3	none
27–33	1	27,28
34–40	1	34,35,36,38,39,40
41–48	4	none
49–57	1	49,50,51
58	−1	none
59–66	0	none

Consequently $u \leq 4$ except possibly at $n = 58$, where $(r, \kappa) = (6, 27)$ gives $u \leq 5$. Lemma B.2 therefore supplies $\mathrm{wt}(V) \geq n$ in every case.

Put

$$s = \lfloor\sqrt{n}\rfloor, \qquad t = \lfloor\sqrt{n/2}\rfloor.$$

These are exactly the two largest parity-class sizes of C: a squarefree class a contains the integers $ab^2 \leq n$, hence has $\lfloor\sqrt{n/a}\rfloor$ elements; removing fresh primes affects only singleton classes. If the parity distribution of D is $\lambda_1 \geq \lambda_2 \geq \cdots$, the comparison CD has at most $M = \sum_i \lambda_i s_i$ terms in any one class, where s_i are the decreasing class sizes of C. In particular,

$$M \leq us; \qquad M \leq (u-1)s + t \quad \text{if } D \text{ meets at least two classes.} \tag{B.16}$$

For $u = 4$ meeting at least two classes, unless the distribution is $(3, 1)$, the stronger bound $M \leq 2s + 2t$ holds. These follow simply by putting as many terms as allowed against the largest class and all remaining terms against the second largest.

If a correction classes are nonzero, residue descent gives

$$m \geq \mathrm{wt}(V) + a(n - 2M), \qquad a(n - M) \leq m - ru. \tag{B.17}$$

Thus $2M \leq n$ immediately excludes a counterexample. If $2M \leq n + ru$, the second inequality forces $a \leq 1$; in that case the first excludes a counterexample whenever $\mathrm{wt}(V) \geq 2M$.

Single-class inputs with $u \geq 3$ can be excluded directly. Let Q_1 count squarefree integers in $(n/4, n]$. Their parity classes in P are singletons, so each contributes exactly u terms to V. Fresh-prime classes cannot meet U. Every other such class is protected: a correction would leave at least $n - u > m - ru$ terms in A_0. Hence $m \geq uQ_1$. For $n \leq 66$, inclusion–exclusion for the squares $4, 9, 25, 49$ gives the exact formula

$$Q_1 = n - 2\lfloor n/4\rfloor - \lfloor n/9\rfloor - \lfloor n/25\rfloor - \lfloor n/49\rfloor + \lfloor n/16\rfloor + 2\lfloor n/36\rfloor.$$

Since $1/25 + 1/49 < 1/16$, this is greater than $4n/9 - 3$. Thus $3Q_1 \geq n$ for $27 \leq n \leq 66$; at $n = 25, 26$, one has $Q_1 = 11, 12$, respectively. Single-class inputs with $u \geq 3$ are impossible.

For $u \le 2$, the first bound in (B.16) gives $2M \le 4s \le n$. For $u = 3$ meeting two classes, $2M \le 4s + 2t \le n$ for every $n \ge 26$ in the range. Indeed the real-variable inequality holds for $n \ge 30$, and $26 \le n \le 29$ has $(s,t) = (5,3)$. At $n = 25$, $M \le 13$ and the comparison bound $28 \ge 2M$ applies, while $2M \le n + 3r$.

For $u = 4$, the preceding count table leaves only its stated four-term exceptions. All have $2(3s + t) \le n + 4r$, so there is at most one correction class. Their capacities and comparison bounds reduce to

n	$3s + t$	$2s + 2t$	General bound	$(3,1)$ bound
27,28	18	16	32	36
34,35	19	18	40	40
36	22	20	40	44
38	22	20	44	44
39,40	22	20	46	46
49–51	≤ 26	≤ 24	56	56

The only improvements in the last column are the three cases of Lemma B.8. Each bound is at least twice the corresponding capacity, completing the four-term case.

Finally, if $u = 5$, then $n = 58$. A mixed parity distribution has $M \le 4 \cdot 7 + 5 = 33$, and $2M \le 58 + 5 \cdot 6$. The comparison bound $\mathrm{wt}(V) \ge 69 > 66 \ge 2M$ excludes this last possibility.

Proof of Theorem B.1. The preceding argument proves characteristic two. Proposition B.7 proves characteristic zero and odd characteristic. The monomial multiplier attains the stated bound in every case. □

C Arithmetic estimates

Throughout, the interval coefficients are nonzero elements of a field. Write $r(n) = \pi(n) - \pi(n/2)$. For a finite set T of primes, let $C_T(x)$ count the positive integers through x divisible by no prime in T, and put $J_T(x) = C_T(x) - C_T(x/2)$. Write C_q, J_q when T consists of all primes at most q. An integer is *q-smooth* if all its prime factors are at most q, and *q-rough* if none are.

C.1 Disjoint components

Let D be normalized, with u terms and largest support prime q. Multiplication by D preserves the q-rough factor. Hence

$$\mathrm{wt}(P_{n,c}D) = \sum_{\substack{b \le n \\ b \text{ is } q\text{-rough}}} \mathrm{wt}(S^{(b)}_{q,\lfloor n/b \rfloor}D), \tag{C.1}$$

where $S^{(b)}_{q,j}$ has the q-smooth integers through j as support and inherits the coefficients c_{ba}. These coefficients may vary with b.

Component costs can be summed by thresholds. For any cost function f on $\{1, \dots, n\}$,

$$\sum_{\substack{b \le n \\ b \text{ is } q\text{-rough}}} f(\lfloor n/b \rfloor) = f(1)C_q(n) + \sum_{j=2}^{n} (f(j) - f(j-1))C_q(n/j). \tag{C.2}$$

Indeed, $f(k) = f(1) + \sum_{j=2}^{k}(f(j) - f(j-1))$, and a rough part has component index at least j exactly when $b \le n/j$. This identity explains the coefficients in the counting bounds below.

Lemma C.1 (Component bounds)**.** *The component of index $j = 1$ has weight u, and for $j \ge 2$,*

$$\mathrm{wt}(S^{(b)}_{q,j}D) \ge \begin{cases} 2(1 + \pi(j)), & 2 \le j < q, \\ 1 + \pi(q), & j \ge q. \end{cases}$$

Consequently, for $q \geq 5$ and $u \geq 4$,

$$\mathrm{wt}(P_{n,c}D) \geq 4C_q(n) + (u-4)J_q(n), \tag{C.3}$$

and for $q \geq 17$,

$$\mathrm{wt}(P_{n,c}D) \geq uJ_q(n) + 4C_q(n/2) + 2C_q(n/3) + 2C_q(n/5). \tag{C.4}$$

Proof. At index one the kernel is a scalar. If $2 \leq j < q$, it is independent of x_q, so at least two nonzero x_q-slices of D remain separate. Each costs at least $1 + \pi(j)$ terms by the dimension bound. If $j \geq q$, the kernel contains the constant and a pure power of every prime through q, giving $1 + \pi(q)$ terms. Applying (C.2) to the lower profiles $u, 4, 4, \ldots$ and $u, 4, 6, 6, 8, 8, \ldots$ gives the two inequalities. □

Theorem C.2 (Localized multipliers)**.** *Let $n \geq 67$, and let D be a normalized nonconstant multiplier with u terms and largest support prime q. If*

$$q \leq n/2, \qquad q < 2(u-1),$$

then $\mathrm{wt}(P_{n,c}D) \geq n$ over every field.

The proof is completed in Section C.7.

C.2 Sieve estimates

The eight residues $\mathcal{R} = \{1, 7, 11, 13, 17, 19, 23, 29\}$ give the exact formula

$$C_5(x) = \sum_{a \in \mathcal{R}} \left\lfloor \frac{x + 30 - a}{30} \right\rfloor. \tag{C.5}$$

Equivalently, if $\lfloor x \rfloor = 30h + t$ with $0 \leq t < 30$, then $C_5(x) = 8h + \#\{a \in \mathcal{R} : a \leq t\}$.

Lemma C.3 (Sieve discrepancies)**.** *Put $\rho(q) = \prod_{p \leq q}(1 - 1/p)$. For every $x \geq 0$,*

$$|C_q(x) - \rho(q)x| \leq \Delta_q, \qquad |J_q(x) - \rho(q)x/2| \leq 2\Delta_q,$$

where

$$\Delta_2 = \tfrac{1}{2}, \qquad \Delta_3 = \tfrac{2}{3}, \qquad \Delta_q = \tfrac{14}{15}2^{\pi(q)-3} \quad (q \geq 5).$$

For $q = 5$ the sharper half-interval bound is

$$|J_5(x) - 2x/15| \leq 22/15.$$

Proof. The cases $q = 2, 3$ follow from the residues modulo two and six. At the eight jumps of C_5 in one period, the values of $15C_5(x) - 4x$ are

$$11, 2, 1, 8, 7, 14, 13, 4.$$

Between jumps the error $C_5(x) - 4x/15$ decreases linearly; its left limit at a jump is one less than its value. Thus its absolute value is at most $14/15$. For a prime $p \notin T$,

$$C_{T \cup \{p\}}(x) = C_T(x) - C_T(x/p),$$

which multiplies the density by $1 - 1/p$ and at most doubles the error. This proves the bound for C_q; subtraction at x and $x/2$ gives the bound for J_q.

The error $J_5(x) - 2x/15$ has period sixty. Between jumps it has slope $-2/15$, and at its upward jumps its numerator is

t	1	7	11	13	17	19	23	29
$15J_5(t) - 2t$	13	1	8	19	11	22	14	2
t	31	37	41	43	47	49	53	59
$15J_5(t) - 2t$	13	1	−7	4	−4	7	14	2

Thus the error is at most $22/15$. For nonintegral $0 < x < 60$, reflection of the residues gives $J_5(60 - x) = 8 - J_5(x)$; hence the error changes sign. One-sided limits give the lower bound at jumps as well. □

Lemma C.4 (A one-step sieve)**.** *Let T and P be disjoint finite sets of primes, and suppose $|C_T(x) - \rho x| \le \Delta$ for all $x \ge 0$. Put*

$$\alpha = \rho\left(1 - \sum_{p\in P}\frac{1}{p}\right), \qquad E = (1 + |P|)\Delta.$$

Then

$$C_{T\cup P}(x) \ge \alpha x - E, \qquad J_{T\cup P}(x) \ge \alpha x/2 - 2E.$$

If the sharper estimate $|J_T(x) - \rho x/2| \le \Lambda$ is known, the second error can be replaced by $(1+|P|)\Lambda$.

Proof. Removing multiples of the added primes gives

$$C_{T\cup P}(x) \ge C_T(x) - \sum_{p\in P} C_T(x/p).$$

Multiplication by $p \notin T$ preserves the T-rough property. Applying the same bound on $(x/2, x]$ gives

$$J_{T\cup P}(x) \ge J_T(x) - \sum_{p\in P} J_T(x/p).$$

Insert the assumed discrepancies, using $\Lambda = 2\Delta$ if no sharper bound is available. □

For $u \ge 4$ and $q \ge 5$, combining this lemma with (C.3) gives

$$\mathrm{wt}(P_{n,c}D) \ge \frac{u+4}{2}\alpha n - 2(u-2)E, \tag{C.6}$$

where P consists of the primes at most q outside the chosen sieve T.

For $T = \{2, 3, 5\}$ the constants are

$$\alpha_q = \frac{4}{15}\left(1 - \sum_{7\le p\le q}\frac{1}{p}\right), \qquad E_q = \frac{14}{15}(\pi(q) - 2). \tag{C.7}$$

For $T = \{2, 3, 5, 7\}$, use $\rho = 8/35$ and $\Delta = 28/15$.

C.3 Finite prime counts

Lemma C.5 (Prime counting below a rough cube)**.** *Put*

$$C_{11}(x) = C_5(x) - C_5(x/7) - C_5(x/11) + C_5(x/77),$$
$$(p_1, \dots, p_8) = (13, 17, 19, 23, 29, 31, 37, 41).$$

For $11 \le x \le 1799$,

$$\pi(x) = 4 + C_{11}(x) - \sum_{i=1}^{8}\max\{C_{11}(x/p_i) - i, 0\}. \tag{C.8}$$

Proof. Inclusion–exclusion gives the formula for C_{11}. Since $1799 < 13^3$, an eleven-rough integer in this range is one, a prime, or a product pq of two primes with $13 \le p \le q$. The smaller prime is one of the listed p_i, since $\sqrt{1799} < 43$. Also $1799/13 < 13^2$, so $C_{11}(x/p_i)$ counts only one and primes. Exactly i eleven-rough integers lie below p_i. Thus the summand counts the composites with smaller prime p_i, including squares. Subtract these and one, then add the five primes through eleven. □

Lemma C.6 (A prime budget)**.** *Let D be a normalized multiplier at n, of weight $u \geq U \geq 4$, where U is an integer, and largest support prime $17 \leq q \leq n/2$. Suppose $q < 2(u-1)$ and $r = \pi(n) - \pi(n/2) \geq 8$. Then*

$$\mathrm{wt}(P_{n,c}D) \geq Ur + 4\pi(n/2) + 2\pi(n/3) + 2\pi(n/5) + 8 - 8\pi(2U-3).$$

At $U = 10$ this becomes

$$\mathrm{wt}(P_{n,c}D) \geq 10r + 4\pi(n/2) + 2\pi(n/3) + 2\pi(n/5) - 48. \tag{C.9}$$

Proof. Every prime in $(n/2, n]$ is q-rough, so $J_q(n) \geq r$. Also $C_q(t) \geq 1 + \pi(t) - \pi(q)$ for all $t \geq 0$: when the right side is positive it counts 1 and primes larger than q; otherwise the assertion is immediate. The component budget (C.4) therefore gives

$$\mathrm{wt}(P_{n,c}D) \geq ur + 4\pi(n/2) + 2\pi(n/3) + 2\pi(n/5) - 8\pi(q) + 8.$$

The hypothesis gives $q \leq 2u - 3$. Each unit increase of the integer parameter in $2u - 3$ adds at most one new odd prime. Thus

$$\pi(q) \leq \pi(2U-3) + (u-U).$$

Substitution leaves the nonnegative term $(u-U)(r-8)$. For $U = 10$, use $\pi(17) = 7$. □

Lemma C.7 (The counts through 1023)**.** *For $67 \leq n \leq 1023$,*

$$r(n) \geq \lfloor \sqrt{n} \rfloor, \qquad 10r(n) + 4\pi(n/2) + 2\pi(n/3) + 2\pi(n/5) - 48 \geq n.$$

Proof. All counts below follow from (C.8). First suppose $67 \leq n \leq 100$. At $n = 67$ the primes in $(n/2, n]$ are $37, 41, 43, 47, 53, 59, 61, 67$. Through $n = 100$, primes enter at $71, 73, 79, 83, 89, 97$ and leave at $74, 82, 86, 94$. Pairing each departure with the preceding arrival gives

$$r(n) \geq 8 + \mathbf{1}_{n \geq 73} + \mathbf{1}_{n \geq 97} \geq \lfloor \sqrt{n} \rfloor.$$

Also $\pi(n/2) \geq 11$, $\pi(n/3) \geq 8$, and $\pi(n/5) \geq 6$, so the second expression is at least $104 \geq n$.

For $101 \leq n \leq 1023$, a row $[a, b]$ gives the lower bounds

$$r_0 = \pi(a) - \pi(b/2), \qquad B_0 = 10r_0 + 4\pi(a/2) + 2\pi(a/3) + 2\pi(a/5) - 48.$$

Monotonicity gives $r(n) \geq r_0$ and a prime budget at least B_0. Each row satisfies $r_0 \geq \lfloor \sqrt{b} \rfloor$ and $B_0 \geq b$:

a	b	r_0	B_0
101	117	10	150
118	141	11	172
142	165	12	200
166	195	13	228
196	225	15	262
226	273	16	302
274	345	19	354
346	421	22	430
422	524	27	524
525	636	33	636
637	765	40	772
766	913	48	916
914	1023	59	1102

For example, the row $[422, 524]$ uses prime counts $82, 55, 47, 34, 23$ at $422, 262, 211, 140, 84$, giving $r_0 = 27$ and $B_0 = 524$. □

For $67 \le n \le 228$, let κ, h be as in Section 4. On each block $[a, b]$ below put

$$r_0 = \pi(a) - \pi(b/2), \quad R_0 = r_0(r_0+1)/2, \quad \kappa_0 = \kappa(a), \quad h_0 = \pi(a/2) - \pi(\sqrt{b}).$$

Then $r \ge r_0$ and $h \ge h_0$. Moreover $\kappa \ge \kappa_0$: between consecutive prime squares the set of primes at most $\sqrt{n}$ is fixed, the existing floor terms increase, and each new prime entering at $n = 2q$ adds two. The only prime squares in this range are $121, 169$, both block starts. The finite sieve formula and integer division give the following table; both final columns are at least b.

a	b	r_0	κ_0	h_0	$\kappa_0 + R_0 + r_0$	$\kappa_0 + R_0 + h_0 + 1$
67	72	8	28	7	72	72
73	81	9	30	7	84	83
82	85	9	37	9	91	92
86	93	9	40	10	94	96
94	101	9	47	11	101	104
102	115	10	50	11	115	117
116	120	13	58	12	162	162
121	133	12	53	12	143	144
134	145	12	62	14	152	155
146	161	12	71	16	161	166
162	168	14	80	17	199	203
169	193	15	72	17	207	210
194	223	15	88	19	223	228
224	228	18	109	23	298	304

This proves (4.4).

Put $d_0 = 1 + \pi(n/2)$ and $R = r(r+1)/2$. For the next table use $r_0 = \pi(a) - \pi(b/2)$, $d_0 = 1 + \pi(a/2)$ and $R_0 = r_0(r_0+1)/2$. The same endpoint bounds give $d_0 + R \ge n$ for $229 \le n \le 1799$:

a	b	r_0	d_0	R_0	$d_0 + R_0$
229	241	20	31	210	241
242	262	21	31	231	262
263	286	22	33	253	286
287	325	24	35	300	335
326	361	25	39	325	364
362	397	27	43	378	421
398	457	29	47	435	482
458	541	31	51	496	547
542	654	34	59	595	654
655	837	39	67	780	847
838	1093	45	82	1035	1117
1094	1480	52	102	1378	1480
1481	1799	80	132	3240	3372

C.4 Fresh primes

Lemma C.8 (Elementary Chebyshev bounds)**.** *Put*

$$A = \frac{14\log 2 + 9\log 3 + 5\log 5}{30} > \frac{23}{25}, \qquad b = \frac{6}{5}A,$$

$$H(x) = \frac{5}{4\log 6}\left(\log x + \frac{1}{2}\log 6 - \frac{6}{5}\right)^2 + 9.$$

For $x \ge 30$,

$$Ax - \frac{5}{2}\log x + 2 < \psi(x) < bx + H(x),$$

where

$$\psi(x) = \sum_{p^a \le x} \log p, \quad \vartheta(x) = \sum_{p \le x} \log p.$$

For $x \ge 256$, moreover,

$$0 \le \psi(x) - \vartheta(x) < \frac{8}{3}\sqrt{x}.$$

Consequently, with $r(n) = \pi(n) - \pi(n/2)$,

$$r(n)\log n > \frac{2A}{5}n - \frac{8}{3}\sqrt{n} - \frac{5}{2}\log n + 2 - H(n/2) \qquad (n \ge 256).$$

Proof. Write $J(t) = \log\lfloor t\rfloor!$ and $h(t) = t\log t - t$. Concavity of the logarithm, applied on the intervals between consecutive integers and on the intervals centred at consecutive integers, gives

$$h(t) - \frac{1}{2}\log t + \frac{1+\log 2}{2} \le J(t) \le h(t) + \frac{1}{2}\log t + 1 \qquad (t \ge 1).$$

The upper bound at an integer k follows from the trapezoidal lower bound for $\int_1^k \log t\,dt$; its extension to real $t \ge 1$ is monotonic. Jensen's inequality gives $J(t) \ge \int_{1/2}^{\lfloor t\rfloor+1/2} \log v\,dv$. Since $t < \lfloor t\rfloor + 1$ and h has derivative $\log t$,

$$h(t) - h(\lfloor t\rfloor + 1/2) \le \tfrac{1}{2}\log t.$$

This proves the lower bound.

Consider the factorial combination

$$Q(x) = J(x) - J(x/2) - J(x/3) - J(x/5) + J(x/30).$$

The displayed bounds imply, for $x \ge 30$,

$$Ax - \frac{5}{2}\log x + \log 60 - 2 \le Q(x) \le Ax + \frac{5}{2}\log x - \log 30 + \frac{1-3\log 2}{2}.$$

In particular,

$$Ax - \frac{5}{2}\log x + 2 < Q(x) < Ax + \frac{5}{2}\log x - 3. \tag{C.10}$$

The function

$$f(t) = \lfloor t\rfloor - \lfloor t/2\rfloor - \lfloor t/3\rfloor - \lfloor t/5\rfloor + \lfloor t/30\rfloor$$

is periodic with period 30, and is constant on each unit interval. In one period its value is one precisely on the intervals whose left endpoints are

$$1, 2, 3, 4, 5, 7, 8, 9, 11, 13, 14, 17, 19, 23, 29;$$

elsewhere its value is zero. In particular it is one on $[1, 6)$. The factorial valuation formula therefore gives

$$Q(x) = \sum_{p^a \le x} f(x/p^a)\log p, \qquad \psi(x) - \psi(x/6) \le Q(x) \le \psi(x).$$

The lower bound for ψ follows at once.

We also need the elementary bound $\psi(t) < t\log 4$ for $t \ge 1$. Equivalently, $\operatorname{lcm}(1,\dots,k) < 4^k$ for integers $k \ge 1$. The case $k = 1$ is immediate. Induct on k. For even k, the lcm increases from its preceding value by a factor at most two. For $k = 2m+1$, each new prime power above $m+1$ contributes its prime as a factor of $\binom{2m+1}{m}$, so

$$\operatorname{lcm}(1,\dots,2m+1) \le \operatorname{lcm}(1,\dots,m+1)\binom{2m+1}{m} < 4^{m+1}4^m.$$

The binomial bound follows by adding its two equal central coefficients.

Iterate $\psi(x) \le Q(x) + \psi(x/6)$ until $t = x/6^k$ lies in $[5, 30)$. The linear terms sum to $b(x-t)$, whereas $\psi(t) < t \log 4$ and $(\log 4 - b)t < 9$. The remaining sum is at most

$$\sum_{j=0}^{k-1} \left(\frac{5}{2}(\log x - j \log 6) - 3 \right) = -\frac{5}{4} \log 6 \, k^2 + \left(\frac{5}{2} \log x + \frac{5}{4} \log 6 - 3 \right) k \le H(x) - 9,$$

by completing the square. This proves the upper bound for ψ.

To remove prime powers, absorb all even exponents into $\psi(\sqrt{x})$:

$$\psi(x) - \vartheta(x) = \psi(\sqrt{x}) + \sum_{\substack{a \ge 3 \\ a \text{ odd}}} \vartheta(x^{1/a}).$$

There are at most $(\log x)/(2 \log 2) - 3/2$ possible odd exponents at least five. The preceding elementary bound for ψ thus gives

$$\frac{\psi(x) - \vartheta(x)}{\sqrt{x}} < \log 4 \left(1 + x^{-1/6} + \left(\frac{\log x}{2 \log 2} - \frac{3}{2} \right) x^{-3/10} \right).$$

For $x \ge 256$, the second term in parentheses is less than $2/5$. The last term decreases on this range, since $\log 2 > 2/3$, and at 256 it equals $(5/2)2^{-12/5} < 1/2$. Hence the parentheses are less than $19/10$, and $\log 4 < 7/5$ gives the claimed bound $8/3$.

Finally $r(n) \log n \ge \vartheta(n) - \vartheta(n/2)$; insert the two estimates to obtain the stated bound. The logarithm comparisons used here and below follow from

$$\log \frac{1+t}{1-t} = 2 \sum_{j \ge 0} \frac{t^{2j+1}}{2j+1} \qquad (0 < t < 1),$$

obtained by integrating the geometric series. The first three terms at $t = 1/3$ give $\log 2 > 693/1000$, and bounding the remaining denominators below by three gives $\log 2 < 25/36 < 7/10$. The first four terms at $t = 1/2$ give $\log 3 > 1098/1000$. Finally $\log 5 = 2 \log 2 + \log(5/4)$; the first two terms at $t = 1/9$ give $\log 5 > 1609/1000$. These three lower bounds give $A > 23/25$ and $\log 6 > 25/14$. The same upper-tail bound at $t = 1/5$ gives $\log(3/2) < 73/180 < 21/50$, so $\log 2 + 6/5 - \frac{1}{2} \log 6 > 99/100$. □

Lemma C.9 (Fresh prime counts)**.** *For every $n \ge 67$, $r(n) \ge \lfloor \sqrt{n} \rfloor$. Moreover,*

$$\begin{aligned} &r(n) > n/30, && 1024 \le n \le 32768, \\ &r(n) > 7n/(20 \log n) > 6\sqrt{n}, && n \ge 32768. \end{aligned}$$

Proof. Lemma C.7 covers $67 \le n \le 1023$. Assume $n \ge 1024$, and put $L = \log n$ and

$$P(L) = \frac{7}{10} \left(L - \frac{99}{100} \right)^2 + \frac{5}{2} L + 7,$$
$$K(L) = \frac{46}{125} - \frac{8}{3} e^{-L/2} - e^{-L} P(L).$$

Lemma C.8 gives

$$\frac{r(n) L}{n} > K(L). \tag{C.11}$$

Indeed, its error term satisfies $H(n/2) < (7/10)(L - 99/100)^2 + 9$: use $5/(4 \log 6) < 7/10$, $\log 2 + 6/5 - (1/2) \log 6 > 99/100$, and $L > 6$.

For $L \ge 6$, K is increasing and strictly concave. Direct differentiation reduces these assertions to $P - P' > 0$ and

$$P - 2P' + P'' = \frac{7}{10} \left\{ \left(L - \frac{299}{100} \right)^2 - 2 \right\} + \frac{5}{2} L + 2 > 0.$$

Both inequalities hold throughout $L \geq 6$; for the first, write $P - P' = (7/10)\{(L - 99/100)^2 - 2(L - 99/100)\} + (5/2)L + 9/2$. Thus $K(L) - L/30$ is strictly concave as well.

At $n = 1024$, use $L < 7$, $\sqrt{n} = 32$, and $P(7) < 50$ to obtain

$$K(L) - L/30 > \frac{46}{125} - \frac{1}{12} - \frac{50}{1024} - \frac{7}{30} = \frac{481}{192000} > 0.$$

At $n = 32768 = 2^{15}$, use $L < 21/2$, $\sqrt{n} > 180$, and $P(21/2) < 97$ to obtain

$$K(L) - \frac{7}{20} > \frac{46}{125} - \frac{2}{135} - \frac{97}{32768} - \frac{7}{20} = \frac{24881}{110592000} > 0.$$

Since $L/30 < 7/20$ at this endpoint, concavity proves $K(L) > L/30$ throughout the first range. Since K is increasing, its value remains greater than $7/20$ throughout the second range. Equation (C.11) proves both estimates.

For $1024 \leq n \leq 32768$, $n/30 > \sqrt{n}$. For larger n, $\sqrt{n}/\log n$ is increasing and, at 32768,

$$\frac{7}{20}\frac{\sqrt{n}}{\log n} > \frac{7}{20}\frac{180}{21/2} = 6.$$

□

C.5 Small support primes

Proposition C.10 (Small support primes)**.** *Let $n \geq 67$. If a normalized nonconstant D has u terms and largest support prime $q \leq 13$ with $q < 2(u-1)$, then* $\mathrm{wt}(P_{n,c}D) \geq n$.

Proof. For $q = 2$, every rough component has at least two terms, so

$$\mathrm{wt}(P_{n,c}D) \geq 2C_2(n) = 2\lceil n/2 \rceil \geq n.$$

For $q = 3$, the hypothesis gives $u \geq 3$. Each component has at least three terms except that the index-two components have at least four: their two nonempty 3-valuation slices each have two endpoints. Thus

$$\mathrm{wt}(P_{n,c}D) \geq 3C_3(n) + C_3(n/2) - C_3(n/3).$$

The residues $1, 5$ modulo 6 give $3C_3(n) \geq n - 1$. Their successive gaps are at most four, so the interval $(n/3, n/2]$, of length $n/6 \geq 4$, contains a 3-rough integer. This proves the required bound for $q = 3$.

For $q = 5$, every component has at least four terms, giving

$$\mathrm{wt}(P_{n,c}D) \geq 4C_5(n) \geq \frac{16n}{15} - \frac{56}{15} \geq n \qquad (n \geq 56).$$

For $q = 7, 11, 13$, the hypothesis gives $u \geq 5, 7, 8$, respectively. The component profile gives

$$\begin{aligned} H_7(n) &:= 5C_7(n) - C_7(n/2) + C_7(n/3), \\ H_{11}(n) &:= 7C_{11}(n) - 3C_{11}(n/2) + 2C_{11}(n/3), \\ H_{13}(n) &:= 8C_{13}(n) - 4C_{13}(n/2) + 2C_{13}(n/3) + C_{13}(n/5), \end{aligned}$$

and $\mathrm{wt}(P_{n,c}D) \geq H_q(n)$. Indeed, after the index-one component of weight u, the lower profiles are respectively

$$(4, 5, 5, \ldots), \qquad (4, 6, 6, \ldots), \qquad (4, 6, 6, 7, 7, \ldots),$$

starting at component index two. Increasing u above these minima adds the corresponding nonnegative multiple of $J_q(n)$.

Equivalently,

$$H_7 = 4C_7 + J_7 + C_7(n/3),$$
$$H_{11} = 4C_{11} + 3J_{11} + 2C_{11}(n/3),$$
$$H_{13} = 4C_{13} + 4J_{13} + 2C_{13}(n/3) + C_{13}(n/5).$$

The base-5 one-step sieve has constants

q	7	11	13
α_q	8/35	236/1155	184/1001
E_q	28/15	14/5	56/15

where $C_q(t) \geq \alpha_q t - E_q$ and $J_q(t) \geq \alpha_q t/2 - 2E_q$. Substituting in the positive expressions above gives

$$H_7(n) \geq \frac{116n - 1372}{105}, \qquad H_{11}(n) \geq \frac{4366n - 116424}{3465}, \qquad H_{13}(n) \geq \frac{18952n - 840840}{15015}.$$

These bounds exceed $n-1$ for $n \geq 116, 126, 210$, respectively, so integrality gives the result in those ranges. The remaining ranges are covered by the following blocks. For a row $[a, b]$ and a column q, put

$$\beta_7 = \min(b, 115), \quad \beta_{11} = \min(b, 125), \quad \beta_{13} = b.$$

When $a \leq \beta_q$, monotonicity of C_q gives the lower bound B_q obtained from H_q by evaluating terms with positive coefficients at a/d and the sole term with a negative coefficient at $\beta_q/2$. Thus $H_q(n) \geq B_q$ on the remaining part $[a, \beta_q]$ of that block.

$[a, b]$	B_7	B_{11}	B_{13}
$[67, 76]$	76	89	91
$[77, 85]$	86	102	105
$[86, 94]$	94	110	114
$[95, 101]$	101	121	127
$[102, 110]$	110	132	139
$[111, 145]$	126	149	149
$[146, 181]$	–	–	181
$[182, 209]$	–	–	238

Every entry is at least the upper endpoint β_q to which it applies. The dashes mean that the preceding linear estimate already applies.

The entries follow from (C.5) and

$$C_7(t) = C_5(t) - C_5(t/7), \quad C_{11}(t) = C_7(t) - C_7(t/11), \quad C_{13}(t) = C_{11}(t) - C_{11}(t/13).$$

For example, in the row $[111, 145]$ the counts at $111, \beta_q/2, 37, 111/5$ are respectively $(26, 13, 9, 5)$, $(25, 14, 8, 4)$, and $(24, 15, 7, 3)$. They give $B_7 = 126$, $B_{11} = 149$, and $B_{13} = 149$. □

C.6 Larger support primes

Lemma C.11 (Reciprocal sums)**.** *One has*

$$\sum_{7 \leq p \leq 53} \frac{1}{p} < \frac{259}{400}, \qquad \sum_{11 \leq p \leq 149} \frac{1}{p} < \frac{229}{320}, \qquad \sum_{11 \leq p \leq 271} \frac{1}{p} < \frac{33}{40}.$$

Proof. Since $\sqrt{271} < 17$, the primes from 17 through 271 are exactly the integers in that range coprime to $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13$. Adding $11, 13$ gives the following list. Let B_j be the reciprocal sum of these primes in $[30j, 30j + 30)$, truncated at 271. The row sums satisfy:

j	denominators in B_j	$4000B_j$ is less than
0	$11, 13, 17, 19, 23, 29$	1429
1	$31, 37, 41, 43, 47, 53, 59$	657
2	$61, 67, 71, 73, 79, 83, 89$	381
3	$97, 101, 103, 107, 109, 113$	230
4	$127, 131, 137, 139, 149$	147
5	$151, 157, 163, 167, 173, 179$	146
6	$181, 191, 193, 197, 199$	105
7	$211, 223, 227, 229, 233, 239$	106
8	$241, 251, 257, 263, 269$	79
9	271	15

The first five upper bounds sum to 2844, and all ten sum to 3295. The first budget follows from the first two rows, since

$$\sum_{7 \le p \le 53} \frac{1}{p} < \frac{1}{7} + \frac{1429 + 657}{4000} - \frac{1}{59} = \frac{259}{400} - \frac{19}{206500} < \frac{259}{400}.$$

The other two reciprocal sums are less than $711/1000$ and $659/800$, respectively. Since $711/1000 < 229/320$ and $659/800 < 33/40$, the claims follow. □

For a prime $q \ge 17$, put

$$h_q = \pi(q) - 2, \qquad \alpha_q = \frac{4}{15}\left(1 - \sum_{7 \le p \le q} \frac{1}{p}\right).$$

The one-step sieve, applied separately to C and J with their two discrepancies, gives

$$C_q(x) \ge \alpha_q x - \frac{14}{15} h_q, \qquad J_q(x) \ge \frac{\alpha_q x}{2} - \frac{22}{15} h_q.$$

Lemma C.12 (Support primes from 17 through 53)**.** *Let D be a normalized multiplier of weight u, with largest support prime $17 \le q \le 53$ and $q < 2(u-1)$. For every $n \ge 1024$, one has $\mathrm{wt}(P_{n,c}D) > n$.*

Proof. Rewrite (C.4) as

$$\mathrm{wt}(P_{n,c}D) \ge 4C_q(n) + (u-4)J_q(n) + 2C_q(n/3) + 2C_q(n/5).$$

The preceding discrepancies imply

$$\mathrm{wt}(P_{n,c}D) \ge \alpha_q \left(\frac{u}{2} + \frac{46}{15}\right) n - \frac{22u + 24}{15} h_q. \tag{C.12}$$

Use the hypothesis $q < 2(u-1)$ and the five columns

q in	$[17, 23]$	$[29, 37]$	$[41, 43]$	$\{47\}$	$\{53\}$
u_*	10	16	22	25	28
a	7/50	7/60	13/125	99/1000	47/500
h_*	7	10	12	13	14

Here $u \ge u_*$, $h_q \le h_*$, and $\alpha_q > a$ throughout each band. The reciprocal comparisons all follow from the single inequality

$$\sum_{7 \le p \le 53} \frac{1}{p} < \frac{259}{400},$$

from Lemma C.11: subtract the terms above the endpoint of each band. At $n = 1024$ and $u = u_*$, the right side of (C.12), with a, h_* in place of α_q, h_q, exceeds n by, respectively,

$$\frac{6964}{375}, \quad \frac{10672}{225}, \quad \frac{126832}{1875}, \quad \frac{106162}{1875}, \quad \frac{40192}{1875}.$$

The slope in u is at least $1024(47/1000) - 22 \cdot 14/15 > 27$. The positive corner values also imply a positive slope in n. Both slopes increase with the other variable, proving the bound for all $n \geq 1024$ and $u \geq u_*$. □

Lemma C.13 (Support primes from 59 through 271)**.** *Let D be a normalized multiplier of weight u, with largest support prime $59 \leq q \leq 271$ and $q < 2(u-1)$. For every $n \geq 32768$, one has* $\mathrm{wt}(P_{n,c}D) > n$.

Proof. Use $R = \{2, 3, 5, 7\}$ as the fixed small sieve. Its density and discrepancy are $\rho = 8/35$ and $\Delta = 28/15$, the latter following by adding 7 to the modulo-thirty sieve. The one-step bound is

$$\mathrm{wt}(P_{n,c}D) \geq \frac{u+4}{2}\alpha n - 2(u-2)E,$$

where

$$\alpha = \frac{8}{35}\left(1 - \sum_{11 \leq p \leq q} \frac{1}{p}\right), \qquad E = \frac{28}{15}\{\pi(q) - 3\}.$$

The modulo-thirty discrepancy gives $\pi(q) \leq 2 + C_5(q) < 3 + 4q/15$, hence $E < 112q/225$.

Lemma C.11 gives the following bounds. The last column is the resulting lower bound minus n at $n = 32768$ and $u = u_*$:

q	u_*	$\alpha >$	$E <$	margin
59–149	31	13/200	75	778/5
151–271	77	1/25	135	1654/25

The slope in u is at least $n/50 - 270 > 0$. The positive corner values imply a positive slope in n, and both slopes increase with the other variable. This proves the claim. □

Lemma C.14 (An elementary prime-product estimate)**.** *For every odd prime q,*

$$\rho(q) = \prod_{p \leq q}(1 - 1/p) > \frac{1}{2\sqrt{q}}.$$

Proof. Including all odd composite factors decreases the product. For every odd integer $m \geq 3$, one has $(1 - 1/m)^2 > (m-2)/m$. Multiplication over $m = 3, 5, \ldots, q$ telescopes to give

$$\rho(q) \geq \frac{1}{2} \prod_{\substack{3 \leq m \leq q \\ m \text{ odd}}} (1 - 1/m) > \frac{1}{2\sqrt{q}}.$$

□

Lemma C.15 (Support primes at least 277)**.** *Let D be a normalized multiplier of weight u. Suppose $n \geq 32768$, $u < (20/7)\log n$, and its largest support prime satisfies $277 \leq q < 2(u-1)$. Then* $\mathrm{wt}(P_{n,c}D) > 5n/4$.

Proof. Put $L = \log n$. The hypotheses give

$$q < \frac{40}{7}L, \qquad L > \frac{7}{40}(q+2) \geq \frac{1953}{40} > 48.$$

The eleven-rough count has density $16/77$ and discrepancy $56/15$. For $q \geq 277$, it includes its unit, all primes greater than 11 and at most q, and the two composite integers $169 = 13^2$ and $221 = 13 \cdot 17$. Consequently

$$\pi(q) \leq C_{11}(q) + 2 \leq \frac{16}{77}q + \frac{86}{15} < \frac{16}{77}q + 6.$$

For the full q-rough sieve, write $\Delta_q = (14/15)2^{\pi(q)-3}$. Since $\log 2 < 7/10$,

$$\Delta_q < \frac{112}{15} \exp\left(\frac{16}{77}q \log 2\right) < \frac{112}{15} \exp\left(\frac{64}{77}L\right).$$

The finite error therefore satisfies

$$\frac{2u\Delta_q}{n} < \frac{128}{3}Le^{-13L/77} < 2048e^{-624/77} < \frac{2048}{2800} < \frac{3}{4}.$$

Here $Le^{-13L/77}$ decreases for $L \geq 48$, and $624/77 > 8$ while $e^8 = e^6e^2 > 20^2 \cdot 7 = 2800$. Indeed,

$$e^3 > \sum_{j=0}^{8} \frac{3^j}{j!} = \frac{89641}{4480} > 20, \qquad e^2 > \sum_{j=0}^{4} \frac{2^j}{j!} = 7.$$

On the other hand, odd-integer telescoping and $u > q/2$ give

$$\frac{u\rho(q)}{2} > \frac{\sqrt{q}}{8} > 2.$$

The positive component budget yields $\mathrm{wt}(P_{n,c}D) \geq uJ_q(n)$, and the unconditional rough discrepancy gives $J_q(n) \geq \rho(q)n/2 - 2\Delta_q$. Thus

$$\frac{\mathrm{wt}(P_{n,c}D)}{n} > 2 - \frac{3}{4} = \frac{5}{4} > 1,$$

as claimed. □

C.7 Completion of the localized estimate

Proof of Theorem C.2. Proposition C.10 handles $q \leq 13$. Otherwise $q \geq 17$ and $u \geq 10$. For $67 \leq n \leq 1023$, Lemma C.7 and (C.9) give the result.

Every prime in $(n/2, n]$ is q-rough and contributes an index-one component, so $\mathrm{wt}(P_{n,c}D) \geq ur$. We may assume $u < n/r$. For $1024 \leq n \leq 32768$, Lemma C.9 gives $u < 30$, hence $q \leq 53$, and Lemma C.12 applies. For $n \geq 32768$, the same lemma gives $u < (20/7)\log n$. Lemmas C.12, C.13, and C.15 cover respectively $q \leq 53$, $59 \leq q \leq 271$, and $q \geq 277$, which include every remaining prime. □

Acknowledgements

This work would not exist without the paper of Philippa Holdridge and Péter Pál Pach [5], whose framework it builds on throughout, as described in Section 1. We are equally grateful to Pilz, who posed the problem and settled its first cases, and to Huang, Ke, Meyer, Nagy, Pach and Szabó, whose work shaped it [1, 2, 3, 4, 6]. Any errors are ours. The formal verification depends on Lean 4 and on mathlib, and we thank their developers and contributors.

How this work was produced. The arguments in this paper, its written proofs, and the Lean 4 formalisation were developed with substantial assistance from AI systems. The written proofs have not been checked line by line by a human mathematician. Correctness rests on the formalisation: the main theorems and corollaries, and the intermediate results recorded in the proof map, are machine-checked using only the standard axioms of Lean's foundations, and every module of the development has been re-checked by an independent kernel replay (`lean4checker`). Where the printed argument and the formal proof differ, the formal proof is authoritative. We state this so that readers can weigh the work appropriately.

References

[1] G. F. Pilz, *On polynomial near-ring codes*, in *Contributions to General Algebra*, vol. 8 (Linz, 1991), Hölder-Pichler-Tempsky, Vienna, 1992, pp. 233–238.

[2] P.-Y. Huang, W.-F. Ke and G. F. Pilz, *The cardinality of some symmetric differences*, Proc. Amer. Math. Soc. **138**(3) (2010), 787–797. doi:10.1090/S0002-9939-09-10189-2.

[3] P. P. Pach and C. Szabó, *On the minimal distance of a polynomial code*, Discrete Math. Theor. Comput. Sci. **13**(4) (2011), 33–44. doi:10.46298/dmtcs.556.

[4] W.-F. Ke and J. H. Meyer, *On a conjecture regarding the symmetric difference of certain sets*, Bull. Aust. Math. Soc. **111**(3) (2025), 397–404. doi:10.1017/S0004972724000807.

[5] P. Holdridge and P. P. Pach, *On the Extended 1-2-3 Conjecture of Pilz*, 2026, arXiv:2607.00934.

[6] J. Nagy and P. P. Pach, *A sumset version of a conjecture of Pilz*, SIAM J. Discrete Math. **40**(2) (2026), 675–679. doi:10.1137/24M1654609; arXiv:2409.15075.

[7] *Pilz's Extended 1–2–3 Conjecture: proofs and Lean 4 formalisations*, Zenodo, 2026. Contains this paper and its Lean development, an earlier proof of the binary case, and a note on the density bound. Concept DOI (resolving to the latest version): doi:10.5281/zenodo.23568997.